Crib of 4F5 exam 2021

April 29, 2022

1. (a) If $\gcd(a,b) = 11$, there exist numbers a' and b' such that $a = 11a'$ and $b = 11b'$, hence $a+b = 11(a'+b') = 1099$ but this is impossible since 1099 is not divisible by 11 hence there exist no such numbers a and b.

   (b) Using the fundamental property and even/odd properties of greatest common divisors, $\gcd(2^{30}+1, 2^{10}+1) = \gcd(2^{30}-2^{10}, 2^{10}+1) = \gcd(2^{20}-1, 2^{10}+1) = \gcd(2^{20}+2^{10}, 2^{10}+1) = \gcd(2^{10}+1, 2^{10}+1) = 2^{10}+1 = 1025$.

   (c) $R_a((a-1)^{2b}) = R_a(R_a((a-1)^2)^b) = R_a(R_a(a^2-2a+1)^b) = R_a(1^b) = 1$ and hence $R_{101}(123,000,000,123) = R_{101}(1230 \times 100^4 + 123) = R_{101}(1230) + R_{101}(123) = 18 + 22 = 40$.

   (d) The residuals of 37 with respect to the pairwise co-prime moduli $(m_1, m_2, m_3) = (3,4,5)$ are $(r_1, r_2, r_3) = (1,1,2)$. Hence the residuals of 37^{-1} are the inverses of the residuals in $\mathbb{Z}_{m_i}$, that is $(r_1^{-1}, r_2^{-1}, r_3^{-1}) = (1,1,3)$. To find the number in $\mathbb{Z}_m$ for $m = 60$ with the residuals $(1,1,3)$, we first compute $u_i = m/m_i$, i.e., $(u_1, u_2, u_3) = (20, 15, 12)$, then compute numbers b_i such that $R_{m_i}(b_i u_i) = 1$ (no need to do an extended gcd for such small numbers, you can work it out in your head), $(b_1, b_2, b_3) = (2,3,3)$ and finally compute $R_m(\sum_i r_i^{-1} b_i u_i) = R_{60}(1\times 2\times 20 + 1\times 3\times 15 + 3\times 3\times 12) = R_{60}(192) = 22$.

   (e) i. $X^2 = 2, X^3 = 2X, X^4 = 1$ so the multiplicative order of X is 4.

   ii. The additive order of X is 3, as is the case for any non-zero element in GF(9).

   iii. If X generates the group, it must have order 8 and hence since $X^8 = (X^4)^2 = 1$, X^4 must have order 2. Note that this also implies that $X^4 = -1 = 2$.

   iv. Following from the previous question, if α generates GF(121), α must have multiplicative order 120, α^{60} must have order 2, and hence $\alpha^{60} = -1 = 11-1 = 10$.

   (f) By Blahut's theorem, the linear complexity of the sequences $\mathbf{x}$ and $\mathbf{y}$ is equal to the Hamming weight of their Discrete Fourier Transforms (DFTs) $\mathbf{X}$ and $\mathbf{Y}$. By the linearity of the DFT, the DFT of $\mathbf{x}+\mathbf{y}$ is $\mathbf{X}+\mathbf{Y}$. When you add two vectors with Hamming weights w_X and w_Y, you obtain a vector with Hamming weight $w_Z \leq w_X + w_Y$, with equality if and only if all the non-zero elements of $\mathbf{X}$ and the non-zero elements of $\mathbf{Y}$ occur in distinct positions. Hence, we conclude that $\mathcal{L}(\mathbf{z}) \leq \mathcal{L}(\mathbf{x}) + \mathcal{L}(\mathbf{y})$.

2. (a) The multiplicative group has order 30 and hence the possible lengths are divisors of 30, excluding 1 and 2 for which Reed-Solomon codes cannot be defined as they would either have rate 0 or not correct any errors, i.e., 3, 5, 6, 10, 15, 30.

   (b) $\alpha^2 = 4, \alpha^3 = 8, \alpha^4 = 16, \alpha^5 = 1$, hence the length is $N = 5$.

