4F5 Advanced Information Theory and Coding 2024 Crib

1) (a) We use the fact that $R_{33}(100) = 1$,

$$\begin{aligned} R_{33}(458923\alpha\beta37257834) &= R_{33}\left(R_{33}(34) + R_{33}(78 \times 100) + R_{33}(25 \times 100^2) + R_{33}(37 \times 100^3)\right. \\ &\quad \left. + R_{33}(\alpha\beta \times 100^4) + R_{33}(23 \times 100^5) + R_{33}(89 \times 100^6) + R_{33}(45 \times 100^7)\right) \\ &= R_{33}\left(1 + 12 + 25 + 4 + 23 + 23 + 12 + R_{33}(\alpha\beta)\right) \\ &= R_{33}\left(R_{33}(\alpha\beta) + 1\right) = 25 \end{aligned}$$

The only possible solution is $\alpha = 2$ and $\beta = 4$, since other values for which $R_{33}(\alpha\beta) = 24$ would require $\alpha > 3$.

(b) We operate the extended Euclidean algorithm to find numbers a and b satisfying the gcd theorem,

n_1	n_2	d	(a_1, b_1)	(a_2, b_2)
1357	4080	3	(1,0)	(0,1)
1357	9	150	(1,0)	(-3,1)
7	9	1	(451,-150)	(-3,1)
7	2	3	(451,-150)	(-454, 151)
1	2		(1813,-603)	

which shows that $1813 \times 1357 - 603 \times 4080 = 1$, hence $R_{4080}(1813 \times 1357) = 1$ and hence the inverse of 1357 in Z_{4080} is 1813.

(c) 531 is divisible by 3 which is not invertible in $\mathcal{Z}_{15}$ and hence, since it residual is not invertible it is not invertible in $\mathcal{Z}_{4080}$. Similarly, 532 is divisible by 2 and hence not invertible in $\mathcal{Z}_{16}$, 235 is divisible by 5 and hence not invertible in $\mathcal{Z}_{15}$.

The only number that has an inverse is 253. Its residuals with respect to 15,16,17 gives its CRT notation $(13, 13, 15)$. We obtain the inverse residuals by inspection $(7, 5, 8)$, verifying that $R_{15}(7 \times 13) = 1, R_{16}(5 \times 13) = 1$ and $R_{17}(8 \times 15) = 1$. If we wanted, we could compute the inverse of 253 in $\mathcal{Z}_{4080}$ to be 2677 and verify that its residuals are indeed 7, 5 and 8, but this was not required in the question.

(d) The multiplicative group of GF(128) has order 127 which is a prime number. Since Lagrange's theorem shows that the order of every element must divide the order of the group and 127 has no divisor other than 1 and itself, the multiplicative order of $1 + X^2$ is 127. As for the additive order, $1 + X^2 + 1 + X^2 = 0$ so the order is 2, as is the case for every element of a binary extension field because $1 + 1 = 0$ in GF(2).

(e) Any element of any binary extension field GF(2^e) except 0 has additive order 2 while its multiplicative order must divide the order $2^e - 1$ of the group which is an odd number and hence the order can never be 2.

For extension fields of other prime numbers GF(p^e) on the other hand, the additive group has order p^e which is an odd number so there can never be an element of additive order 2, while $p-1 ='' -1''$ always has multiplicative order 2, simply because $R_p((p-1)^2) = R_p(p^2-2p+1) = 1$. Hence: 4 has multiplicative order 2 in GF(5) but there is no element of additive order 2 as shown above, 30 has multiplicative order 2 in GF(31) but there is no element of additive order 2, 1 has additive order 2 in GF(128) but there is no element of multiplicative order 2, and finally 126 has multiplicative order 2 in GF(127^{25}) but there is no element of additive order 2.

