Final Exam

- You have 3 hours to complete the exam.
- This is a closed-book exam, except that five $8.5'' \times 11''$ sheets of notes are allowed.
- Calculators are allowed (provided that erasable memory is cleared).
- There are three problems on the exam. They are not necessarily in order of difficulty. The first two problems are multipart problems worth 60 and 40 points, respectively. The third problem consists of five unrelated true-false questions worth 10 points each.
- Even if you can't do one part of a multipart problem, try to do succeeding 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.

Figure 1. $P_b(E)$ *vs.* E_b/N_0 for uncoded binary PAM.

Figure 2. $P_s(E)$ *vs.* $\mathrm{SNR}_{\mathrm{norm}}$ for uncoded $(M \times M)$-QAM.

α	dB (approx.)	dB (exact)
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 A. Values of certain small factors α in dB.

RM 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 B. Parameters of certain Reed-Muller (RM) codes.

Table 1: Rate-1/2 binary linear convolutional codes

ν	d_{free}	γ_{c}	dB	K_b	γ_{eff}(dB)
1	3	1.5	1.8	1	1.8
2	5	2.5	4.0	1	4.0
3	6	3	4.8	2	4.6
4	7	3.5	5.2	4	4.8
5	8	4	6.0	5	5.6
6	10	5	7.0	46	5.9
6	9	4.5	6.5	4	6.1
7	10	5	7.0	6	6.7
8	12	6	7.8	10	7.1

Table 2: Rate-1/3 binary linear convolutional codes

ν	d_{free}	γ_{c}	dB	K_b	γ_{eff}(dB)
1	5	1.67	2.2	1	2.2
2	8	2.67	4.3	3	4.0
3	10	3.33	5.2	6	4.7
4	12	4	6.0	12	5.3
5	13	4.33	6.4	1	6.4
6	15	5	7.0	11	6.3
7	16	5.33	7.3	1	7.3
8	18	6	7.8	5	7.4

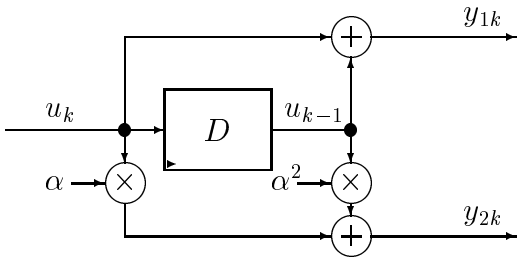
Table 3: Rate-1/4 binary linear convolutional codes

ν	d_{free}	γ_{c}	dB	K_b	γ_{eff}(dB)
1	7	1.75	2.4	1	2.4
2	10	2.5	4.0	2	3.8
3	13	3.25	5.1	4	4.7
4	16	4	6.0	8	5.6
5	18	4.5	6.5	6	6.0
6	20	5	7.0	37	6.0
7	22	5.5	7.4	2	7.2
8	24	6	7.8	2	7.6

Problem F.1 (60 points)

In this problem we consider a convolutional code C over the quaternary field $\mathbb{F}_4$. The elements of $\mathbb{F}_4$ may be denoted as $\{00, 01, 10, 11\}$ (additive representation) or as $\{0, 1, \alpha, \alpha^2\}$ (multiplicative representation), where α is a primitive element of $\mathbb{F}_4$ and a root of x^2+x+1. You might wish to jot down the addition and multiplication tables of $\mathbb{F}_4$.

The convolutional code C is generated by the encoder shown below.



The input u_k at time k is an element of $\mathbb{F}_4$, and the delay element (denoted by D) stores the previous input u_{k-1}. There are two $\mathbb{F}_4$ outputs at each time k, whose equations are

$$\begin{aligned} y_{1k} &= u_k + u_{k-1}; \\ y_{2k} &= \alpha u_k + \alpha^2 u_{k-1}. \end{aligned}$$

(a) Show that the convolutional code C is linear over $\mathbb{F}_4$.

(b) Let $u(D), y_1(D)$ and $y_2(D)$ be the D-transforms of the sequences $\{u_k\}, \{y_{1k}\}$ and $\{y_{2k}\}$, respectively. Give expressions for $y_1(D)$ and $y_2(D)$ in terms of $u(D)$.

(c) Specify the number of states in this encoder. Draw a single section of a trellis diagram for C, labelling each branch with a quaternary 2-tuple $(y_{1k}, y_{2k}) \in (\mathbb{F}_4)^2$.

(d) Show that this encoder for C is noncatastrophic.

(e) Find the minimum Hamming distance $d_{\text{free}}(C)$, and the average number of nearest neighbors $K_{\min}(C)$ per unit time.

Now define the *binary image* of C as the binary convolutional code C' obtained by mapping the outputs $y_{jk} \in \mathbb{F}_4$ into the additive representation $\{00, 01, 10, 11\}$, where each representative is a pair of elements of $\mathbb{F}_2$.

