Error Correcting Codes - Midterm Mock Exam

1   Terminology

Unless otherwise specified, there is a $[n, k, d]$ linear code over a finite field F.

[1] A symbol corresponds to (A) a basis (B) a vector (C) a linear subspace (D) a finite field element

[2] A codebook corresponds to (E) a basis (F) a vector (G) a linear subspace (H) a finite field element

[3] A codeword corresponds to (I) a basis (J) a vector (K) a linear subspace (L) a finite field element

[4] A generator matrix corresponds to (M) a basis (N) a vector (O) a linear subspace (P) a finite field element

[5] The alphabet is?

[6] The code rate is?

[7] The block length is?

[8] The code dimension is?

[9] The minimum distance is?

[10] The number of codewords is?

2   Popular Codes

[11] A code invariant under rotating is called (Q) cyclic code (R) repetition code (S) tensor product code (T) single parity-check code

[12] A code that looks like a sudoku puzzle is called (U) cyclic code (V) repetition code (W) tensor product code (X) single parity-check code

[13] A nontrivial code having relative distance 1 is called (Y) cyclic code (Z) repetition code (A) tensor product code (B) single parity-check code

[14] A code obtained by forcing an even number of 1's in each codeword is called (C) cyclic code (D) repetition code (E) tensor product code (F) single parity-check code

[15] A code whose syndrome is the binary representation of the error location is called (G) Hamming code (H) Reed–Muller code (I) Reed–Solomon code (J) Bose–Chaudhuri–Hocquenghem code

[16] A code obtained by evaluating univariate polynomials is called (K) Hamming code (L) Reed–Muller code (M) Reed–Solomon code (N) Bose–Chaudhuri–Hocquenghem code

[17] A code obtained by evaluating multilinear polynomials is called (O) Hamming code (P) Reed–Muller code (Q) Reed–Solomon code (R) Bose–Chaudhuri–Hocquenghem code

[18] A code where we care about consecutive roots of polynomials is called (S) Hamming code (T) Reed–Muller code (U) Reed–Solomon code (V) Bose–Chaudhuri–Hocquenghem code

[19] A code that can uniquely correct t errors and s erasures need minimum distance at least?

[20] According to the sphere packing bound, a $[9, 3]$ code can have minimum distance at most?

3 Linear Algebra

[21] What are the parameters $[n, k]$ if the following $G \in \mathbf{F}_2^{4 \times 6}$ is used?

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

**[22] What is the d for the G above?**

[23] What is its weight enumerator (univariate)?

[24] List all information set containing the first column. (Use the format 1234, 1235, 1245, 1345, ...)

[25] What is the H corresponding to this G?

[26] What are the parameters $[n, k, d]$ if G is treated as a matrix in $\mathbf{F}_3^{4 \times 6}$?

[27] What is the smallest Reed–Muller code containing the codeword below? Answer the parameters $[n, k, d]$ and (r, m).
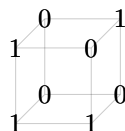
[28] What is the generator matrix of the $[16, 11]$ Reed–Muller code? Order the evaluation points lexicographically and reorder the rows such that the first 11 columns form an identity matrix.

[29] What is the generator polynomial of the smallest cyclic code containing 0000001111?

[30] The first row of H is 001 and the last row is 111. Between them are binary representations of 2–6. Correct the received word 10010110 that is flipped at most once.

4 Finite Field

[31] List the sizes of all finite fields up to 10.

[32] List the sizes of all finite fields from 10 to 20.

[33] Consider $\mathbf{F}_4$; let 0 be the additive identity, 1 be the multiplicative identity, and 2 and 3 be the other two elements. Complete the addition table on the answer sheet.

+	0 1 2 3
0	
1	
2	
3	

[34] Complete the multiplication table on the answer sheet.

[35] Factorize $x^5 + x^4 + 1 \in \mathbf{F}_2[x]$.

[36] What is the G of the $[5, 2]$ Reed–Solomon code over $\mathbf{F}_5$.

