**MATH3411 INFORMATION, CODES & CIPHERS**

**Test 1, Session 2 2011, SOLUTIONS**

# Version A

Multiple choice: d,b,e,b,e
True/False: T, F, F, F, T

1. **(d)**:

2. **(b)**: $I(A, B) = H(B) - H(B \mid A) = H(0.1 + 0.4p) - (0.7p + 0.2)$, differentiating with respect to $p$ gives the turning point at
$$0.4 \log_2((0.1 + 0.4p)^{-1} - 1) = 0.7,$$
or $(0.1 + 0.4p)^{-1} = 2^{7/4} + 1 \approx 4.36$. Solving for $p$ gives $p \approx 0.32$.

3. **(e)**:



4. **(b)**: We find $x_1 = 10$ and $x_2 = 101$, so $|x_2 - x_1| = 91 = 7 \times 13$, so $\gcd(|x_2 - x_1|, n) = 13$ (or use Euclidean algorithm).



5. **(e)**: the output stream is 3, 0, 5, 6, 2, 4 then repeats.

6. (a) **True**: $\dfrac{L^{(n)}}{n} < H(S) + \dfrac{1}{n}$, so average has to be less than 2.75.



   (b) **False**: entropy of output is zero if all symbols are corrupted to 0 (say), and equiprobable input has binary entropy 1.

   (c) **False**: it is 8.

   (d) **False**: number of primitive elements is $\phi(48) = \phi(16)\phi(3) = (16 - 8) \times 2 = 16$.

   (e) **True**: because then $\alpha(\alpha^2 + 1) = \alpha^3 + \alpha = 1 = \alpha^7$.

7. (a) 2.179

   (b) The respective lengths are 1, 2, 2, 2, 3, and the code is then 0, 10, 11, 12, 200 with average length $\dfrac{7}{4} = 1.75$.

   (c) The shortest codeword will correspond to $s_1 s_1 s_1$ with probability $3^{-3}$. Its length is then $\ell$ with $2^{\ell-1} < 3^3 = 27 \le 2^\ell$ and we need $\ell = 5$.

   The second shortest will correspond to $s_2 s_1 s_1$ (or some permutation) with probability $(3^2 \times 4)^{-1} = 36^{-1}$. So with length $\ell$ we have $2^{\ell-1} < 36 < 2^\ell$ and so the length is 6.

## Version B

Multiple Choice: a, c, d, d, e
True/False: T, T, T, T, F

1. **(a)**:

2. **(c)**: $I(A, B) = H(B) - H(B \mid A) = H(0.1 + 0.5p) - (0.8p + 0.3)$, differentiating with respect to $p$ gives the turning point at

$$0.5 \log_2((0.1 + 0.5p)^{-1} - 1) = 0.8,$$

or $(0.1 + 0.5p)^{-1} = 2^{8/5} + 1 \approx 4.03$. Solving for $p$ gives $p \approx 0.30$.

3. **(d)**:

4. **(d)**: We find $x_1 = 10$ and $x_2 = 101$, so $|x_2 - x_1| = 91 = 7 \times 13$, so $\gcd(|x_2 - x_1|, n) = 91$ (or use Euclidean algorithm).



5. **(e)**: the output stream is $1, 0, 4, 2, 3, 6$ then repeats.

6. (a) **True**: $\dfrac{L^{(n)}}{n} < H(S) + \dfrac{1}{n}$, so average has to be less than 2.6.



   (b) **True**: entropy of output is zero if all symbols are corrupted to 0 (say), and equiprobable input has binary entropy 1.



   (c) **False**:

   (d) **True**: number of primitive elements is $\phi(120) = \phi(8)\phi(3)\phi(5) = (8 - 4) \times 2 \times 4 = 32$.

   (e) **False**: because then $\alpha(\alpha^2 + 1) = \alpha^3 + \alpha \neq 1$, and $\alpha^7 = 1$.

7. (a) 2.091

   (b) The respective lengthes are 1, 2, 2, 3, 3, and the code is then 0, 10, 11, 120, 121 with average length $\dfrac{107}{60} \approx 1.78$.

   (c) The longest codeword will correspond to $s_5 s_5$ with probability $12^{-2}$. Its length is then $\ell$ with $2^{\ell-1} < 12^2 = 144 \leq 2^{\ell}$ and we need $\ell = 8$.

   The second longest will correspond to $s_4 s_5$ (or $s_5 s_4$) with probability $(120)^{-1}$. So with length $\ell$ we have $2^{\ell-1} < 120 < 2^{\ell}$ and so the length is 7.