Midterm

- You have 110 minutes (9:05-10:55 am) to complete the test.
- This is a closed-book test, except that three 8.5″ × 11″ sheets of notes are allowed.
- Calculators are allowed (provided that erasable memory is cleared).
- There are two problems on the quiz. The first is a seven-part problem, each part worth 10 points. There is also an optional eighth part, for which you can receive up to 10 points of extra credit. The second problem consists of three unrelated true-false questions, each worth 10 points.
- The problems are not necessarily in order of difficulty.
- Even if you can't prove a proposition stated in one part of a problem, you may assume that it is true in subsequent parts.
- A correct answer does not guarantee full credit and a wrong answer does not guarantee loss of credit. You should concisely indicate your reasoning and show all relevant work. The grade on each problem is based on our judgment of your level of understanding as reflected by what you have written.
- If we can't read it, we can't grade it.
- If you don't understand a problem, please ask.

α	dB	dB
	(round numbers)	(two decimal places)
1	0	0.00
1.25	1	0.97
2	3	3.01
2.5	4	3.98
e	4.3	4.34
3	4.8	4.77
π	5	4.97
4	6	6.02
5	7	6.99
8	9	9.03
10	10	10.00

Table 1. Values of certain small factors α in dB.

code	ρ	γ_c	(dB)	N_d	K_b	γ_{eff} (dB)	s	t
(8,7,2)	1.75	7/4	2.43	28	4	2.0	1	2
(8,4,4)	1.00	2	3.01	14	4	2.6	2	3
(16,15,2)	1.88	15/8	2.73	120	8	2.1	1	2
(16,11,4)	1.38	11/4	4.39	140	13	3.7	3	5
(16, 5,8)	0.63	5/2	3.98	30	6	3.5	3	4
(32,31, 2)	1.94	31/16	2.87	496	16	2.1	1	2
(32,26, 4)	1.63	13/4	5.12	1240	48	4.0	4	7
(32,16, 8)	1.00	4	6.02	620	39	4.9	6	9
(32, 6,16)	0.37	3	4.77	62	10	4.2	4	5
(64,63, 2)	1.97	63/32	2.94	2016	32	1.9	1	2
(64,57, 4)	1.78	57/16	5.52	10416	183	4.0	5	9
(64,42, 8)	1.31	21/4	7.20	11160	266	5.6	10	16
(64,22,16)	0.69	11/2	7.40	2604	118	6.0	10	14
(64, 7,32)	0.22	7/2	5.44	126	18	4.6	5	6

Table 2. Parameters of RM codes with lengths $n \leq 64$.

Problem M.1 (70 points)

In this problem, we will study a class of codes called *product codes.*

Suppose that $\mathcal{C}_1$ and $\mathcal{C}_2$ are two binary linear block codes with parameters (n_1, k_1, d_1) and (n_2, k_2, d_2), respectively. We will assume that the first k_1 and k_2 coordinate positions are information sets of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively.

The product code $\mathcal{C}$ is the code obtained by the following three-step encoding method. In the first step, k_1 independent information bits are placed in each of k_2 rows, thus creating a $k_2 \times k_1$ rectangular array (see Figure 1a). In the second step, the k_1 information bits in each of these k_2 rows are encoded into a codeword of length n_1 in $\mathcal{C}_1$, thus creating a $k_2 \times n_1$ rectangular array (see Figure 1b). In the third step, the k_2 information bits in each of the n_1 columns are encoded into a codeword of length n_2 in $\mathcal{C}_2$, thus creating an $n_2 \times n_1$ rectangular array (see Figure 1c).

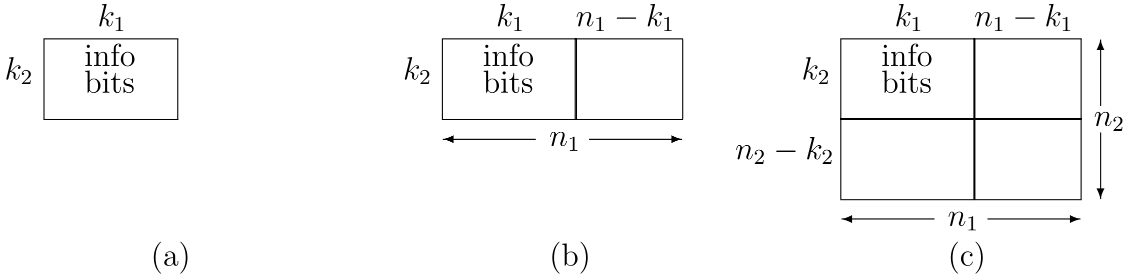

Figure 1. (a) $k_2 \times k_1$ information bit array. (b) $k_2 \times n_1$ array after row encoding. (c) $n_2 \times n_1$ array after column encoding.