(f) i. We first need to compute Bob's secret key, the inverse of his public key 55 in $\mathbb{Z}_{\varphi(323)} = \mathbb{Z}_{(17-1)(19-1)} = \mathbb{Z}_{288}$. We run an extended Euclidean algorithm

n_1	n_2	d	(a_1, b_1)	(a_2, b_2)
288	55	5	(1,0)	(0,1)
13	55	4	(1, -5)	(0,1)
13	3	4	(1,-5)	(-4,21)
1			(17,-89)	

hence $17 \times 288 - 89 \times 55 = 1$ and so $55^{-1} = 288 - 89 = 199$ in $\mathbb{Z}_{288}$ so Bob's secret key is 199, which is 1100111 in binary. We precompute the binary powers of the received encrypted message $y = 206$ in $\mathbb{Z}_{323}$ to obtain $y^2 = 123, y^4 = 271, y^8 = 120, y^{16} = 188, y^{32} = 137, y^{64} = 35$ and $y^{128} = 256$ and conclude from the binary expansion that the secret message is

$$x = R_{323}(206 \times 123 \times 271 \times 35 \times 256) = 111$$

ii. For this question, we don't actually need to decrypt the message. We Eve and Alice's public keys to their signatures to verify that they give the encrypted message:

- For Eve, we need to compute $R_{319}(284^{33})$. For this, we pre-compute the binary powers of s_E in $\mathbb{Z}_{319}$: $s_E^1 = 284, s_E^2 = 268, s_E^4 = 49, s_E^8 = 168, s_E^{16} = 152$ and $s_E^{32} = 136$ and compute that $s_E^{33} = s_E^1 \times s_E^{32} = 284 \times 136 = 25$, which verifies Eve's signature.
- For Alice, we pre-compute in $\mathbb{Z}_{299}$: $s_A^1 = 64.s_A^2 = 209, s_A^4 = 27, s_A^8 = 131, s_A^{16} = 118$ and $s_A^{32} = 170$ and compute $s_A^{35} = s_A^1 \times s_A^2 \times s_A^{32} = 64 \times 209 \times 170 = 25$, whic hverifies Alice's signature.

iii. These signatures do not prove their friendship to Bob because one of them could just have intercepted the other's encrypted message and signed it. If they signed the secret message instead of the encrypted message, that would prove that they both knew the original secret text, but then anyone intercepting the signature could decrypt the message and the message would no longer be secret.

A solution might be for Eve and Alice to apply their secret key to the signed encrypted message of the other. Bob could then verify that Alice has signed Eve's signature and Eve has signed Alice's signature, indicating that they clearly both agreed on the principle of sending a secret message jointly. The only remaining danger is that one of them might have encrypted a slightly modified message and had both of them sign it, and the other didn't bother to verify that the correct message has been encrypted (as she could do by encrypting their joint message herself using Bob's public key and verifying that it maps to the encrypted message they are signing.)

Another approach which fixes this is that both of them first sign the original message using their resepective secret keys, then encrypt the result using Bob's public key. This way, Bob would obtain two distinct encrypted signatures which he could decrypt using his secret key, then recover the original text in two different ways by applying the public key of Eve and Alice to their respective signatures, thereby proving, if the two messages are identical, that this is the message they had both agreed on and each signed independently. The message remains secret because only Bob is able to recover the two signatures using his secret key.

2) (a) The possible code lengths are all the lengths that divide $41-1=40$, i.e., 2, 4, 5, 8, 10, 20 and 40.

(b)

$$\boldsymbol{F} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 10 & 18 & 16 & 37 \\ 1 & 18 & 37 & 10 & 16 \\ 1 & 16 & 10 & 37 & 18 \\ 1 & 37 & 16 & 18 & 10 \end{bmatrix}$$

(c) The code rate is $R=3/5=0.6$ and we obtain the parity-check matrix by taking the first two rows of the DFT matrix,

$$\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 10 & 18 & 16 & 37 \end{bmatrix}$$

(d) We need to compute the inverse DFT matrix

$$\boldsymbol{F}^{-1} = \frac{1}{5}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 37 & 16 & 18 & 10 \\ 1 & 16 & 10 & 37 & 18 \\ 1 & 18 & 37 & 10 & 16 \\ 1 & 10 & 18 & 16 & 37 \end{bmatrix} = \begin{bmatrix} 33 & 33 & 33 & 33 & 33 \\ 33 & 32 & 36 & 20 & 2 \\ 33 & 36 & 2 & 32 & 20 \\ 33 & 20 & 32 & 2 & 36 \\ 33 & 2 & 20 & 36 & 32 \end{bmatrix}$$

