Error Correcting Codes - Final Mock

考試時間 Test time 09:30:00 am to 12:00:00 pm; 2.5 hours. 以投影機時鐘為準 Using the projected clock. 在答案卷作答 Answer on answer sheet. 每個題號一分 One point per problem. 全對才給分 No partial credit. 可以帶紙製品 Materials made of paper are allowed. 聽音樂請帶耳機 Use earphones for music. 禁止操作電子設備 Do not touch electronic devices. 舉手問問題 Raise your hand to ask questions.

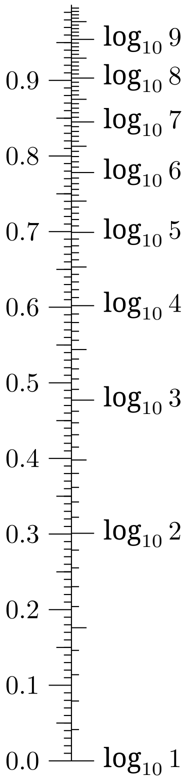
$\mathbf{F}_4$ is generated by 111 (i.e., $x^2 + x + 1$).
Its Zech table (i.e., $1 + \alpha^j = \alpha^{z(j)}$) is 0, 2, 1, 0.

$\mathbf{F}_8$ is generated by 1011 (i.e., $x^3 + x + 1$).
Its Zech table (i.e., $1 + \alpha^j = \alpha^{z(j)}$) is 0, 3, 6, 1, 5, 4, 2, 0.

$\mathbf{F}_{16}$ is generated by 10011
(i.e., $x^4 + x + 1$). Its Zech table is
0, 4, 8, 14, 1, 10, 13, 9, 2, 7,
5, 12, 11, 6, 3, 0.

$\mathbf{F}_{64}$ is generated by 1011011
(i.e., $x^6 + x^4 + x^3 + x + 1$). Its Zech table is
0, 56, 49, 13, 35, 30, 26, 8, 7, 27,
60, 23, 52, 3, 16, 34, 14, 39, 54, 48,
57, 42, 46, 11, 41, 58, 6, 9, 32, 44,
5, 59, 28, 38, 15, 4, 45, 43, 33, 17,
51, 24, 21, 37, 29, 36, 22, 61, 19, 2,
53, 40, 12, 50, 18, 62, 1, 20, 25, 31,
10, 47, 55, 0.

$\mathbf{F}_{128}$ is generated by 10000011
(i.e., $x^7 + x + 1$). Its Zech table is
0, 7, 14, 63, 28, 54, 126, 1, 56, 90,
108, 87, 125, 55, 2, 31, 112, 43, 53, 29,
89, 57, 47, 82, 123, 105, 110, 66, 4, 19,
62, 15, 97, 77, 86, 109, 106, 46, 58, 100,
51, 75, 114, 17, 94, 68, 37, 22, 119, 122,
83, 40, 93, 18, 5, 13, 8, 21, 38, 104,
124, 88, 30, 3, 67, 95, 27, 64, 45, 107,
91, 79, 85, 78, 92, 41, 116, 33, 73, 71,
102, 118, 23, 50, 101, 72, 34, 11, 61, 20,
9, 70, 74, 52, 44, 65, 111, 32, 117, 103,
39, 84, 80, 99, 59, 25, 36, 69, 10, 35,
26, 96, 16, 115, 42, 113, 76, 98, 81, 48,
121, 120, 49, 24, 60, 12, 6, 0.



$\mathbf{F}_{32}$ is generated by 100101
(i.e., $x^5 + x^2 + 1$). Its Zech table is
0, 18, 5, 29, 10, 2, 27, 22, 20, 16,
4, 19, 23, 14, 13, 24, 9, 30, 1, 11,
8, 25, 7, 12, 15, 21, 28, 6, 26, 3,
17, 0.