   (c)
$$\mathbf{F} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 4 & 16 & 2 & 8 \\ 1 & 8 & 2 & 16 & 4 \\ 1 & 16 & 8 & 4 & 2 \end{bmatrix}$$

   (d) The parity-check matrix verifies that the first two coefficients of the DFT of a codeword are zero, hence it consists of the first two columns of the DFT matrix, transposed, i.e.,
$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \end{bmatrix}$$

   (e) The encoder matrix consists of the last 3 rows of the inverse DFT matrix, i.e.,
$$\mathbf{G} = \begin{bmatrix} 25 & 14 & 19 & 28 & 7 \\ 25 & 7 & 28 & 19 & 14 \\ 25 & 19 & 7 & 14 & 28 \end{bmatrix}$$

   (f) Examining the first two digits of $\mathbf{R}$, we note that the DFT of the error sequence is generated by the recurrence relation $E_{k+1} = E_k$ and hence the full error sequence in the frequency domain is $\mathbf{E} = [23, 23, 23, 23, 23]$. We subtract the error sequence from the received word in the frequency domain to obtain $\mathbf{R} - \mathbf{E} = [0, 0, 26, 28, 4]$ and cut out the information digits $\mathbf{U} = [26, 28, 4]$.

   (g) This can be worked out either by row manipulations on the encoder or on the parity-check matrix. Since the parity-check matrix has only 2 rows, it's far easier and we opt to do find the systematic parity-check matrix.
$$\begin{aligned} \mathbf{H}' &= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 24 & 25 & 27 & 0 & 8 \end{bmatrix} && \mathbf{h_2} - 8\mathbf{h_1} \\ \mathbf{H}'' &= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & 7 & 15 & 0 & 1 \end{bmatrix} && 4\mathbf{h_2} \\ \mathbf{H}_{\text{sys}} &= \begin{bmatrix} 29 & 25 & 17 & 1 & 0 \\ 3 & 7 & 15 & 0 & 1 \end{bmatrix} && \mathbf{h_1} - \mathbf{h_2} \end{aligned}$$
   and we now use the relation $\mathbf{G} = [\mathbf{I}, \mathbf{P}], \mathbf{H} = [-\mathbf{P}^T, \mathbf{I}]$ to obtain the systematic encoder matrix
$$\mathbf{G}_{\text{sys}} = \begin{bmatrix} 1 & 0 & 0 & 2 & 28 \\ 0 & 1 & 0 & 6 & 24 \\ 0 & 0 & 1 & 14 & 16 \end{bmatrix}$$

(h) This can be worked out by solving a system of two linear equations with two unknowns or using a Reed-Solomon decoder for erasure channels, but we note here that the non-erased received symbols match the last row of the encoder matrix in Question (e), which is a codeword of the Reed-Solomon code, irrespective of which encoder matrix was used. Since there can only be one codeword that matches the received word in 3 positions, $[25, 19, 7, 14, 28]$ was the transmitted codeword and hence the information digits are $[25, 19, 7]$.

3. (a) i. Only Alice can read Bob's message, by computing $R_{m_A}(y^{d_A}) = R_{m_A}(x^{e_A d_A}) = x$. Nobody else can decrypt the message because only Alice knows the inverse d_A of e_A and it can't be computed without knowing Euler's function $\phi(m_A)$ which requires a prime factorisation of m_A. Anyone could have generated this message. Hence Alice has no guarantee that the message originates from Bob. This is an intended use of an RSA PKC, for example when implementing an anonymous feedback system where anyone should be able to write their feedback, only the intended recipient is allowed to read the anonymous feedback, but the intended recipient is not meant to have the ability to determine the author of a message.

ii. Only Bob can decrypt and read Eve's message by computing $R_{m_B}(y^{d_B}) = R_{m_B}(x^{e_B d_B}) = x$. Anyone could have generated this message and Bob should not be fooled by the fact that the message claims to be from Alice. This is a malicious misuse of an RSA PKC and not one that it's intended for.

