Crib of 4F5 exam 2019

JS

May 24, 2019

1. (a) The least significant digits are obtained by taking the remainder of 2^{100} when divided by 100, hence

$$\begin{aligned} R_{100}(2^{100}) &= R_{100}\left(R_{100}(2^{10})^{10}\right) = R_{100}\left(R_{100}(1024)^{10}\right) \\ &= R_{100}(24^{10}) = R_{100}\left(R_{100}(24^2)^5\right) = R_{100}\left(R_{100}(576)^5\right) \\ &= R_{100}(76^5) = R_{100}\left(R_{100}(76^2)R_{100}(76^3)\right) = R_{100}\left(R_{100}(5776)R_{100}(76^3)\right) \\ &= R_{100}(76^4) = 76 \end{aligned}$$ [10%]

(b) $\varphi(56) = \varphi(2^3 \cdot 7) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{7}\right) 56 = 6 \cdot 4 = 24$ [10%]

(c) (i) Since x and y are co-prime, we know by definition that $\gcd(x, y) = 1$, and by the greatest common divisor theorem, there exist integers a' and b' such that $a'x + b'y = \gcd(x, y) = 1$. For any n,

$$n = n \gcd(x, y) = n(a'x + b'y) = (na')x + (nb')y$$

which proves the result since we can set $a = na'$ and $b = nb'$. [10%]

(ii) if there existed integers a and b such that $6a + 9b = 11$, we could divide the equation by 3 to yield

$$2a + 3b = 11/3$$

where the expression on the left is an integer and the expression on the right is a fractional number and hence equality cannot hold if a and b are integers. [10%]

(d) We have $105 = 3 \cdot 5 \cdot 7$ and hence we can use the Chinese Remainder Theorem for inversions of integers $x \in \mathbb{Z}^\star_{105}$ with residues $[R_3(x), R_5(x), R_7(x)]$.

(i) 3 has no multiplicative inverse because $R_3(3) = 0$ and 0 has no multiplicative inverse in $\mathbb{Z}_3$, and we would need to compute such an inverse in order to invert 3 using the Chinese Remainder Theorem. [10%]

(ii) The residues of 44 are $[R_3(44), R_5(44), R_7(44)] = [2, 4, 2]$. Hence, the residues of the inverse of 44 are the inverses of 2, 4 and 2 in $\mathbb{Z}_3, \mathbb{Z}_5$ and $\mathbb{Z}_7$, respectively, i.e., $[2, 4, 4]$. To compute the number from its residues, we need to compute b_j and u_j following the example in the lecture notes, i.e.,

$$\begin{cases} (u_1, u_2, u_3) &= (105/3, 105/5, 105/7) = (35, 21, 15) \text{ and} \\ (b_1, b_2, b_3) &= \left(R_3(35)^{-1}\big|_{\mathbb{Z}_3}, R_5(21)^{-1}\big|_{\mathbb{Z}_5}, R_7(15)^{-1}\big|_{\mathbb{Z}_7} \right) = (2, 1, 1) \end{cases}$$

and hence $44^{-1} = R_{105}(2 \cdot 2 \cdot 35 + 4 \cdot 1 \cdot 21 + 4 \cdot 1 \cdot 15) = 74$ [10%]

(iii) That's Euler's function of 105, i.e., $\varphi(105) = (3-1)(5-1)(7-1) = 48$ [10%]

(e) (i) The multiplicative group has order $128 - 1 = 127$, which is a prime number. Hence every element int he multiplicative group must have the same order and the multiplicative order of $1 + X$ is 127. [10%]

(ii) .

$$\begin{aligned}
X^7 &= 1 + X^3 \\
X^{14} &= (1 + X^3)^2 = 1 + X^6 \\
X^{15} &= X(1 + X^6) = 1 + X + X^3 \\
X^{30} &= (1 + X + X^3)^2 = 1 + X^2 + X^6 \\
X^{31} &= X(1 + X^2 + X^6) = 1 + X \\
X^{62} &= (1 + X)^2 = 1 + X^2 \\
(1 + X)^{-1} &= X^{-31} = X^{127-31} = X^{96} \\
&= X^{62+31+3} = (1 + X^2)(1 + X)X^3 \\
&= X^3(1 + X + X^2 + X^3) = X^3 + X^4 + X^5 + X^6
\end{aligned}$$

We verify $(1 + X)(X^3 + X^4 + X^5 + X^6) = X^3 + X^7 = 1$. [10%]

