Test 2 Session 2 2015 SOLUTIONS

Version A

Multiple choice: **c**, **c**, **a**, **d**, **d**
True/False: **T**, **F**, **T**, **T**, **T**.

1. **(c)**: Encode the message $bba\bullet$:

	subinterval start	**width**
begin	0	1
b	0.4	0.5
b	$0.4 + 0.4 \times 0.5 = 0.6$	$0.5 \times 0.5 = 0.25$
a	0.6	$0.4 \times 0.25 = 0.1$
$\bullet$	$0.6 + 0.9 \times 0.1 = 0.69$	$0.1 \times 0.1 = 0.01$

so the message encodes as a number in the interval $[0.69, 0.70)$.

2. **(c)**: $M_H = \dfrac{7}{12}H(0.5) + \dfrac{5}{12}H(0.7) \approx 0.951$.

3. **(a)**: Note that $H(\frac{5}{8}) = H(\frac{3}{8})$.

4. **(d)**: $\phi(125) = \phi(5^3) = 5^3 - 5^2 = 100$, so by Euler's Theorem,

$$2^{2015} \equiv (2^{100})^{20} \times 2^{15} \equiv 1^{20} \times (2^7)^2 \times 2 \equiv 128^2 \times 2 \equiv 3^2 \times 2 \equiv 18 \pmod{125}.$$

5. **(d)** $\gcd(9, 28) = 1$ and $9^{27} \equiv 1 \pmod{28}$.

6. (i) **True**: $a|aa|ab|aaa|aab|aaaa$
   (ii) **False**: The binary entropy is approximately 1.53.

   (iii) **True**: $t = 46$ and $s = 15$, so $a = 31$ and $b = 61$.
   (iv) **True**: The longest two codeword lengths are 5 and 7.
   (v) **True**: There are $\phi(48) = 16$ primitive elements in $GF(49)$.

7. (i) Here, we have that $\alpha^3 = \alpha + 1$:

$$\boxed{\begin{aligned} \alpha^1 &= \alpha \\ \alpha^2 &= \alpha^2 \\ \alpha^3 &= \alpha + 1 \\ \alpha^4 &= \alpha^2 + \alpha \\ \alpha^5 &= \alpha^2 + \alpha + 1 \\ \alpha^6 &= \alpha^2 + 1 \\ \alpha^7 &= 1 \end{aligned}}$$

   (ii)

$$\left(\begin{array}{cc|c} \alpha^3 & \alpha^5 & \alpha \\ \alpha^2 & \alpha^3 & \alpha^6 \end{array}\right) \xrightarrow[R2 = \alpha^{-2}R2]{R1 = \alpha^4 R1} \left(\begin{array}{cc|c} 1 & \alpha^2 & \alpha^5 \\ 1 & \alpha & \alpha^4 \end{array}\right) \xrightarrow{R2 = R2 - R1} \left(\begin{array}{cc|c} 1 & \alpha^2 & \alpha^5 \\ 0 & \alpha^2 + \alpha & \alpha^4 - \alpha^5 \end{array}\right) = \left(\begin{array}{cc|c} 1 & \alpha^2 & \alpha^5 \\ 0 & \alpha^4 & 1 \end{array}\right)$$

$$\xrightarrow{R2 = \alpha^3 R2} \left(\begin{array}{cc|c} 1 & \alpha^2 & \alpha^5 \\ 0 & 1 & \alpha^3 \end{array}\right) \xrightarrow{R1 = R1 - \alpha^2 R2} \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & \alpha^3 \end{array}\right)$$

   so $x = 0$ and $y = \alpha^3 = \alpha + 1$.

   (iii) $\{\alpha^5, \alpha^{10} = \alpha^3, \alpha^6, \alpha^{12} = \alpha^5, \ldots\} = \{\alpha^3, \alpha^5, \alpha^6\}$, so the minimal polynomial of α^5 is

$$\begin{aligned} (x - \alpha^3)(x - \alpha^5)(x - \alpha^6) &= x^3 - (\alpha^3 + \alpha^5 + \alpha^6)x^2 + (\alpha^3\alpha^5 + \alpha^3\alpha^6 + \alpha^5\alpha^6)x - \alpha^3\alpha^5\alpha^6 \\ &= x^3 + (\alpha + 1 + \alpha^2 + \alpha + 1 + \alpha^2 + 1)x^2 + (\alpha + \alpha^2 + \alpha^4)x + 1 \\ &= x^3 + x^2 + (\alpha + \alpha^2 + \alpha^2 + \alpha)x + 1 \\ &= x^3 + x^2 + 1\,. \end{aligned}$$

Version B

Multiple choice: **c**, **a**, **c**, **e**, **e**
True/False: **T**, **T**, **F**, **T**, **T** .