(a) Given an (n, k) binary linear block code $\mathcal{C}$, show that the first k coordinate positions are an information set of $\mathcal{C}$ if and only if there exists a generator matrix G for $\mathcal{C}$ whose first k columns form a $k \times k$ identity matrix.

(b) Show that the encoding method given above produces the same codeword whether the encoder encodes first rows and then columns, or first columns and then rows.

(c) Show that the product code $\mathcal{C}$ is an $(n_1 n_2, k_1 k_2, d_1 d_2)$ binary linear block code.

(d) Express the nominal coding gain $\gamma_c(\mathcal{C})$ of the Euclidean-space image $s(\mathcal{C})$ of $\mathcal{C}$ in terms of the nominal coding gains $\gamma_c(\mathcal{C}_1)$ and $\gamma_c(\mathcal{C}_2)$ of the Euclidean-space images $s(\mathcal{C}_1)$ and $s(\mathcal{C}_2)$ of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Express the nominal spectral efficiency $\rho(\mathcal{C})$ of $\mathcal{C}$ in terms of the nominal spectral efficiencies $\rho(\mathcal{C}_1)$ and $\rho(\mathcal{C}_2)$ of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively.

(e) Starting with Reed-Muller codes of lengths less than 64, is it possible to use the product code construction to construct a product code of length 64 that has better parameters $(64, k, d)$ than the corresponding RM code of length 64?

(f) Starting with Reed-Muller codes of lengths less than 64, is it possible to obtain a sequence of product codes whose nominal coding gains increase without limit by iterating the product code construction— *i.e.,* by extending the above construction to an m-dimensional product code that maps an array of $k_1 \times k_2 \times \cdots \times k_m$ information bits into $n_1 \times n_2 \times \cdots \times n_m$ binary symbols using binary linear block codes $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_m$? Is it possible to do this while keeping the nominal spectral efficiency above some nonzero value?

(g) The construction of $\mathcal{C}$ suggests the following two-step decoding method. First decode each row, using an optimum (minimum Euclidean distance) decoding method for $\mathcal{C}_1$. This first decoding step yields an array of noisy received bits. Then decode each column, using an optimum (minimum Hamming distance) decoding method for $\mathcal{C}_2$.

Compare the performance and complexity of this two-step decoding method with that of the optimum decoding method on a binary-input AWGN channel. If you like, you may let both $\mathcal{C}_1$ and $\mathcal{C}_2$ be the $(8, 4, 4)$ RM code. As a figure of merit for performance, you may use the minimum squared norm of any error sequence that can cause a decoding error.

(h) [Optional; extra credit] Propose a two-step decoding method that has same figure of merit for performance as optimum decoding, but has decoding complexity similar to that of the suboptimal two-step method proposed in part (g).

Problem M.2 (30 points)

For each of the propositions below, state whether the proposition is true or false, and give a proof of not more than a few sentences, or a counterexample. No credit will be given for a correct answer without an adequate explanation.

(a) A signal constellation $\mathcal{A}$ consisting of a subset of 2^k points of the 2^n vertices of the n-cube, $k < n$, has a nominal spectral efficiency $\rho(\mathcal{A}) < 2$ b/2D and a nominal coding gain $\gamma_c(\mathcal{A}) \geq 1$.

(b) Let $S = \{a, b, c, d, e, f\}$ be a set of six elements, and let a binary operation $\oplus$ be defined on S by the following "addition table:"

$\oplus$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

Then S forms a group under the binary operation $\oplus$. (You need not check the associative law.)

(c) Considering the weight distribution of a $(6, 3, 4)$ code over $\mathbb{F}_4$, it is possible that such a code exists.