Midterm Solutions

Problem M.1 (70 points)

Recall that an M-simplex signal set is a set of M signals $\mathcal{A} = \{\mathbf{a}_j \in \mathbb{R}^{M-1}, 1 \le j \le M\}$ in an $(M-1)$-dimensional real space $\mathbb{R}^{M-1}$, such that, for some $E_{\mathcal{A}} > 0$,

$$\langle \mathbf{a}_i, \mathbf{a}_j \rangle = \begin{cases} E_{\mathcal{A}}, & \text{if } i = j; \\ -\frac{E_{\mathcal{A}}}{M-1}, & \text{if } i \neq j. \end{cases}$$

Initially we will assume that M is a power of 2, $M = 2^m$, for some integer m.

(a) Compute the nominal spectral efficiency $\rho(\mathcal{A})$ and the nominal coding gain $\gamma_c(\mathcal{A})$ of an M-simplex signal set $\mathcal{A}$ on an AWGN channel as a function of $M = 2^m$.

The M-simplex signal set has $M = 2^m$ points, so the number of bits per symbol is $\log_2 M = m$. The number of dimensions is $N = M - 1$. The nominal spectral efficiency is therefore

$$\rho(\mathcal{A}) = \frac{2\log_2 M}{M-1} = \frac{2m}{M-1} \text{ b/2D}.$$

This equals 2 for $M = 2$ and decreases monotonically with M, so we are in the power-limited regime. Indeed, as $M \to \infty$, $\rho \to 0$.

The nominal coding gain in the power-limited regime is defined as $\gamma_c(\mathcal{A}) = d^2_{\min}(\mathcal{A})/4E_b$. The squared distance between any two distinct signals is

$$||\mathbf{a}_i - \mathbf{a}_j||^2 = ||\mathbf{a}_i||^2 - 2\langle \mathbf{a}_i, \mathbf{a}_j \rangle + ||\mathbf{a}_j||^2 = 2E_{\mathcal{A}} + 2\frac{E_{\mathcal{A}}}{M-1} = \frac{M}{M-1} 2E_{\mathcal{A}},$$

so $d^2_{\min}(\mathcal{A}) = 2ME_{\mathcal{A}}/(M-1)$. The energy per signal is $E_{\mathcal{A}}$, so the energy per bit is $E_b = E_{\mathcal{A}}/(\log_2 M) = E_{\mathcal{A}}/m$. The nominal coding gain is therefore

$$\gamma_c(\mathcal{A}) = \frac{d^2_{\min}(\mathcal{A})}{4E_b} = \frac{M}{M-1}\frac{\log_2 M}{2} = \frac{M}{M-1}\frac{m}{2}.$$

This equals 1 when $M = 2$, and increases monotonically (albeit slowly) with M. As $M \to \infty$, $\gamma_c(\mathcal{A}) \to \infty$.

(b) What is the limit of the effective coding gain $\gamma_{\text{eff}}(\mathcal{A})$ of an M-simplex signal set $\mathcal{A}$ as $M \to \infty$, at a target error rate of $\Pr(E) \approx 10^{-5}$?

As shown in 6.450 and reiterated this term, orthogonal or simplex signal sets approach the ultimate Shannon limit on E_b/N_0 as $M \to \infty$; *i.e.*, they can achieve arbitrarily low $\Pr(E)$ for any $E_b/N_0 > \ln 2$ (-1.59 dB). For the baseline 2-PAM signal set, $\Pr(E) \approx 10^{-5}$ when $E_b/N_0 \approx 9.6$ dB. Therefore the limit of $\gamma_{\text{eff}}(\mathcal{A})$ as $M \to \infty$ is ≈ 11.2 dB.

[Note: only one student answered this question correctly.]

(c) Give a method of implementing an $(M = 2^m)$-simplex signal set $\mathcal{A}$ in which each signal $\mathbf{a}_j$ is a sequence of points from a 2-PAM signal set $\{\pm\alpha\}$.

We saw in the problem sets that the Euclidean image of a $(2^m - 1, m, 2^{m-1})$ binary linear code $\mathcal{C}$ could form a 2^m-simplex signal set, in two different cases:

- $\mathcal{C}$ is obtained by shortening a $(2^m, m+1, 2^{m-1})$ biorthogonal RM$(1, m)$ code;
- $\mathcal{C}$ is a maximum-length-shift-register code generated by a length-m shift register.

In either case each signal $\mathbf{a}_j$ is a sequence of $2^m - 1$ points from a 2-PAM signal set. (In 6.450 you also saw a construction of an orthogonal signal set from a Hadamard matrix.)

