

CORRECTIONS

Lecture 5 Page 5

Correct

$$\mathbb{P}(A_j = a_j | a_1 = a_1, A_2 = a_2, \dots, A_{j-1} = a_{j-1}) = \mathbb{P}(A_j = a_j | A_{j-1} = a_{j-1})$$

to

$$\mathbb{P}(A_j = a_j | A_1 = a_1, A_2 = a_2, \dots, A_{j-1} = a_{j-1}) = \mathbb{P}(A_j = a_j | A_{j-1} = a_{j-1})$$

Lecture 5 Page 6

Correct $H(A_{r-1}|A_r)$ to $H(A_{r-1}|A_{r-2})$ in the second displayed equation to get:

$$\begin{aligned} H(A_1, A_2, \dots, A_r) &= H(A_r | A_{r-1}) + H(A_{r-1} | A_{r-2}) + \dots + H(A_2 | A_1) + H(A_1) \\ &= (r-1)H(A_2 | A_1) + H(A_1) . \end{aligned}$$

Example Sheet 1 Question 7

The inequality in the displayed equation should be reversed to give:

$$H((1-\lambda)\mathbf{p} + \lambda\mathbf{q}) \geq (1-\lambda)H(\mathbf{p}) + \lambda H(\mathbf{q}) .$$

Lecture 7

Correct Corollary 7.6 to:

Corollary 7.6

Let $c: \mathcal{A} \rightarrow \{0, 1\}^N$ be a code with minimum distance δ . Then

$$K = |\mathcal{A}| \leq \frac{2^N}{V(N, \lfloor \frac{1}{2}(\delta + 1) \rfloor)} .$$

Moreover, there is a code with minimum distance δ and

$$K = |\mathcal{A}| \geq \frac{2^N}{V(N, \delta)} .$$

Lecture 10

Correct equation (1) to

$$\mathbb{P}(d(\mathbf{c}_o, \mathbf{c}'_o) \geq r) \leq \frac{p(1-p)}{N(q-p)^2} \quad (1).$$

and make the same change ($q \mapsto (q-p)$) in later equations (twice).

Example Sheet 2 Question 17

The letters Y and Z were interchanged. The question should read:

Data Processing Inequality

Consider two independent channels in series. A random variable X is sent through channel 1 and received as Y . This is then sent through channel 2 and received as Z . Our aim is to prove that $I(X, Z) \leq I(X, Y)$, so the further processing of the second channel can only reduce the mutual information.

The independence of the channels means that, if we condition on the value of Y , then $(X|Y = y)$ and $(Z|Y = y)$ are independent. Deduce that

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

By writing the conditional entropies as $H(A|B) = H(A, B) - H(B)$, show that

$$H(X, Y, Z) + H(Y) = H(X, Y) + H(Y, Z) .$$

Define $I(X, Y|Z)$ as $H(X|Z) + H(Y|Z) - H(X, Y|Z)$ and show that

$$I(X, Y|Z) = I(X, Y) - I(X, Z) .$$

Deduce from this the *data processing inequality*:

$$I(X, Z) \leq I(X, Y) .$$

When is there equality?

Lecture 11 Proof of Proposition 11.2

The displayed equation is wrong. In order to correspond with the words, it should read

$$f = \left(\sum_{M \notin I} \alpha_I \pi_I \right) + \left(\sum_{M \in I} \alpha_I \pi_{I \setminus \{M\}} \right) \pi_M = f_0 + f_1 \cdot \pi_M .$$

Lecture 13 Proof of Theorem 13.3

The displayed matrix equation should be:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{2(N-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \alpha^{3(\delta-1)} & \dots & \alpha^{(N-1)(\delta-1)} \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \\ p_2 \\ \vdots \\ p_{N-2} \\ p_{N-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Lecture 20 20.4 The Elgamal Signature Scheme

The least common multiple and highest common factor are confused in the explanation of why different random numbers must be used in the Elgamal signature scheme. It should read:

Recall that $xs \equiv h \pmod{m}$ has either no solutions for x or else (m, s) solutions modulo m . Hence, there are $(p-1, s_1 - s_2)$ solutions for k modulo $p-1$.

⋮

This gives $(p-1, r)$ solutions for b .

Lecture 21 21.3 Semantic Security

j became an i in the displayed equation defining $e(a_j)$. It should read:

Now Bob encrypts his message m as $e(a_1)e(a_2) \dots e(a_K)$ where

$$e(a_j) \equiv \begin{cases} x_j^2 \pmod{N} & \text{when } a_j = 0 \\ yx_j^2 \pmod{N} & \text{when } a_j = 1 \end{cases}.$$

Exercise Sheet 4 Question 8

This question is wrong and should not ask for a homomorphism attack on the Elgamal signature scheme. Replace it by:

8. Describe the Elgamal signature scheme.

Alice uses the Elgamal signature scheme to sign a sequence of messages, incrementing the value of k by 2 for each new message. Show how to determine Alice's private key from any two successive signed messages.

These corrections have been made to the files here. I am sorry that they occurred. Please let me know of any further corrections that are necessary.