$\mathbf{F}_{256}$ is generated by 100011101
(i.e., $x^8 + x^4 + x^3 + x^2 + 1$). Its Zech table is
0, 25, 50, 223, 100, 138, 191, 112, 200, 120,
21, 245, 127, 99, 224, 33, 145, 68, 240, 92,
42, 10, 235, 196, 254, 1, 198, 104, 193, 181,
66, 45, 35, 15, 136, 32, 225, 179, 184, 106,
84, 157, 20, 121, 215, 31, 137, 101, 253, 197,
2, 238, 141, 147, 208, 63, 131, 83, 107, 82,
132, 186, 90, 55, 70, 162, 30, 216, 17, 130,
64, 109, 195, 236, 103, 199, 113, 228, 212, 174,
168, 160, 59, 57, 40, 170, 242, 167, 175, 203,
62, 209, 19, 158, 202, 176, 251, 190, 139, 13,
4, 47, 221, 74, 27, 248, 39, 58, 161, 71,
126, 246, 7, 76, 166, 243, 214, 122, 164, 153,
9, 43, 117, 183, 180, 194, 110, 12, 140, 239,
69, 56, 60, 250, 177, 144, 34, 46, 5, 98,
128, 52, 218, 150, 135, 16, 217, 53, 206, 188,
143, 178, 226, 119, 201, 159, 169, 41, 93, 155,
81, 108, 65, 182, 118, 227, 114, 87, 80, 156,
85, 211, 229, 232, 79, 88, 95, 134, 151, 37,
124, 29, 163, 123, 38, 249, 61, 204, 149, 219,
97, 6, 247, 28, 125, 72, 23, 49, 26, 75,
8, 154, 94, 89, 187, 207, 148, 205, 54, 91,
241, 171, 78, 233, 116, 44, 67, 146, 142, 189,
252, 102, 237, 3, 14, 36, 152, 165, 77, 172,
231, 230, 173, 213, 244, 22, 73, 222, 51, 129,
18, 210, 86, 115, 234, 11, 111, 192, 105, 185,
133, 96, 220, 48, 24, 0.

For questions with precision requirements, (2x) means that your answer should be in $[a/2, 2a]$, (5x) means $[a/5, 5a]$. For this kind of questions, answer in scientific notation such as 1.2e345.

[1] Parallel combination makes channels (A) less noisy (B) more noisy

[2] Serial combination makes channels (C) less noisy (D) more noisy

[3] Parallel combination turns two BECs into (E) a BEC for sure (F) a generic channel. PS. For this type of problem where one choice implies the other, you must chose the strongest choice. That is, running a red light will be fined ≥ 1800, not ≥ 1.

[4] Serial combination turns two BECs into (G) a BEC for sure (H) a generic channel

[5] Parallel combination turns two BSCs into (I) a BSC for sure (J) a generic channel

[6] Serial combination turns two BSCs into (K) a BSC for sure (L) a generic channel

[7] A bounded martingale $M_n \in [0, 1]$ converges to (M) a random variable $M_\infty \in \{0, 1\}$ for sure (N) a random variable $M_\infty \in [0, 1]$ (O) unfortunately it may not converge

[8] A submartingale is like a martingale, except that tomorrow's expectation can be better than today's. A

bounded submartingale $S_n \in [0,1]$ converges to (P) a random variable $S_\infty \in \{0,1\}$ for sure (Q) a random variable $S_\infty \in [0,1]$ (R) unfortunately it may not converge

[9] If a submartingale Z_n converges to $Z_\infty \in \{0,1\}$, then the probability $P(Z_\infty = 1)$ is (S) $\geq Z_0$ (T) $\leq Z_0$ (U) not necessarily comparable to Z_0.

[10] Using the Zech representation, what is $12 + 34$ in $\mathbf{F}_{64}$?

[11] Using the Zech representation, what is $56 + 78 + 90$ in $\mathbf{F}_{256}$?

[12] With the polynomial representation (notice how binary strings correspond to polynomials in the table above), what is $11011 \cdot 10101$ in $\mathbf{F}_{32}$?

[13] With the polynomial representation (notice how binary strings correspond to polynomials in the table above), what is $0001111 \cdot 1110000 \cdot 0011100$ in $\mathbf{F}_{128}$?