Now consider a concatenated coding scheme in which

- *the outer code is an (n, k, d) linear code $\mathcal{C}$ over a finite field $\mathbb{F}_q$ with $q = 2^m$, which has N_d codewords of minimum nonzero weight;*
- *outer q-ary code symbols are mapped into a q-simplex signal set $\mathcal{A}$ via a one-to-one map $s : \mathbb{F}_q \to \mathcal{A}$.*

If $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is an n-tuple in $(\mathbb{F}_q)^n$, then $s(\mathbf{x}) = (s(x_1), s(x_2), \ldots, s(x_n))$ will be called the Euclidean image of $\mathbf{x}$. Let $\mathcal{A}' = s(\mathcal{C}) = \{s(\mathbf{x}), \mathbf{x} \in \mathcal{C}\}$ denote the signal set consisting of the Euclidean images of all codewords $\mathbf{x} \in \mathcal{C}$.

(d) Compute the nominal spectral efficiency $\rho(\mathcal{A}')$ of the concatenated signal set $\mathcal{A}'$ on an AWGN channel. Is this signal set appropriate for the power-limited or the bandwidth-limited regime?

The size of $\mathcal{A}'$ is $|\mathcal{A}'| = |\mathcal{C}| = q^k$, and the dimension of $\mathcal{A}'$ is $n(q-1)$. Therefore

$$\rho(\mathcal{A}') = \frac{2k \log_2 q}{n(q-1)} = \frac{k}{n}\rho(\mathcal{A}) \leq 2,$$

and we are in the power-limited regime.

(e) Compute $d^2_{\min}(\mathcal{A}')$, $K_{\min}(\mathcal{A}')$, and $\gamma_c(\mathcal{A}')$. Give a good estimate of an appropriately normalized error probability for $\mathcal{A}'$.

The squared distance between the Euclidean images of two distinct codewords $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ that differ by Hamming distance $d_H(\mathbf{x}, \mathbf{y})$ is

$$||s(\mathbf{x}) - s(\mathbf{y})||^2 = d_H(\mathbf{x}, \mathbf{y}) d^2_{\min}(\mathcal{A}),$$

since the coordinatewise distance is $d^2_{\min}(\mathcal{A})$ in each coordinate where the two words differ, and 0 otherwise. Therefore

$$d^2_{\min}(\mathcal{A}') = d d^2_{\min}(\mathcal{A}) = \frac{M}{M-1} 2dE_{\mathcal{A}},$$

and moreover every point in $\mathcal{A}'$ has $K_{\min}(\mathcal{A}') = N_d$ nearest neighbors. Since $E_b(\mathcal{A}') = (n/k)E_b(\mathcal{A})$, the nominal coding gain is

$$\gamma_c(\mathcal{A}') = \frac{d^2_{\min}(\mathcal{A}')}{4E_b(\mathcal{A}')} = \frac{d d^2_{\min}(\mathcal{A})}{4(n/k)E_b(\mathcal{A})} = \frac{kd}{n}\gamma_c(\mathcal{A}) = \frac{kd}{n}\frac{q}{q-1}\frac{\log_2 q}{2}.$$

Notice that this reduces to $\gamma_c(\mathcal{A}') = kd/n$ when $q = 2$.

The union bound estimate (UBE) gives a good estimate of the error probability $\Pr(E)$. In the power-limited regime, we normalize to the error probability per bit, $P_b(E)$, and express it as a function of E_b/N_0. The UBE of $P_b(E)$ is

$$P_b(E) \approx K_b(\mathcal{A}')Q^{\surd}(2\gamma_c(\mathcal{A}')E_b/N_0) = \frac{N_d}{k\log_2 q}Q^{\surd}\left(\frac{kd}{n}\frac{q}{q-1}(\log_2 q)E_b/N_0\right),$$

where we use the fact that $\log_2|\mathcal{A}'| = k\log_2 q$ bits.

Now consider the case in which $\mathcal{C}$ is an $(n = q+1, k = 2, d = q)$ linear code over $\mathbb{F}_q$.

(f) Show that a code $\mathcal{C}$ with these parameters exists whenever q is a prime power, $q = p^m$. Show that all nonzero codewords in $\mathcal{C}$ have the same Hamming weight.

A finite field $\mathbb{F}_q$ exists whenever $q = p^m$. In an exercise which we did as a homework problem, we showed that a doubly-extended $(n = q+1, k, d = n-k+1)$ RS code exists over any field $\mathbb{F}_q$ for $1 \le k \le n$. Thus there exists a $(q+1, 2, q)$ code over $\mathbb{F}_q$. (Its generators are:

$$\mathbf{g}_0 = (1, 1, 1, \ldots, 1, 0), \mathbf{g}_1 = (0, 1, \alpha, \ldots, \alpha^{q-2}, 1).)$$

Examples: the $(3, 2, 2)$ SPC code over $\mathbb{F}_2$; the $(4, 2, 3)$ "tetracode" over $\mathbb{F}_3$; a $(5, 2, 4)$ code over $\mathbb{F}_4$.

A $(q+1, 2, q)$ code is MDS, and therefore

$$N_d = \binom{n}{d}(q-1) = \binom{q+1}{q}(q-1) = (q+1)(q-1) = q^2 - 1.$$

Thus all $q^2 - 1$ nonzero codewords have Hamming weight $d = q$.