[37] What is the best degree-1 polynomial if $[1, 3, 4, 2, e]$ is received, where e means an erasure?

[38] Reduce α^{12} to a low degree polynomial if 101110001 (a polynomial in α) is used to construct $\mathbf{F}_{256}$.

[39] Reduce $\alpha^{100000000000000000}$.

[40] A BCH code with designed roots $\alpha, \alpha^2, \alpha^3$ is used. A received word r of is such that $r(\alpha) = \alpha^{-1}$ and $r(\alpha^3) = \alpha^{-6}$. Find the error-locating polynomial $aX^2 + bX + c$.

5   Probability

Answer in scientific notation such as 2e-5. A problem with 2x precision requirement means that you get full credit if your answer is in $[a/2, 2a]$, where a is the correct answer; 5x means that your answer should be in $[a/5, 5a]$. And so on. $\log_e(2) = 0.69305$. $\log_{10}(2) = 0.30101$. $\log_2(e) = 1.44283$. $\log_{10}(e) = 0.43427$. $\log_2(10) = 3.32237$. $\log_e(10) = 2.30257$.
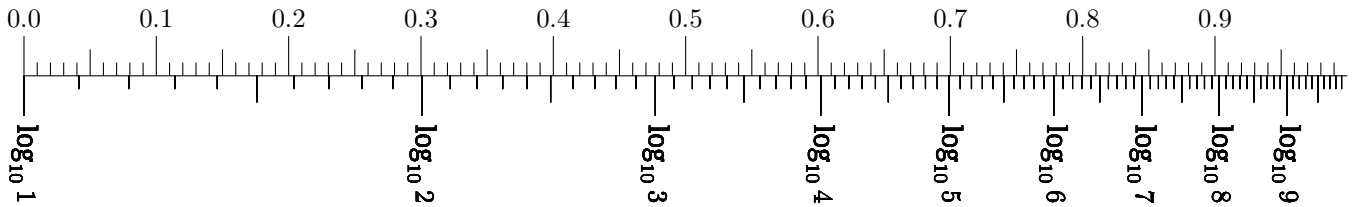
[41] (2x) If a wifi environment is such that every 1 MiB of data has an error probability of 10^{-8}, what is the probability that a 1-GiB file has an unrecoverable error?

[42] (2x) What if the file is 1-TiB file?

[43] (2x) What is the capacity of the binary symmetric channel with crossover probability 10^{-3}?

[44] (2x) What is the frame error rate if a single parity-check code of length 5 is used over the BSC above?

[45] (2x) BPSK is used and one of $-1, 1$ is sent, with equal probability. Three symbols whose product is 1 is sent. What is frame error probability?

[46] (2x) QPSK is used and one of $1, -1, i, -i$ is sent, with equal probability. The sigma of the complex Gaussian noise is 1 and $2 + i$ is received. What is the posterior probability that 1 is sent?

[47] (2x) What is the probability that i is sent.

[48] (2x) What is the probability that -1 is sent.

[49] (2x) The same symbol is transmitted again and $1 - i$ is received. What is the new posterior probability that 1 is sent?

[50] (2x) Consider a tensor product code whose codewords are 12×12 binary matrices whose rows and columns sum to even numbers. How many codewords have weight 6?

6   Relevant Knowledge

[51] (5x) What is the typical size of an internet packet?

[52] (5x) How much USB-drive storage can you buy with 1000 TWD?

[53] (5x) How many integer arithmetics can a consumer level CPU do in one second.

[54] (10x) What is coverage radius of a 5G cell tower (the one with the highest possible speed)?

[55] (10x) What is the design capacity of the FASTER trans-Pacific submarine communications cable?

Error Correcting Codes - Midterm Mock Exam

考試時間 Test time 09:30:00 am to 12:00:00 pm; 2.5 hours. 以教室投影機時鐘為準 Using the projected clock. 在本頁作答 Answer on this page. 每題一分 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.

姓名 Name (zh or en)   **學號 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]

[51]   [52]   [53]   [54]   [55]