[14] A tetrahedral erasure channel TEC(p,q,r,s,t) is a channel with input alphabet $\mathbf{F}_4$ and output alphabet $\{0,1,*\}^3$. Note that there is a trace function tr: $\mathbf{F}_4 \to \mathbf{F}_2$ that is the same trace function as if $\mathbf{F}_4$ is represented as 2-by-2 matrices over $\mathbf{F}_2$. Given an input $x \in \mathbf{F}_4$, the TEC outputs

- $(\mathrm{tr}(x\omega), \mathrm{tr}(x), \mathrm{tr}(x/\omega))$ w.p. p,
- $(\mathrm{tr}(x\omega), *, *)$ w.p. q,
- $(*, \mathrm{tr}(x), *)$ w.p. r,
- $(*, *, \mathrm{tr}(x/\omega))$ w.p. s, and
- $(*, *, *)$ w.p. t.

Here, $\omega \in \mathbf{F}_4$ is a fixed element that is not in $\mathbf{F}_2$. Show that, if I send $a \in \mathbf{F}_2$ through BEC(ϕ) and $b \in \mathbf{F}_2$ through BEC(ψ), then this is equivalent to sending $a + b\omega$ through a TEC. Express the pqrst of this TEC using ϕ and ψ.

[15] Find the conditional entropy of TEC(p,q,r,s,t).

[16] Length-2 quaternary polar code is used over TEC. Show that the parallel combination of TEC(p,q,r,s,t) and TEC(p',q',r',s',t') is a TEC by finding the new pqrst using $p,\dots,t'$

[17] The same problem for serial combination.

[18] Recall that parallel and serial combinations turn the x in BEC(x) to $x \pm x(1-x)$. So the the difference between the conditional entropies of the parallel and serial combinations is $2x(1-x)$. Now, for the special case TEC(p,r,r,r,t), express (simplify) the difference between the conditional entropies of the parallel and serial combinations.

[19] Alice is sending some bits. The channel Bob sees is BEC with erasure probability 0.1. The channel Eve sees is BEC with capacity 0.1. Find a sequence of P (parallel) and S (serial) so that Bob's new erasure probability is less than 0.01, and Eve's new capacity is less than 0.01. (If your answer is too pathological for my computer to double-check, I will ask you to show me a proof of correctness.)

[20] Show that, for any $\varepsilon > 0$, there exists a $\delta > 0$ such that, if $H(W) < \delta$ for some BMSC W, then $Z(W) < \varepsilon$. Here, H is the conditional entropy (equivocation), and Z is the Bhattacharyya parameter of W.

[21] Show that, for any $\varepsilon > 0$, there exists a $\delta > 0$ such that, if $Z(W) < \delta$ for some BMSC W, then $H(W) < \varepsilon$.

[22] Prove that, for any $\varepsilon > 0$, there exists a $\delta > 0$ such that, if $H(W) > 1-\delta$ for some BMSC W, then $Z(W) > 1-\varepsilon$.

[23] Prove that, for any $\varepsilon > 0$, there exists a $\delta > 0$ such that, if $Z(W) > 1-\delta$ for some BMSC W, then $H(W) > 1-\varepsilon$.

[24] Let W and V be two BMSCs. If there exists a randomized function f such that the output of W can be simulated by passing the output of V through f, we say that W is a *degrade* of V, and V is an *upgrade* of W. For any $0 < p < q < 1$, it is known that BEC(q) is a degrade of BEC(p). What does the randomized function f look like?

[25] For any $0 < p < q < 1$, it is known that BSC(q) is a degrade of BSC(p). What does the randomized function f look like?

[26] For any $0 << s < 1$, it is known that AWGN(s) is a degrade of AWGN(t), where s and t are variances, and the inputs are ± 1. What does the randomized function f look like?

[27] Show that, if W is a degrade of V, then $W \star U$ is a degrade of $V \star U$, where $\star$ means parallel combination.

[28] Do the same problem if $\star$ means serial combination.