iii. Anyone can read the message (x, y) and there is no need for decryption since the message x is transmitted in plaintext. However, only Alice could have generated y, as anyone can verify by computing $R_{m_A}(y^{e_A}) = R_{m_A}(x^{d_A e_A}) = x$ and verify that the result is x. Hence, this provides a certificate for the authenticity of the message x and guarantees that Alice is its author. This is an intended use of an RSA PKC. An example application is when the TA publishes its users' public key pairs (m, e): these may be signed with the TA's own secret key to ensure that nobody can tamper with the public keys when they are transmitted to users who requested them.

iv. Only Bob can decrypt and read the message x by computing $R_{m_B}(y_1^{d_B}) = R_{m_B}(x^{e_B d_B}) = x$, and he can verify that the message is from Alice by computing $R_{m_A}(y_2^{e_A}) = R_{m_A}(y_1^{d_A e_A}) = y_1$ and verifying that it is equal to y_1. This is an intended use of an RSA PKC and provides both secrecy and authenticity. Its practical uses are many, for example when transmitting orders for financial transactions to your bank: nobody else should be able to intercept and read your order, and the bank must be sure that the order is from you.

(b) i. We write

$$Q^n(y^n) = \prod_{i=1}^{n} Q(y_i) \tag{1}$$

$$= \prod_{a\in\mathcal{Y}} Q(a)^{n\hat{P}_{y^n}(a)} \tag{2}$$

$$= e^{\sum_{a\in\mathcal{Y}} \log Q(a)^{n\hat{P}_{y^n}(a)}} \tag{3}$$

$$= e^{n\sum_{a\in\mathcal{Y}} \hat{P}_{y^n}(a)\log Q(a)} \tag{4}$$

$$= e^{n\sum_{a\in\mathcal{Y}} \hat{P}_{y^n}(a)\log Q(a)\frac{\hat{P}_{y^n}(a)}{\hat{P}_{y^n}(a)}} \tag{5}$$

$$= e^{n\sum_{a\in\mathcal{Y}} \hat{P}_{y^n}(a)\log P_{y^n}(a) + n\sum_{a\in\mathcal{Y}} P_{y^n}(a)\log\frac{Q(a)}{\hat{P}_{y^n}(a)}} \tag{6}$$

$$= e^{-n\left(H(\hat{P}_{y^n}) + D(\hat{P}_{y^n}\|Q)\right)}. \tag{7}$$

ii. The likelihood ratio test checks whether

$$\frac{P_0^n(y^n)}{P_1^n(y^n)} \lessgtr \xi \tag{8}$$

This is equivalent to

$$\log\frac{P_0^n(y^n)}{P_1^n(y^n)} \lessgtr \log\xi. \tag{9}$$

Now, using (a),

$$\log\frac{P_0^n(y^n)}{P_1^n(y^n)} = \log\frac{e^{-n\left(H(\hat{P}_{y^n}) + D(\hat{P}_{y^n}\|P_0)\right)}}{e^{-n\left(H(\hat{P}_{y^n}) + D(\hat{P}_{y^n}\|P_1)\right)}} \tag{10}$$

$$= nD(\hat{P}_{y^n}\|P_1) - nD(\hat{P}_{y^n}\|P_0). \tag{11}$$

Dividing by n and letting $\gamma = \frac{1}{n}\log\xi$ gives the result.

iii. The assumption implies that $P_0(0) = 1-p$ and that $P_1(0) = p$. The Stein exponent in this case is

$$D(P_1\|P_0) = \sum_y P_1(y)\log\frac{P_1(y)}{P_0(y)} \tag{12}$$

$$= \underbrace{p\log\frac{p}{1-p}}_{y=0} + \underbrace{(1-p)\log\frac{1-p}{p}}_{y=1} \tag{13}$$

$$= p\log\frac{p}{(1-p)} - \log p - h(p) \tag{14}$$

4. (a) The ensemble average error probability is given by

$$\bar{p}_e = \sum_{v=1}^{M} q_v \,\mathrm{E}\left[\Pr\left[\bigcup_{v'\neq v}\left\{q_{v'}W^n(Y^n|X^n(v')) \geq q_v W^n(Y^n|X^n(v))\middle|X^n(v), Y^n\right\}\right]\right] \tag{15}$$

