Homework 3 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

30.10.2012

Solution to Exercise 8.

(a) Claim: $\text{Var}(I_C) = \kappa(1-\kappa) + \frac{4}{3}(n-2)(\beta - \kappa^2)$ with $\kappa = \sum_{l=1}^{m} p_l^2$ and $\beta = \sum_{l=1}^{m} p_l^3$.

Recall: $I_C = \frac{1}{\binom{n}{2}} \sum_{i<j} Y_{ij}$, where $Y_{ij} = \begin{cases} 1 & C_i = C_j \\ 0 & \text{otherwise} \end{cases}$ and $E(Y_{ij}) = \sum_{l=1}^{m} p_l^2 = \kappa$.

Then it holds

$$\text{Var}(I_C) = \text{Var}\left(\frac{1}{\binom{n}{2}} \sum_{i<j} Y_{ij}\right) = \frac{1}{\binom{n}{2}} \left(\sum_{i<j} \text{Var}(Y_{ij}) + \sum_{i<j} \sum_{\substack{k<l \\ (i,j)\neq(k,l)}} \text{Cov}(Y_{ij}, Y_{kl}) \right)$$

$$\overset{(1)}{=} \frac{1}{\binom{n}{2}} \left(\sum_{i<j} \text{Var}(Y_{ij}) + 2 \sum_{i<j} \sum_{\substack{k<l \\ (i,j)<(k,l)}} \text{Cov}(Y_{ij}, Y_{kl}) \right)$$

$$\overset{(2),(3)}{=} \frac{1}{\binom{n}{2}} \left(\sum_{i<j} \kappa(1-\kappa) + \frac{2}{3} n(n-1)(n-2)(\beta - \kappa^2) \right)$$

$$= \kappa(1-\kappa) + \frac{4}{3}(n-2)(\beta - \kappa^2)$$

(1) This equality holds for the definition:
$(i,j) < (k,l) \Leftrightarrow i < k \vee ((i = k) \wedge (j < l))$.

(2) It holds

$$\text{Var}(Y_{ij}) = E(Y_{ij}^2) - E(Y_{ij})^2 = 1^2 \cdot P(Y_{ij} = 1) - \kappa^2 = E(Y_{ij}) - \kappa^2 = \kappa(1-\kappa).$$

(3) For the covariance it holds

$$\text{Cov}(Y_{ij}, Y_{kl}) = E(Y_{ij} \cdot Y_{kl}) - E(Y_{ij}) \cdot E(Y_{kl}) = E(Y_{ij} \cdot Y_{kl}) - \kappa^2$$

Investigate: $Y_{ij} \cdot Y_{kl} = 1 \Leftrightarrow Y_{ij} = Y_{kl} = 1 \Leftrightarrow C_i = C_j \wedge C_k = C_l$.
There are three disjoint cases (i)-(iii):

(i) $\mathbf{i} = \mathbf{k}$: In that case $j < l$ must hold with respect to (1). Hence,

$$Y_{ij} \cdot Y_{il} = 1 \Leftrightarrow Y_{ij} = Y_{il} = 1 \Leftrightarrow C_i = C_j \wedge C_i = C_l \Leftrightarrow C_i = C_j = C_l$$

$$\Rightarrow E(Y_{ij} \cdot Y_{il}) = 1 \cdot P(Y_{ij} \cdot Y_{il} = 1) = P(C_i = C_j = C_l) = \sum_{n=1}^{m} p_n^3 = \beta$$

$$\Rightarrow \text{Cov}(Y_{ij}, Y_{il}) = E(Y_{ij} \cdot Y_{il}) - \kappa^2 = \beta - \kappa^2 = \alpha$$