[29] Suppose that the channel Bob sees is BEC(p), and the channel Eve sees is BEC(q). Suppose that Eve's channel must output erasure if Bob's channel does. So Eve's channel is a *physical* degrade of Bob's, not just a *statistical* degrade. Now, for any sequence $\sigma \in \{p, s\}^n$ of parallel and serial, show that BEC$(q)^\sigma$ is a physical degrade of BEC$(p)^\sigma$.

[30] Let us analyze $(3, 6)$-LDPC using density evolution. When the underlying channel is BEC$(1/3)$, how many iterations of belief propagation do you need to bring the fraction of erased VNs to $1/10$ or below.

[31] When the underlying channel is W, the LLRs on each VN is a random variable. The distribution of these random variable changes after one iteration of BP. Which channel's LLR has the same distribution as that?

[32] Which channel describes the distribution of LLRs after two iterations of BP?

[33] Polar codes have a great ability called *rate matching*. At length 2^n, polar codes offer codes of rates $1/2^n, 2/2^n, \ldots, (2^n - 1)/2^n$ by selecting info sets and frozen sets of proper sizes. That is, one chip can handle multiple code rates by reusing decoder area. To determine info and frozen sets, the following procedure is used: Assume that every channel is a frozen bit, that is, the decoder always has the correct "u_1" when decoding for "u_2". However, we still record if a u_i is mis-decoded. Now, for a polar code of length 4, suppose that only the second BEC outputs erasure, which bit-channel(s) is mis-decoded? PS. For those of you who does not think BEC is a good model of channel, imagine that the same question is asked for BSC.

[34] The same question but the first and the last BEC output erasures.

[35] In the bit-flip basis, also called the Z-basis, $\langle\uparrow|$ is the row vector $[1\,0]$ and $\langle\downarrow|$ is the row vector $[0\,1]$. In the phase basis, also called the X-basis, $\langle+|$ is the row vector $[1\,1]/\sqrt{2}$, and $\langle-|$ is the column vector $[1\,-1]/\sqrt{2}$. Find the 2-by-2 matrix H such that $\langle\uparrow|H = \langle+|$ and $\langle\downarrow|H = \langle-|$.

[36] Find the matrix H' that does the opposite direction of change of basis. That is, $\langle+|H' = \langle\uparrow|$ and $\langle-|H' = \langle\downarrow|$.

[37] The NOT gate in the phase basis maps

- $\langle+|$ to $\langle-|$, and
- $\langle-|$ to $\langle+|$.

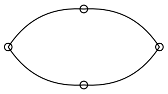
Express this NOT gate in the bit flip basis.

[38] The CNOT gate in the phase basis maps

- $\langle++|$ to $\langle++|$,
- $\langle+-|$ to $\langle+-|$,
- $\langle-+|$ to $\langle--|$, and
- $\langle--|$ to $\langle-+|$.

Express this CNOT gate in the bit flip basis.

[39] Find a 2-by-2 matrix S such that S^2 is the NOT gate in the bit flip basis.

[40] PS is  Draw PPSPS.

[41] (2x) Express $\binom{1000}{333}$ in scientific notation.

[42] (2x) Express $Z(\text{BSC}(0.1)^{ppppp})$ in scientific notation.

[43] (2x) Express $Z(\text{BSC}(0.1)^{sssss})$ in scientific notation.

[44] (2x) Define $T(\text{BSC}(p))$ as $|1-2p|$. Define the T of any convex combination of BSCs to be the same convex combination of the T's of the BSCs. Express $T(\text{BSC}(0.2345)^{p})$ in scientific notation.

[45] (2x) Express $T(\text{AWGN}(0.2345))$ in scientific notation.

[46] [47] [48] [49] [50] (5x) There will be five problems that ask you to guess certain quantities regarding real-world usage of error-correcting codes.

Error Correcting Codes - Final Mock

Name (zh or en)　Student ID

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14]

[15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27]

[28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40]

[41] [42] [43] [44] [45] [46] [47] [48] [49] [50]