(g) Show that the Euclidean image $\mathcal{A}' = s(\mathcal{C})$ of $\mathcal{C}$ is a q^2-simplex signal set.

The number of points in $\mathcal{A}'$ is $|\mathcal{A}'| = |\mathcal{C}| = q^2$. Each point in $\mathcal{A}'$ is a sequence of $q+1$ points in $\mathcal{A}$, so the dimension of $\mathcal{A}'$ is

$$\dim(\mathcal{A}') = (q+1)\dim(\mathcal{A}) = (q+1)(q-1) = q^2 - 1.$$

The energy of each point in $\mathcal{A}'$ is $E_{\mathcal{A}'} = (q+1)E_{\mathcal{A}}$. Since the inner product between symbols is $E_{\mathcal{A}}$ where they agree and $-E_{\mathcal{A}}/(q-1)$ where they disagree, and any two distinct points $\mathbf{x}, \mathbf{y} \in \mathcal{A}'$ agree in one component and disagree in q components, we have

$$\langle s(\mathbf{x}), s(\mathbf{y})\rangle = E_{\mathcal{A}} - \frac{q}{q-1}E_{\mathcal{A}} = -\frac{E_{\mathcal{A}}}{q-1} = -\frac{E_{\mathcal{A}'}}{q^2-1}.$$

Therefore $\mathcal{A}'$ is a q^2-simplex signal set.

Thus we can see how we might recursively generate simplex signal sets with $2, 4, 16, 256, 2^{16}, \ldots$ points, starting from a 2-PAM signal set and using doubly-extended $(q+1, 2, q)$ RS codes over $\mathbb{F}_q$.

Scores on Problem 1: $4 \in [9, 19]; 8 \in [20, 29]; 4 \in [30, 39]; 8 \in [40, 49]; 2 \in [50, 60]$.

Problem M.2 (30 points)

(a) Let $p(t)$ be a complex $\mathcal{L}_2$ signal with Fourier transform $P(f)$. If the set of time shifts $\{p(t - kT), k \in \mathbb{Z}\}$ is orthonormal for some $T > 0$, then $P(0) \neq 0$.

False. The orthonormality condition is

$$\frac{1}{T} \sum_m |P(f - m/T)|^2 = 1, \forall f.$$

This can be satisfied by, *e.g.*, $|P(f)|^2 = T$ for $1/T \leq f < 2/T$ and $P(f) = 0$ elsewhere, including $P(0) = 0$.

(b) Let $s(\mathcal{C})$ be the Euclidean-space image of a binary linear block code $\mathcal{C}$ under a 2-PAM map $s : \{0, 1\} \to \{\pm\alpha\}$. Then the mean $\mathbf{m}$ of the signal set $s(\mathcal{C})$ is $\mathbf{0}$, unless there is some coordinate in which all codewords of $\mathcal{C}$ have the value 0.

True. This proposition holds if and only if half the codewords in any binary linear code $\mathcal{C}$ have a 0 in any coordinate position, and half have a 1 (unless all are 0).

To show this, recall that $\mathcal{C}$ can be specified as the set of all binary linear combinations of some set of generators, and that a given generator $\mathbf{g}$ is a component (with a 1 coefficient) of precisely half the codewords. In fact, we can group the codewords into pairs $(\mathbf{c}, \mathbf{c}+\mathbf{g})$ of codewords that do and do not include $\mathbf{g}$, respectively. Now given any coordinate position, we can find a generator $\mathbf{g}$ that has a 1 in the given position, unless all codewords have a 0 in that position. Given such a $\mathbf{g}$, exactly one of each pair $(\mathbf{c}, \mathbf{c} + \mathbf{g})$ has a 0 in the given position, and one has a 1. Therefore precisely half the codewords have a 1 in the given position, unless all have a 0. This argument holds for all coordinate positions.

(c) A polynomial $f(z) \in \mathbb{F}_q[z]$ satisfies $f(\beta) = 0$ for all $\beta \in \mathbb{F}_q$ if and only if $f(z)$ is a multiple of $z^q - z$.

True. A polynomial $f(z)$ satisfies $f(\beta) = 0$ if and only if $z - \beta$ is a factor of $f(z)$. Thus $f(\beta) = 0$ for all $\beta \in \mathbb{F}_q$ if and only if $\prod_{\beta \in \mathbb{F}_q} (z - \beta)$ divides $f(z)$. But according to Theorem 3.1 of Lecture 7, this product is equal to $z^q - z$.

Scores on Problem 2: $6 \in [0, 9]; 9 \in [10, 19]; 11 \in [20, 31]$.

Scores on Midterm: $1 \in [10, 19]; 2 \in [20, 29]; 5 \in [30, 39]; 5 \in [40, 49]; 3 \in [50, 59]; 5 \in [60, 69]; 3 \in [70, 79]; 2 \in [80, 90]$. Median 52, 75% = 64, 25% = 36.