$$\leq \sum_{v=1}^{M} q_v \,\mathrm{E}\left[\min\left\{1, \sum_{v'\neq v}\Pr\left[q_{v'}W^n(Y^n|X^n(v')) \geq q_v W^n(Y^n|X^n(v))\middle|X^n(v), Y^n\right]\right\}\right] \tag{16}$$

$$\leq \sum_{v=1}^{M} q_v \,\mathrm{E}\left[\min\left\{1, \sum_{v'\neq v}\Pr\left[q_{v'}^s W^n(Y^n|X^n(v'))^s \geq q_v^s W^n(Y^n|X^n(v))^s\middle|X^n(v), Y^n\right]\right\}\right] \tag{17}$$

$$\leq \sum_{v=1}^{M} q_v \,\mathrm{E}\left[\min\left\{1, \sum_{v'\neq v}\frac{\mathrm{E}\left[q_{v'}^s W^n(Y^n|X^n(v'))^s\middle|X^n(v), Y^n\right]}{q_v^s W^n(Y^n|X^n(v))^s}\right\}\right] \tag{18}$$

$$\leq \sum_{v=1}^{M} q_v \,\mathrm{E}\left[\left(\sum_{v'\neq v}\frac{\mathrm{E}\left[q_{v'}^s W^n(Y^n|X^n(v'))^s\middle|X^n(v), Y^n\right]}{q_v^s W^n(Y^n|X^n(v))^s}\right)^{\rho}\right] \tag{19}$$

$$= \sum_{v=1}^{M} q_v^{1-s\rho} \,\mathrm{E}\left[\left(\sum_{v'=1}^{M}\frac{\mathrm{E}\left[q_{v'}^s W^n(Y^n|X^n(v'))^s\middle|X^n(v), Y^n\right]}{W^n(Y^n|X^n(v))^s}\right)^{\rho}\right] \tag{20}$$

where (15) follows from the definition of the MAP decoding error event, (16) follows from the union bound, (17) holds for any $s > 0$, (18) follows from Markov's inequality, (19) follows from $\min\{1, x\} \leq x^\rho$ for $0 \leq \rho \leq 1$ and (20) from bringing q_v outside.

Write the inner average as

$$\mathrm{E}\left[q_{v'}^s W^n(Y^n|X^n(v'))^s\middle|X^n(v) = x^n(v), Y^n = y^n\right] = q_{v'}^s \sum_{x^n(v')} Q(x^n(v')W^n(y^n|x^n(v'))^s \tag{21}$$

since the random codewords are generated independently of the messages. Thus,

$$\sum_{v'=1}^{M}\frac{\mathrm{E}\left[q_{v'}^s W^n(Y^n|X^n(v'))^s\middle|X^n(v) = x^n(v), Y^n = y^n\right]}{W^n(Y^n|X^n(v))^s}$$

$$= \sum_{v'=1}^{M} q_{v'}^s \sum_{x^n(v')} Q(x^n(v'))\frac{W^n(y^n|x^n(v'))^s}{W^n(y^n|x^n(v))^s} \tag{22}$$

$$= \sum_{\bar{x}^n} Q(\bar{x}^n)\frac{W^n(y^n|\bar{x}^n)^s}{W^n(y^n|x^n(v))^s}\sum_{v'=1}^{M} q_{v'}^s \tag{23}$$

where (22) follows since the codewords are generated independently from the messages, (23) follows since the sum over $x^n(v')$ is the same for every v', and we used $\bar{x}^n$ as dummy summation index.