(iii) The equivalent linear code has a parity check matrix of $5 \cdot 7 = 35$ rows and $11 \cdot 7 = 77$ columns and hence has length $N = 77$ and dimension $K = 77 - 35 = 42$. [10%]

2. (a) Any number $n > 1$ that divides $101 - 1 = 100$ is a possible code length, i.e., 2, 5, 10, 20, 25, 50, 100. [10%]

(b) Since $\beta = 4 = \alpha^2$ and we've been told that $\alpha = 2$ generates the group, i.e., has maximum order 100, β must have order 50 (because $\beta^{50} = (\alpha^2)^{50} = \alpha^{100}$) ahd hence the code length is $N = 50$. [10%]

(c) .

$$\mathbf{F} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 10 & 100 & 91 \\ 1 & 100 & 1 & 100 \\ 1 & 91 & 100 & 10 \end{bmatrix}$$

$$\mathbf{F}^{-1} = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 91 & 100 & 10 \\ 1 & 100 & 1 & 100 \\ 1 & 10 & 100 & 91 \end{bmatrix} = \begin{bmatrix} 76 & 76 & 76 & 76 \\ 76 & 48 & 25 & 53 \\ 76 & 25 & 76 & 25 \\ 76 & 53 & 25 & 48 \end{bmatrix}$$

where we have used the hint that $1/N = 1/4 = 76$ in GF(101). [15%]

(d) The parity-check matrix consists of the first $N - K$ rows of the inverse DFT matrix. In this case, $N = 4$ and since we're told that $R = 1/2$, we have $K = RN = 2$ and hence $N - K = 2$, hence $\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 10 & 100 & 91 \end{bmatrix}$ [5%]

(e) The code has $q^K = 101^2 = 10201$ codewords. [10%]

(f) The RS code can detect up to $d_{\min} - 1 = N - K = 2$ errors. [5%]

(g) The RS code can correct up to 1 error. [5%]

(h) The encoding operation multiplies a vector of 2 zeros followed by 2 information digit by the inverse DFT matrix, hence it is equivalent to multiplying the information vector by the last two rows of the inverse DFT matrix, and hence the encoder matrix is

$$\mathbf{G} = \begin{bmatrix} 76 & 25 & 76 & 25 \\ 76 & 53 & 25 & 48 \end{bmatrix} \qquad [10\%]$$

(i) We take the DFT of the received vector

$$\mathbf{R} = [91, 10, 73, 30] \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 10 & 100 & 91 \\ 1 & 100 & 1 & 100 \\ 1 & 91 & 100 & 10 \end{bmatrix} = [2, 20, 23, 16]$$

and recognise, since the first two frequency components of the codeword were zero, that there must have been a transmission error and the error sequence in the frequency domain can be reconstructed by a recurrence relation of order 1, i.e., $E_n = cE_{n-1}$. Since $E_2/E_1 = 20/2 = 10$, clearly $c = 10$ and hence the full error sequence is $\mathbf{E} = [2, 20, 99, 81]$. The information symbols can be recovered by subtracting the errors in the frequency domain:

$$\begin{cases} u_1 = C_3 = R_3 - E_3 = 23 - 99 = 23 + 2 = 25 \\ u_2 = C_4 = R_4 - E_4 = 16 - 81 = 16 + 20 = 36 \end{cases}$$

so the information sequence is $\mathbf{u} = [25, 36]$. [20%]

(j) The probability of successful decoding is the probability that the received sequence will contain no errors or one error, i.e., $P_s = (1-p)^4 + 4p(1-p)^3 = 0.9477$ [10%]

3. (a) (i) The public key is $(m, e) = (187, 13)$ and hence the message $X = 22$ is encrypted as

$$Y = R_m(X^e) = R_{187}(22^{13}) = R_{187}(22 \times 22^4 \times 22^8) = R_{187}(22 \times 132 \times 33) = 88.$$

[15%]

(ii) We note from the hint that $d = 37$ is the multiplicative inverse of 13 in $\mathbb{Z}_{\phi(m)} = \mathbb{Z}_{6\times16} = \mathbb{Z}_{96}$. Hence, the plaintext can be recovered from the ciphertext as

$$X = R_m(Y^d) = R_{187}(88^{37}) = R_{143}(88 \times 88^4 \times 88^{32}) = R_{143}(88 \times 132 \times 154) = 22.$$

[15%]

(b) (i)

$$A = 2^{16} = 88$$

Calculating the secret key $a = 16$ from the public key $A = 88$ would require one to take a discrete logarithm to the base 2 for which no efficient algorithms currently exist. [10%]