(ii) $\mathbf{i} < \mathbf{k} \wedge \mathbf{j} = \mathbf{l}:$ In that case it holds

$$\begin{aligned}
&Y_{ij} \cdot Y_{kj} = 1 \Leftrightarrow Y_{ij} = Y_{kj} = 1 \Leftrightarrow C_i = C_j \wedge C_k = C_j \Leftrightarrow C_i = C_j = C_k \\
\Rightarrow &E(Y_{ij} \cdot Y_{kj}) = 1 \cdot P(Y_{ij} \cdot Y_{kj} = 1) = P(C_i = C_j = C_k) = \sum_{n=1}^{m} p_n^3 = \beta \\
\Rightarrow &\operatorname{Cov}(Y_{ij}, Y_{kj}) = E(Y_{ij} \cdot Y_{kj}) - \kappa^2 = \beta - \kappa^2 = \alpha
\end{aligned}$$

(iii) $\mathbf{i} < \mathbf{k} \wedge \mathbf{j} \neq \mathbf{l}:$ In that case it holds that the indices are pairwise unequal. Therefore,

$$\begin{aligned}
&Y_{ij} \cdot Y_{kl} = 1 \Leftrightarrow Y_{ij} = Y_{kl} = 1 \Leftrightarrow C_i = C_j \wedge C_k = C_l \\
\Rightarrow &E(Y_{ij} \cdot Y_{kl}) = 1 \cdot P(Y_{ij} \cdot Y_{kl} = 1) = P(Y_{ij} = 1) \cdot P(Y_{kl} = 1) = \kappa^2 \\
\Rightarrow &\operatorname{Cov}(Y_{ij}, Y_{kl}) = E(Y_{ij} \cdot Y_{kl}) - \kappa^2 = \kappa^2 - \kappa^2 = 0
\end{aligned}$$

It follows:

$$\begin{aligned}
&2 \sum_{i<j} \sum_{k<l,(i,j)<(k,l)} \operatorname{Cov}(Y_{ij}, Y_{kl}) \\
=&2 \sum_{i<j} \left(\sum_{l=j+1}^{n} \operatorname{Cov}(Y_{ij}, Y_{il}) + \sum_{k=i+1}^{n} \left(\operatorname{Cov}(Y_{ij}, Y_{kj}) + \sum_{l=k+1,l\neq j}^{n} \operatorname{Cov}(Y_{ij}, Y_{kl}) \right) \right) \\
=&2 \sum_{i<j} \left(\sum_{l=j+1}^{n} \alpha + \sum_{k=i+1}^{n} \left(\alpha + \sum_{l=k+1,l\neq j}^{n} 0 \right) \right) \\
\overset{(4)(5)}{=}&2\alpha \left(\frac{1}{6} n(n-1)(n-2) + \frac{1}{6} n(n-1)(n-2) \right) \\
=&\frac{2}{3} (\beta - \kappa^2) n(n-1)(n-2)
\end{aligned}$$

(4) It holds

$$\begin{aligned}
&\sum_{i<j} \sum_{l=j+1}^{n} \alpha = \sum_{i=1}^{n} \sum_{j=i+1}^{n} \sum_{l=j+1}^{n} \alpha = \alpha \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} (n-j) = \alpha \sum_{i=1}^{n-1} \sum_{j=1}^{n-i-1} j \\
&= \frac{\alpha}{2} \sum_{i=1}^{n-1} (n-i)(n-i-1) = \frac{\alpha}{2} \sum_{i=1}^{n-2} (n^2 - n\,i - n - n\,i + i^2 + i) \\
&= \frac{\alpha}{2} \left[(n-2)(n^2-n) + (1-2n) \sum_{i=1}^{n-2} i + \sum_{i=1}^{n-2} i^2 \right] \\
&= \frac{\alpha}{2} \left[(n-2)(n-1)n + (1-2n) \frac{1}{2} (n-1)(n-2) + \frac{1}{3} (n-1)^3 - \frac{1}{2} (n-1)^2 + \frac{1}{6} (n-1) \right] \\
&= \frac{\alpha}{12} (n-1) \left[6n^2 - 12n - 6n^2 + 15n - 6 + 2n^2 - 4n + 2 - 3n + 3 + 1 \right] \\
&= \frac{\alpha}{12} (n-1) \left[2n^2 - 4n \right] = \frac{\alpha}{6} n(n-1)(n-2)
\end{aligned}$$

(5) It holds

$$\begin{aligned}
\sum_{i<j} \sum_{k=i+1}^{n} \alpha &= \sum_{i=1}^{n} \sum_{j=i+1}^{n} \sum_{k=i+1}^{j-1} \alpha = \alpha \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} (j-1-i) \\
&= \alpha \sum_{i=1}^{n} \sum_{j=1}^{n-i-1} j \overset{(4)}{=} \frac{\alpha}{6} n(n-1)(n-2)
\end{aligned}$$

Solution to Exercise 9.