Summarising, from (20) and (23), and by spelling out the outer expectation in (20) we have that

$$\bar{p}_e \leq \sum_{v=1}^{M} q_v^{1-s\rho} \sum_{x^n(v),y^n} Q(x^n(v))W^n(y^n|x^n(v))\left(\sum_{\bar{x}^n} Q(\bar{x}^n)\frac{W^n(y^n|\bar{x}^n)^s}{W^n(y^n|x^n(v))^s}\sum_{v'=1}^{M} q_{v'}^s\right)^\rho \tag{24}$$

$$= \sum_{v=1}^{M} q_v^{1-s\rho}\left(\sum_{v'=1}^{M} q_{v'}^s\right)^\rho \sum_{x^n,y^n} Q(x^n)W^n(y^n|x^n)\left(\sum_{\bar{x}^n} Q(\bar{x}^n)\frac{W^n(y^n|\bar{x}^n)^s}{W^n(y^n|x^n)^s}\right)^\rho \tag{25}$$

$$= \left(\sum_{v=1}^{M} q_v^{\frac{1}{1+\rho}}\right)^{1+\rho} \sum_{x^n,y^n} Q(x^n)W^n(y^n|x^n)\left(\sum_{\bar{x}^n} Q(\bar{x}^n)\frac{W^n(y^n|\bar{x}^n)^{\frac{1}{1+\rho}}}{W^n(y^n|x^n)^{\frac{1}{1+\rho}}}\right)^\rho \tag{26}$$

$$= \left(\sum_{v=1}^{M} q_v^{\frac{1}{1+\rho}}\right)^{1+\rho} \sum_{x^n,y^n} Q(x^n)W^n(y^n|x^n)^{\frac{1}{1+\rho}}\left(\sum_{\bar{x}^n} Q(\bar{x}^n)W^n(y^n|\bar{x}^n)^{\frac{1}{1+\rho}}\right)^\rho \tag{27}$$

$$= \left(\sum_{v=1}^{M} q_v^{\frac{1}{1+\rho}}\right)^{1+\rho} \sum_{y^n}\left(\sum_{x^n} Q(x^n)W^n(y^n|x^n)^{\frac{1}{1+\rho}}\right)^{1+\rho} \tag{28}$$

where (25) follows by noticing that the sum over $x^n(v)$ does not depend on v (since it is an average over the generation of codeword $x^n(v)$), (26) follows from setting $s = \frac{1}{1+\rho}$, (27) brings the term $W^n(y^n|\bar{x}^n)^{\frac{1}{1+\rho}}$ outside the sum over $\bar{x}^n$, and (28) froups the sums over $x^n, \bar{x}^n$, as these are dummy indices.

(b) If the messages are sequences of length n from a DMS V, then,

$$\sum_{v=1}^{M} q_v^{\frac{1}{1+\rho}} = \sum_{v^n}\prod_{i=1}^{n} P_V(v_i)^{\frac{1}{1+\rho}} \tag{29}$$

$$= \left(\sum_{v} P_V(v)^{\frac{1}{1+\rho}}\right)^n \tag{30}$$

$$= \mathrm{e}^{nE_s(\rho)} \tag{31}$$

Similarly,

$$\sum_{y^n}\left(\sum_{x^n} Q(x^n)W^n(y^n|x^n)^{\frac{1}{1+\rho}}\right)^{1+\rho} = \left(\sum_{y}\left(\sum_{x} Q(x)W(y|x)^{\frac{1}{1+\rho}}\right)^{1+\rho}\right)^n \tag{32}$$

$$= \mathrm{e}^{-nE_0(\rho)}\,. \tag{33}$$

Thus,

$$\bar{p}_e \leq \mathrm{e}^{-n(E_0(\rho)-E_s(\rho))}\,. \tag{34}$$

(c) The error probability will tend to zero as $n \to \infty$ whenever

$$E_0(\rho) > E_s(\rho), \text{for some } \rho \in [0,1]. \tag{35}$$

We know from the lectures that $E_0(\rho)$ is concave, increasing in ρ and $E_0(0) = 0$. Similarly, $E_s(\rho)$ is convex, increasing in ρ and $E_s(0) = 0$. Thus, the error exponent

will be > 0 as long as there is a ρ for which $E_0(\rho) > E_s(\rho)$. This is guaranteed to happen whenever

$$\frac{dE_0(\rho)}{d\rho}\Big|_{\rho=0} > \frac{dE_s(\rho)}{d\rho}\Big|_{\rho=0}. \tag{36}$$

From the notes, we know that

$$\frac{dE_0(\rho)}{d\rho}\Big|_{\rho=0} = I(X;Y) \tag{37}$$

$$\frac{dE_s(\rho)}{d\rho}\Big|_{\rho=0} = H(V). \tag{38}$$

Thus, for every input distributionP_X, if $I(X;Y) > H(V)$, $\bar{p}_e \to 0$ as $n \to \infty$, which is equivalent to $C > H(V)$.