1. **(c)**:

code number rescaled	in interval	decoded symbol
0.35	$[0, 0.4)$	a
$0.35/.4 = 0.875$	$[0.4, 0.9)$	b
$(0.875 - 0.4)/.5 = 0.95$	$[0.9, 1)$	$\bullet$

2. **(a)**: $M_H = \dfrac{5}{7}H(0.8) + \dfrac{2}{7}H(0.5) \approx 0.801$.

3. **(c)**

4. **(e)**: $\phi(125) = \phi(5^3) = 5^3 - 5^2 = 100$, so by Euler's Theorem,

$$3^{2015} \equiv (3^{100})^{20} \times 3^{15} \equiv 1^{20} \times (3^5)^3 \equiv 243^3 \equiv (-7)^3 \equiv -343 \equiv 32 \pmod{125}\,.$$

5. **(e)**

6. (i) **True**: $a|aa|b|aaa|aab|ba$

   (ii) **True**: The binary entropy is approximately 1.46 and by Shannon's Theorem, we can get arbitrarily close to this.

   (iii) **False**: $a = 37$ and $b = 61$, so $2a - b = 13$.

   (iv) **True**: The two shortest codeword lengths are 1 and 3.

   (v) **True**: $3^5 \equiv 15 \pmod{19}$ and $\gcd(5, 18) = 1$.

7. (i) Here, we have that $\alpha^3 = \alpha^2 + 1$:

$$\boxed{\begin{aligned} \alpha^1 &= \alpha \\ \alpha^2 &= \alpha^2 \\ \alpha^3 &= \alpha^2 + 1 \\ \alpha^4 &= \alpha^2 + \alpha + 1 \\ \alpha^5 &= \alpha + 1 \\ \alpha^6 &= \alpha^2 + \alpha \\ \alpha^7 &= 1 \end{aligned}}$$

   (ii)

$$\left(\begin{array}{cc|c} \alpha^2 & \alpha^5 & \alpha^3 \\ \alpha^4 & \alpha^6 & 1 \end{array}\right) \xrightarrow[R2 = \alpha^3 R2]{R1 = \alpha^{-2} R1} \left(\begin{array}{cc|c} 1 & \alpha^3 & \alpha \\ 1 & \alpha^2 & \alpha^3 \end{array}\right) \xrightarrow{R2 = R2 - R1} \left(\begin{array}{cc|c} 1 & \alpha^3 & \alpha \\ 0 & \alpha^2 + \alpha^3 & \alpha^3 + \alpha \end{array}\right) = \left(\begin{array}{cc|c} 1 & \alpha^3 & \alpha \\ 0 & 1 & \alpha^4 \end{array}\right)$$
$$\xrightarrow{R1 = R1 - \alpha^3 R2} \left(\begin{array}{cc|c} 1 & 0 & \alpha + 1 \\ 0 & 1 & \alpha^4 \end{array}\right)$$

   so $x = \alpha + 1 = \alpha^5$ and $y = \alpha^4 = \alpha^2 + \alpha + 1$.

   (iii) $\{\alpha^3, \alpha^6, \alpha^{12} = \alpha^5, \alpha^{10} = \alpha^3, \ldots\} = \{\alpha^3, \alpha^5, \alpha^6\}$, so the minimal polynomial of α^3 is

$$\begin{aligned} (x - \alpha^3)(x - \alpha^5)(x - \alpha^6) &= x^3 - (\alpha^3 + \alpha^5 + \alpha^6)x^2 + (\alpha^3\alpha^5 + \alpha^3\alpha^6 + \alpha^5\alpha^6)x - \alpha^3\alpha^5\alpha^6 \\ &= x^3 + (\alpha^2 + 1 + \alpha + 1 + \alpha^2 + \alpha)x^2 + (\alpha + \alpha^2 + \alpha^2 + \alpha + 1)x + 1 \\ &= x^3 + x + 1\,. \end{aligned}$$