(f) Repeat parts (a)-(e) for C', replacing $\mathbb{F}_4$ by $\mathbb{F}_2$ where appropriate. (For part (b), map $u_k \in \mathbb{F}_4$ to its binary image.)

(g) Compute the nominal spectral efficiency $\rho(C')$ and the nominal coding gain $\gamma_{\text{c}}(C')$, and estimate the effective coding gain $\gamma_{\text{eff}}(C')$ using our usual rule of thumb. Compare the performance of C' to that of the best rate-$1/n$ binary linear convolutional code with the same spectral efficiency and number of states (see tables above).

Now define another binary convolutional code C'' as the code obtained by mapping the outputs $y_{jk} \in \mathbb{F}_4$ into the codewords $\{000, 011, 101, 110\}$ in the $(3, 2, 2)$ binary SPC code, where each representative is now a 3-tuple of elements of $\mathbb{F}_2$.

(h) Repeat parts (a)-(e) for C'', replacing $\mathbb{F}_4$ by $\mathbb{F}_2$ where appropriate. (For part (b), map $u_k \in \mathbb{F}_4$ to its binary image.)

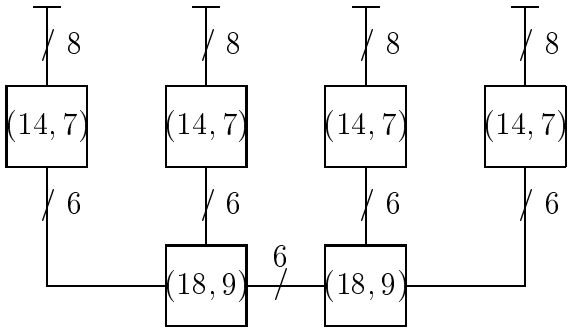
(i) Compute $\rho(C'')$ and $\gamma_c(C'')$, and estimate $\gamma_{\text{eff}}(C'')$. Compare the performance of C'' to that of the best rate-$1/n$ binary linear convolutional code with the same spectral efficiency and number of states (see tables above).

Problem F.2 (40 points)

In this problem we consider graphical representations and decoding of the $(32, 16, 8)$ binary Reed-Muller code RM$(2, 5)$.

(a) Show that there is a partition of the 32 symbols of this code into four 8-tuples such that the projection of RM$(2, 5)$ onto any 8-tuple is the $(8, 7, 2)$ binary SPC code, and the subcode corresponding to each 8-tuple is the $(8, 1, 8)$ binary repetition code; moreover, the 8-tuples may be paired such that the projection onto each resulting 16-tuple is the $(16, 11, 4)$ extended Hamming code, and the subcode corresponding to each resulting 16-tuple is the $(16, 5, 8)$ biorthogonal code.

(b) Using part (a), show that there is a normal realization of RM$(2, 5)$ whose graph is as follows:



[Tip: to find the constraint code dimensions, you may use the fact (not proved in 6.451) that the constraint codes in a cycle-free representation of a self-dual code are self-dual.]

(c) Using part (b), give a high-level description of an efficient algorithm for maximum-likelihood decoding of RM$(2, 5)$ on an arbitrary memoryless channel.

(d) Compare the performance (probability of error) and complexity (number of arithmetic operations, roughly) of the algorithm of part (c) to that of the Viterbi algorithm applied to an efficient trellis realization of RM$(2, 5)$. [Hint: start by finding a trellis-oriented generator matrix for RM$(2, 5)$, and then find an efficient sectionalization.]

Problem F.3 (50 points)

For each of the propositions below, state whether the proposition is true or false, and give a brief proof. If a proposition is false, the proof will usually be a counterexample. Full credit will not be given for correct answers without an adequate explanation.

(a) The Euclidean image of an (n, k, d) binary linear block code is an orthogonal signal set if and only if $k = \log_2 n$ and $d = n/2$.

(b) Every element $\beta \in \mathbb{F}_{32}$ is the root of a binary polynomial $f(x) \in \mathbb{F}_2[x]$ of degree less than or equal to 5.

(c) If codewords in an (n, k, d) binary linear block code with d even are transmitted equiprobably over an AWGN channel using a standard 2-PAM map and are optimally detected, then the minimum squared distance to any decision boundary is twice the minimum squared distance that is achieved if binary hard decisions are made first on each symbol and then the resulting binary received word is optimally decoded.

(d) Capacity-approaching codes must have trellis complexity parameters that become arbitrarily large as the Shannon limit is approached arbitrarily closely.

(e) If the points $\mathbf{x}$ in a lattice Λ are transmitted with unequal probabilities $\{p(\mathbf{x}), \mathbf{x} \in \Lambda\}$ over an AWGN channel and optimally detected, then $\Pr(E) \approx K_{\min}(\Lambda) Q^{\surd}(d^2_{\min}(\Lambda)/4\sigma^2)$, where $d^2_{\min}(\Lambda)$ is the minimum squared distance between points in Λ, and $K_{\min}(\Lambda)$ is the average number of nearest neighbors to each transmitted point.