The encoder matrix consists of the last 3 rows of the inverse DFT matrix,

$$\boldsymbol{G} = \begin{bmatrix} 33 & 36 & 2 & 32 & 20 \\ 33 & 20 & 32 & 2 & 36 \\ 33 & 2 & 20 & 36 & 32 \end{bmatrix}$$

(e) We take the DFT of the received word

$$[12,0,30,5,0]\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 10 & 18 & 16 & 37 \\ 1 & 18 & 37 & 10 & 16 \\ 1 & 16 & 10 & 37 & 18 \\ 1 & 37 & 16 & 18 & 10 \end{bmatrix} = [6,17,24,5,8]$$

Since the first two components of the result are non-zero, there was clearly a transmission error as these would have been zero for a codeword. We now construct the recurrence relation $E_{k+1}=\beta E_k$ that maps 17 to 6, where $\beta = 17 \times 6^{-1} = R_{41} 17 \times 7 = 37$, which allows us to reconstruct the complete error sequence in the frequency domain $\boldsymbol{E}=[6,17,14,26,19]$. We obtain the transmitted codeword as $\boldsymbol{R}-\boldsymbol{E}=[0,0,10,20,30]$ and hence recover the information sequence $[10,20,30]$.

(f) We note the positions 0 and 4 of the erasures and replace them (probably wrongly) by zeros, then take the DFT as previously to yield

$$[0,8,16,8,0]\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 10 & 18 & 16 & 37 \\ 1 & 18 & 37 & 10 & 16 \\ 1 & 16 & 10 & 37 & 18 \\ 1 & 37 & 16 & 18 & 10 \end{bmatrix} = [32,4,37,10,40]$$

The first two symbols are non-zero, indicating that the erasures must indeed have not been two zeros. We now obtain the recurrence relation in the D domain from the position of the erasures as

$$p(D) = (1 - \alpha^0 D)(1 - \alpha^4 D) = (1 - D)(1 - 37D) = 1 - 38D - 4D^2$$

and hence $E_k = 38E_{k-1} + 4E_{k-2}$, giving the complete error vector $\boldsymbol{E} = [32, 4, 34, 37, 25]$. We recover the transmitted codeword in the frequency domain as $\boldsymbol{R} - \boldsymbol{E} = [0, 0, 3, 14, 15]$ and hence the information sequence $[3, 14, 15]$.

(g) Since the parity-check matrix has only 2 rows, it is much easier to manipulate the parity-check matrix to put it into systematic form to obtain the systematic encoder matrix, rather than manipulate the encoder matrix directly. We put the parity-check matrix in systematic form by row manipulations

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 10 & 18 & 16 & 37 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 26 & 35 & 2 & 0 & 21 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 11 & 29 & 4 & 0 & 1 \end{bmatrix}$$

and finally

$$\boldsymbol{H}_{\text{sys}} = \begin{bmatrix} 31 & 13 & 38 & 1 & 0 \\ 11 & 29 & 4 & 0 & 1 \end{bmatrix}$$

and we obtain the systematic encoder matrix as by mapping $\boldsymbol{H}_{\text{sys}} = [-P^T; I]$ to $\boldsymbol{G}_{\text{sys}} = [I; P]$ as per the information data book

$$\boldsymbol{G}_{\text{sys}} = \begin{bmatrix} 1 & 0 & 0 & 10 & 30 \\ 0 & 1 & 0 & 28 & 12 \\ 0 & 0 & 1 & 3 & 37 \end{bmatrix}$$

3) (a) i. The channel transition probability matrix is given by

$$W = \begin{bmatrix} 1-(K-1)\delta & \delta & \delta & \dots & \delta \\ \delta & 1-(K-1)\delta & \delta & \dots & \delta \\ \vdots & \ddots & & & \\ \delta & \delta & \dots & \delta & 1-(K-1)\delta \end{bmatrix}$$

ii. The optimal decoder in terms of error probability is the maximum likelihood (ML) decoder given by

$$\hat{m} = \arg\max_{m=1,\dots,M} \prod_{i=1}^{n} W(y_i|x_{m,i})$$

iii. If $\delta < \frac{1}{K}$, then the diagonal term $1 - (K-1)\delta > \delta$.