(ii)

$$K = 11^{16} = 2^{ab} = 2^{16b} = 54.$$

Bob doesn't know $a = 16$ but knows b and $A = 2^a$, hence he can calculate $A^b = 2^{ab}$ to obtain the same result. [10%]

(c) (i) Expanding, we have,

$$\begin{aligned}\frac{1}{n}\log\frac{P_1^n(X_1^n)}{P_2^n(X_1^n)} &= \frac{1}{n}\log\left(\frac{\prod_{i=1}^n P_1(X_i)}{\prod_{i=1}^n P_2(X_i)}\right)\\ &= \frac{1}{n}\log\left(\prod_{i=1}^n \frac{P_1(X_i)}{P_2(X_i)}\right)\\ &= \frac{1}{n}\sum_{i=1}^n \log\left(\frac{P_1(X_i)}{P_2(X_i)}\right),\end{aligned}$$

which is the empirical average of the IID RVs $Z_i = \log\frac{P_1(X_i)}{P_2(X_i)}$. Therefore, by the WLLN, as $n\to\infty$ the above expression converges in probability to,

$$E(Z_1) = E\left(\log\frac{P_1(X_1)}{P_2(X_1)}\right),$$

where $X_1 \sim Q$. So the limit is:

$$\begin{aligned}\sum_x Q(x)\log\frac{P_1(x)}{P_2(x)} &= \sum_x Q(x)\log\left(\frac{P_1(x)}{P_2(x)}\frac{Q(x)}{Q(x)}\right)\\ &= \sum_x Q(x)\log\left(\frac{P_1(x)}{Q(x)}\right) + \sum_x Q(x)\log\left(\frac{Q(x)}{P_2(x)}\right)\\ &= D(Q\|P_2) - D(Q\|P_1).\end{aligned}$$

[25%]

(ii) If $R = D(Q\|P_2) - D(Q\|P_1) > 0$, then the likelihood ratio $P_1^n(X_1^n)/P_2^n(X_1^n)$ will increase to infinity exponentially fast, so the test will declare P_1 to be the true distribution.
If, on the other hand, $R = D(Q\|P_2) - D(Q\|P_1) < 0$, then the likelihood ratio $P_1^n(X_1^n)/P_2^n(X_1^n)$ will decrease to zero exponentially fast, and the test will declare P_2 to be the true distribution.
[With a little more work, the borderline case when $R = D(Q\|P_2) - D(Q\|P_1)$ is exactly zero can be similarly analysed by employing the central limit theorem instead of the WLLN.] [25%]

4. (a) The log-likelihood of x_1^n is,

$$\log_e P_\theta^n(x_1^n) = \log_e\left(\prod_{i=1}^n \theta(1-\theta)^{x_i-1}\right) = n\log_e\theta + [\log_e(1-\theta)]\sum_{i=1}^n (x_i-1),$$

and its derivative with respect to θ is,

$$\frac{\partial}{\partial\theta}\big(\log_e P_\theta^n(x_1^n)\big) = \frac{n}{\theta} - \frac{1}{1-\theta}\sum_{i=1}^n (x_i-1) = \frac{n}{\theta} - \frac{n(\bar{x}_n-1)}{1-\theta},$$

where $\bar{x}_n$ denotes the empirical mean $\frac{1}{n}\sum_{i=1}^n x_i$. Setting this equal to zero and solving for θ gives:

$$\hat{\theta}_{\mathrm{MLE}}(x_1^n) = \frac{1}{\bar{x}_n} = \left[\frac{1}{n}\sum_{i=1}^n x_i\right]^{-1}.$$

[20%]

(b) Let $\bar{X}_n$ denote the empirical mean of the random X_1^n, so that:

$$E_\theta(\bar{X}_n) = E_\theta\left[\frac{1}{n}\sum_{i=1}^n X_i\right] = \frac{1}{n}\sum_{i=1}^n E_\theta(X_i) = \frac{1}{\theta}.$$

The function $f(x) = 1/x$ is strictly convex for $x > 0$. Therefore, Jensen's inequality implies that,

$$E_\theta[\hat{\theta}_{\text{MLE}}(X_1^n)] = E_\theta\Big(\frac{1}{\bar{X}_n}\Big) > \frac{1}{E_\theta(\bar{X}_n)} = \frac{1}{1/\theta} = \theta,$$

where we have strict inequality because $\bar{X}_n$ is not constant. [20%]