(d) i. In this case,

$$E_s(\rho) = \rho \log |\mathcal{V}|. \tag{39}$$

Since, for a fixed rate R, $M = \mathrm{e}^{nR}$, we also have that $M = |\mathcal{V}|^n = \mathrm{e}^{n \log |\mathcal{V}|}$. Comparing both expressions, if we associate $R = \log |\mathcal{V}|$, we recover the channel coding theorem.

ii. Similarly, if the channel is noiseless

$$W(y|x) = \begin{cases} 1 & y = x \\ 0 & \text{otherwise.} \end{cases} \tag{40}$$

In this case, choosing $Q(x) = \frac{1}{|\mathcal{X}|}$ gives $E_0(\rho) = \rho \log |\mathcal{X}|$. Again associating $\log |\mathcal{X}| = R$ gives the result.

ENGINEERING TRIPOS PART IIB 2021

ASSESSOR'S REPORT

MODULE 4F5: Advanced Information Theory and Coding

The examination was taken by 58 current undergraduates, one undergraduate from the 2019/20 cohort, and 3 graduate students. The raw marks satisfied the distribution guidelines and hence did not require scaling. The numbers and averages below only refer to the 58 current undergraduates who took the examination.

Q1 Mathematical Fundamentals

58 attempts, Average mark 13.0/20, Maximum 18, Minimum 4.

This question was generally done well. In (b) a combination of Euclid and Stein steps considerably reduced the difficulty but most students found the right result tediously using only Euclid or Stein. In (c), the majority applied the Chinese Remainder Theorem correctly, but a few students did not provide sufficient evidence to ascertain that they used the theorem and lost method points as a result. In (e)(iv), only a handful of students realised that for any finite field GF($q=p^e$) with $p>2$ and generator α, $\alpha^{(q-1)/2} = -1 = p-1$.The format with many short questions is in its 4th session and has established itself well. It is easy to mark, provides a good mixture of straightforward questions and slightly trickier questions, and helps verify that students have engaged because the math used in this module is different from that used in other engineering modules.

Q2 Reed Solomon Coding

58 attempts, Average mark 16.09/20, Maximum 20, Minimum 1.

This is a predictable question testing students' ability to implement Reed Solomon decoding on a small field. Students generally did very well on the question. The mark distribution and average is almost identical to last time the exam was held in 2019. This is by no means an easy question, 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. While the high average on this question means that it is not as good at discriminating student ability as the other questions, the question provides an excellent validation of the progress achieved in teaching this course: when I started teaching Reed-Solomon codes in 2013/14, barely half of the students would have been able to solve this question accurately.

Q3 Cryptography / Hypothesis testing

58 attempts, Average mark 9.55/20, Maximum 19, Minimum 0.

This was a mixed question with (a) covering Cryptography and (b) covering Hypothesis testing. The cryptography part asked students to think of various scenarios for the use of the RSA cryptosystem, explain whether they were intended use of the cryptosystem, and think of practical situations in which this scenario comes into play. Only a minority of students came up with good realistic examples for the use of each scenario. Those who did demonstrated an excellent conceptual understanding of practical cryptography. Students were less successful on the hypothesis testing part of the question, with approximately 10 students barely attempting it or not at all, accounting for the low average mark on this question.

Q4 Error Exponents

No attempts. Only one graduate student attempted this question and got 11/20.

This reflects the feedback expressed by many students at the end of lectures that they experienced the second part of the course has being harder than the first part. The teaching for the second part will be re-calibrated next year in light of this feedback.

Jossy Sayir (Principal Assessor)