$$\begin{aligned} \hat{m} &= \arg\max_m \prod_{i=1}^{n} W(y_i|x_{m,i}) && (1) \\ &= \arg\max_m (1-(K-1)\delta)^{n-d(\boldsymbol{x}_m,y^n)} \delta^{d(\boldsymbol{x}_m,y^n)} && (2) \\ &= \arg\max_m -d(\boldsymbol{x}_m, y^n) \log \frac{1-(K-1)\delta}{\delta} && (3) \\ &= \arg\min_m d(\boldsymbol{x}_m, y^n) && (4) \end{aligned}$$

where $d(\boldsymbol{x}_m, y^n)$ is the Hamming distance between y^n and codeword $\boldsymbol{x}_m$, and the last step follows since $1 - (K-1)\delta > \delta$.

iv. The function $E_0(\rho)$ implicitly defines the error exponent of the error probability $E_r(R) = \max_{\rho\in[0,1]} E_0(\rho) - \rho R$. Since $E_0'(0) = I(X;Y)$, the function $E_0(\rho)$ fundamentally characterizes the limits of data transmission.

$$E_0(\rho) = -\log \sum_y \Bigg(\sum_x P_X(x) P_{Y|X}(y|x)^{\frac{1}{1+\rho}} \Bigg)^{1+\rho} \tag{5}$$

$$= \log K^\rho - \log \Bigg((1-(K-1)\delta)^{\frac{1}{1+\rho}} (K-1)\delta^{\frac{1}{1+\rho}} \Bigg)^{1+\rho} \tag{6}$$

v. The mutual information is found as $E_0'(0) = I(X;Y) = \sum_{x,y} P_X(x) W(y|x) \log \frac{W(y|x)}{P_Y(y)}$.

vi. For $\delta = \frac{1}{K}$ the capacity is zero.

(b) i. If $\gamma < \frac{1}{K}$, the decoder operates as before

$$\hat{m} = \arg\max_m (1-(K-1)\gamma)^{n-d(\boldsymbol{x}_m,y^n)} \gamma^{d(\boldsymbol{x}_m,y^n)} \tag{7}$$

$$= \arg\max_m -d(\boldsymbol{x}_m, y^n) \log \frac{1-(K-1)\gamma}{\gamma} \tag{8}$$

$$= \arg\min_m d(\boldsymbol{x}_m, y^n) \tag{9}$$

ii. Since the decoder operates exactly in the same way as the ML decoder, the corresponding achievable rate will be the same, the mutual information $I(X;Y)$.

4) (a) i. In the Neyman-Pearson setting we do not know the priors for the hypotheses. Thus, we design tests characterized by a distribution $T(h|y^n), h = 1,2$ according to the optimality criterion given by a tradeoff between the two pairwise error probabilities $\epsilon_1(P_1, T) = \sum_{y^n} P_1^n(y^n) T(2|y^n), \epsilon_2(P_2, T) = \sum_{y^n} P_2^n(y^n) T(1|y^n)$ expressed as

$$\alpha_\beta(P_1, P_2) = \min_{T:\epsilon_2(P_2,T)\leq\beta} \epsilon_1(P_1, T)$$

where the minimization is over all tests such that $\epsilon_2(P_2, T) \leq \beta$.

ii. The optimal test is the likelihood ratio test expressed as a conditional probability distribution

$$T(1|y^n) = \begin{cases} 1 & \frac{P_1^n(y^n)}{P_2^n(y^n)} > \gamma \\ p_0 & \frac{P_1^n(y^n)}{P_2^n(y^n)} = \gamma \\ 0 & \frac{P_1^n(y^n)}{P_2^n(y^n)} < \gamma \end{cases}$$

where γ, p_0 are chosen so as to have $T : \epsilon_2(P_2, T) = \beta$.