(c) We already computed the derivative of the log-likelihood in part (a), which for $n = 1$ becomes,

$$\frac{\partial}{\partial\theta}\big(\log_e P_\theta(x)\big) = \frac{1}{\theta} - \frac{(x-1)}{1-\theta} = -\Big(\frac{x - \frac{1}{\theta}}{1-\theta}\Big).$$

Therefore,

$$J(\theta) = E_\theta\left[\left(\frac{\partial}{\partial\theta}\big(\log_e P_\theta(X)\big)\right)^2\right] = E_\theta\left[\left(\frac{X - \frac{1}{\theta}}{1-\theta}\right)^2\right] = \frac{\text{Var}_\theta(X)}{(1-\theta)^2} = \frac{1}{\theta^2(1-\theta)}.$$

[20%]

(d) First we compute the mean of $\hat{\theta}_{\text{MLE}}$ in the case $n = 1$:

$$E_\theta(\hat{\theta}_{\text{MLE}}) = E_\theta\Big(\frac{1}{X}\Big) = \sum_{k=1}^\infty \theta(1-\theta)^{k-1}\frac{1}{k} = \frac{\theta}{1-\theta}\sum_{k=1}^\infty \frac{(1-\theta)^k}{k} = -\frac{\theta}{1-\theta}\log_e\theta,$$

where we used the series in the hint. Therefore,

$$\text{bias}(\hat{\theta}_{\text{MLE}};\theta) = -\frac{\theta}{1-\theta}\log_e\theta - \theta = -\theta\left[1 + \frac{\log_e\theta}{1-\theta}\right].$$

[20%]

(e) First we compute the derivative of the bias:

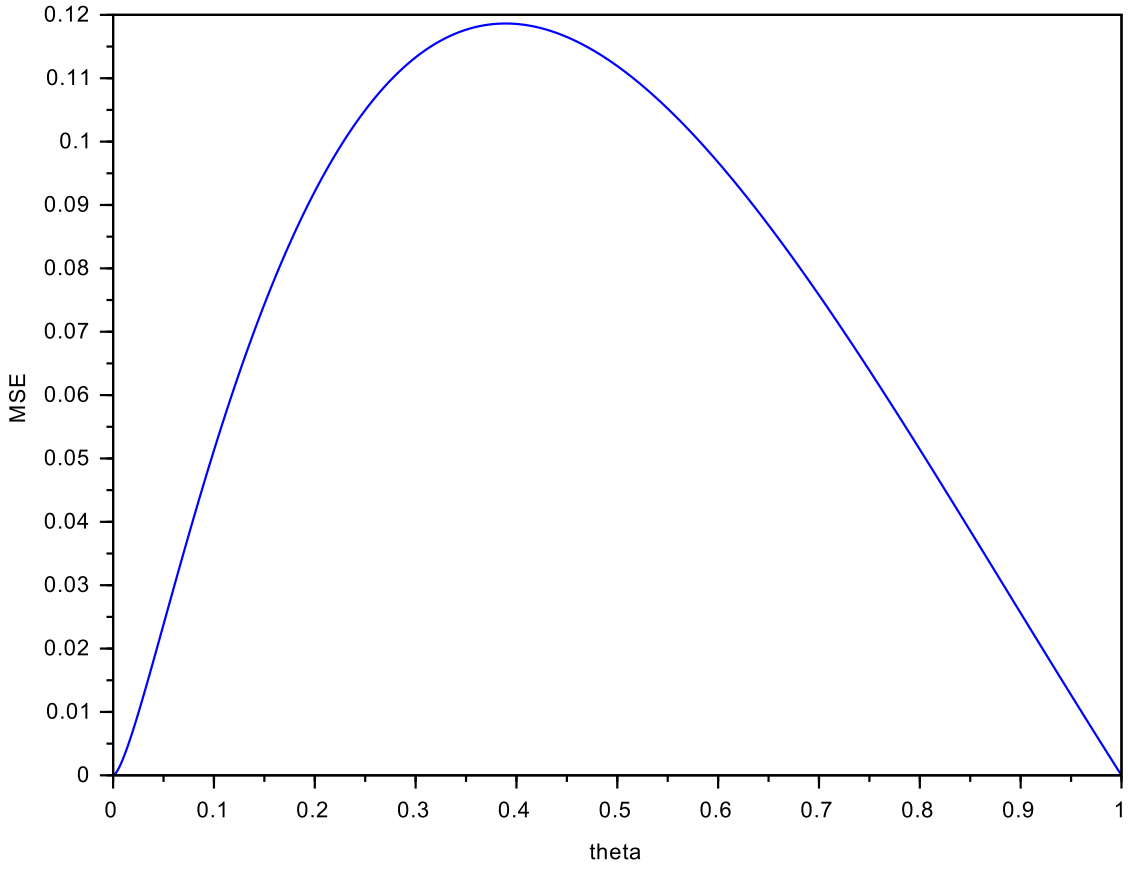
$$\text{bias}'(\hat{\theta}_{\text{MLE}};\theta) = -\frac{1}{1-\theta} - \frac{\log_e\theta}{(1-\theta)^2} - 1.$$