Theorem 4.3 shall be proven.

(a) X is a discrete random variable with $p_i = P(X = x_i)$, $i = 1, \ldots, m$. It holds

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

as $p_i \geq 0$ and $-\log p_i \geq 0$ for $0 < p_i \leq 1$ and $0 \cdot \log 0 = 0$ per definition. Equality holds, if all addends are zero, i.e.,

$$p_i \log p_i = 0 \Leftrightarrow p_i \in \{0, 1\} \quad i = 1, \ldots, m,$$

as $p_i > 0$ and $-\log p_i > 0$, thus, $-p_i \log p_i > 0$ for $0 < p_i < 1$.

(b)

$$\begin{aligned}
H(X) - \log m &= -\sum_i p_i \log p_i - \underbrace{\sum_i p_i}_{=1} \log m \\
&= \sum_{i:p_i>0} p_i \log \frac{1}{m\,p_i} \\
&= (\log e) \sum_{i:p_i>0} p_i \ln \frac{1}{m\,p_i} \\
&\overset{\ln z \leq z-1}{\leq} (\log e) \sum_{i:p_i>0} p_i \left(\frac{1}{m\,p_i} - 1 \right) \\
&= (\log e) \left(\sum_{i:p_i>0} \frac{1}{m} - 1 \right) \leq 0.
\end{aligned}$$

As $\ln z = z - 1$ only holds for $z = 1$ it follows that equality holds iff $p_i = 1/m$, $i = 1, \ldots, m$. In particular, it follows $p_i > 0$, $i = 1, \ldots, m$.

(c) Define for $i = 1, \ldots, m$ and $j = 1, \ldots, d$

$$p_{i|j} = P(X = x_i \mid Y = y_j).$$

Show $H(X \mid Y) - H(X) \leq 0$ which is equivalent to the claim.

$$\begin{aligned}
H(X \mid Y) - H(X) &= -\sum_{i,j} p_{i,j} \log p_{i|j} + \sum_i p_i \log p_i \\
&= -\sum_{i,j} p_{i,j} \log \frac{p_{i,j}}{p_j} + \sum_i \underbrace{\sum_j p_{i,j}}_{=p_i} \log p_i \\
&= \log(e) \sum_{i,j:p_{i,j}>0} p_{i,j} \ln \frac{p_i\, p_j}{p_{i,j}} \\
&\overset{\ln z \leq z-1}{\leq} \log(e) \sum_{i,j:p_{i,j}>0} p_{i,j} \left(\frac{p_i\, p_j}{p_{i,j}} - 1 \right) \\
&= \log(e) \left(\sum_{i,j:p_{i,j}>0} p_i\, p_j - 1 \right) \leq 0
\end{aligned}$$

Note that from $p_{i,j} > 0$ it follows $p_i, p_j > 0$. Equality hold for $\frac{p_i\, p_j}{p_{i,j}} = 1$ which is equivalent to X and Y being stochastically independent.

This means that the transinformation $I(X, Y) = H(X) - H(X \mid Y)$ is nonnegative.

(d) It holds

$$\begin{aligned}
H(X, Y) &= -\sum_{i,j} p_{i,j} \log p_{i,j} \\
&= -\sum_{i,j} p_{i,j} \left[\log p_{i,j} - \log p_i + \log p_i\right] \\
&= -\sum_{i,j} p_{i,j} \log \underbrace{\frac{p_{i,j}}{p_i}}_{p_{j|i}} - \sum_i \underbrace{\sum_j p_{i,j}}_{=p_i} \log p_i \\
&= H(Y \mid X) + H(X).
\end{aligned}$$

(e) It holds

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

with equality as in (c) iff X and Y are stochastically independent.