iii. We have that

$$\log \frac{P_1^n(y^n)}{P_2^n(y^n)} = \sum_{i=1}^n \log \frac{P_1(y_i)}{P_2(y_i)} \tag{10}$$

$$= n \sum_{i=1}^n \sum_{a\in\mathcal{Y}} \frac{\mathbb{1}\{y_i = a\}}{n} \log \frac{P_1(a)}{P_2(a)} \tag{11}$$

$$= n \sum_{a\in\mathcal{Y}} \hat{P}_{y^n}(a) \log \frac{P_1(a)}{P_2(a)} \tag{12}$$

$$= nD(\hat{P}_{y^n} \| P_2) - nD(\hat{P}_{y^n} \| P_1) \tag{13}$$

The test estimates the empirical distribution of the observation and checking (by means of relative entropy) whether it is closer to either of the testing distributions P_1, P_2. The test is expressed as

$$T(1|y^n) = \begin{cases} 1 & D(\hat{P}_{y^n}\|P_2) - D(\hat{P}_{y^n}\|P_1) > \frac{1}{n}\log\gamma \\ p_0 & D(\hat{P}_{y^n}\|P_2) - D(\hat{P}_{y^n}\|P_1) = \frac{1}{n}\log\gamma \\ 0 & D(\hat{P}_{y^n}\|P_2) - D(\hat{P}_{y^n}\|P_1) < \frac{1}{n}\log\gamma. \end{cases}$$

iv. We have that as $n \to \infty$

$$\frac{1}{n}\log\frac{P_1^n(y^n)}{P_2^n(y^n)} = \sum_{i=1}^n \log\frac{P_1(y_i)}{P_2(y_i)} \tag{14}$$

$$\to \mathbb{E}_Q\Big[\log\frac{P_1(y_i)}{P_2(y_i)}\Big] \tag{15}$$

$$= D(Q\|P_2) - D(Q\|P_1) \tag{16}$$

Thus, the test decides for hypothesis 1 whenever $D(Q\|P_2) > D(Q\|P_1)$ (Q closer to P_1) since $\frac{1}{n}\log\gamma \to 0$.

(b) i. The error probability is given by

$$p_e = \sum_{v^n \notin \mathcal{A}} P_{V^n}(v^n)$$

ii. Since the source sequences in $\mathcal{A}$ are the M that have the highest probability, if we move a sequence from $\mathcal{A}$ to $\mathcal{A}^c$ (where $\mathcal{A}^c$ denotes the complement) and replace it by a sequence from $\mathcal{A}^c$, the error probability will be higher from the previous equation.

iii. Write for $r > 0$

$$p_c^r = \Big(\sum_{v^n\in\mathcal{A}} P_{V^n}(v^n)\Big)^r \tag{17}$$

$$= \Big(M\sum_{v^n\in\mathcal{A}} \frac{1}{M}P_{V^n}(v^n)\Big)^r \tag{18}$$

$$\leq M^r \sum_{v^n\in\mathcal{A}} \frac{1}{M}P_{V^n}(v^n)^r \tag{19}$$

where the last step follows from Jensen's inequality and since $|\mathcal{A}| = M$ (the sum in (18) can be understood as an expectation).

iv. If we set $r = \frac{1}{1+\rho}$ we get that, for $-1 < \rho < 0$

$$p_c \leq M^{-\rho}\Big(\sum_{v^n\in\mathcal{V}^n} P_{V^n}(v^n)^{\frac{1}{1+\rho}}\Big)^{1+\rho}.$$

v. Thus,

$$p_e \geq 1 - M^{-\rho}\Big(\sum_{v^n\in\mathcal{V}^n} P_{V^n}(v^n)^{\frac{1}{1+\rho}}\Big)^{1+\rho} \tag{20}$$

$$= 1 - e^{-n(\rho R - E_s(\rho))} \tag{21}$$

where the last line follows since the source is memoryless and $\Big(\sum_{v^n\in\mathcal{V}^n} P_{V^n}(v^n)^{\frac{1}{1+\rho}}\Big)^{1+\rho} = \Big(\sum_{v\in\mathcal{V}} P_V(v)^{\frac{1}{1+\rho}}\Big)^{n(1+\rho)}$.