Then Cramér-Rao bound for biased estimators gives:

$$\begin{aligned}
\text{MSE}(\hat{\theta}_{\text{MLE}};\theta) &\geq \frac{[1 + \text{bias}'(\hat{\theta};\theta)]^2}{J(\theta)} + \text{bias}(\hat{\theta};\theta)^2 \\
&= \frac{\theta^2}{1-\theta}\left[1 + \frac{\log_e\theta}{1-\theta}\right]^2 + \theta^2\left[1 + \frac{\log_e\theta}{1-\theta}\right]^2 \\
&= \frac{\theta^2(2-\theta)}{1-\theta}\left[1 + \frac{\log_e\theta}{1-\theta}\right]^2.
\end{aligned}$$

[20%]

The graph below is offered to help revising students visualise the result but was not required as part of the solution to the exam question.



4F5 ASSESSOR'S COMMENTS

Q1 Mathematical Fundamentals

44 attempts, Average mark 13.8/20, Maximum 20, Minimum 4.

This question was generally done well but there were a few surprises. In part c(ii) a simple proof was required but many students' proofs did not stand to scrutiny because they confused "there exists" with "for all". In part d(ii), the majority of students used Euclid's extended GCD algorithm to obtain the correct result, even though we had told the students during the revision class that they were not expected to know this algorithm and the question could be solved with the Chinese Remainder Theorem. In part e(i), many students correctly identified that since the group order 127 was a prime number, every element must have order 127, but some students tediously did 127 multiplication to obtain the same result. Finally, part e(iii) was supposed to be the easiest question but only a few students got it right and understood what a "equivalent binary code" means, showing that more emphasis needs to be put on this in future lectures.

Q2 Reed Solomon Coding

44 attempts, Average mark 16.4/20, Maximum 20, Minimum 4.

This was predictably a popular question that students generally did very well, having access to several past exams and a very extensive examples paper to prepare for this question. This is by no means an easy question and I doubt that many who have not taken this course would be able to solve it, so it is very pleasing to see so many of our students being able to demonstrate such a detailed and in-depth understanding of Reed Solomon coding and decoding. Part (b) could be done easily by realising that $4=2^2$ and hence, since we were told that $\alpha=2$ generates the field and must hence have the field order 100, the answer must be $100/2=-50$, but many students tediously multiplied 4 by itself 50 times to determine the order.

Q3 Cryptography / Hypothesis testing

46 attempts, Average mark 14.9/20, Maximum 20, Minimum 0.

This was a mixed question with (a),(b) covering the cryptography part of the course, and (c) covering hypothesis testing, which was lectured by different lecturers and marked by the two lecturers. The cryptography part was done very well and a vast proportion of the students who did this question got 10/10 points on the cryptography part. The hypothesis testing part was harder but many students did very well too.

Formal correction: There was a typo in part a(ii) where it said "gcd(160,11) = 1 = 37 x 13 – 3 x 160" where it should have said "gcd(160,13)" instead. The typo would not had hampered students' ability to solve the exam since all they needed to know was that "37 x 13 – 3 x 160 = 1" and the left-hand side of the equation was redundant, and since 11 is a prime number the equation was not in fact wrong. However, a formal correction was issued because the examiner feared that some students may wonder if there was a trick hidden behind the fact that we wrote "gcd(160,11)" instead of the obvious "gcd(160,13)". Two students pointed out the typo during reading time, specifically asking whether the "11" should have been a "13", and the correction was issued during reading time and communicated to colleges within the first few minutes of the examination.

Q4 Estimation

16 attempts, Average mark 12.75/20, Maximum 19, Minimum 3.

This was predictably the least popular question because this part of the course was new this year and, although we had issued an extensive collection of typical exam questions, students had no past exam questions to prepare for this. We expect that more students will choose to answer this question next year.