ECE 259A: Final Exam

The solutions are due by 11:59 pm on Saturday, December 14, 2019. The easiest way to submit your solutions is to scan and e-mail them to (avardy@ucsd.edu) and (hay125@eng.ucsd.edu). This is the only way to submit that allows full use of the allocated time until the deadline. Alternatively, you can submit the hard copy of your solutions in Room 4107 of the Atkinson Hall (a.k.a. Qualcomm Institute or CalIT2 building). If the door is locked, please slide the solutions under the door. However, the Atkinson Hall will be locked as of 7:00pm on Friday, December 13, 2019. Therefore, if you choose this alternative, then 7:00pm on Friday, December 13, 2019, may become your submission deadline.

You should work on all the problems on this exam by yourself. If you have any questions regarding this exam, you are welcome to consult with me or with the TA, but not with any other person.

You are allowed to use calculators, computers, and any auxiliary material, including materials posted online. However, you are required to explicitly state this in full detail. Computer programs should not be necessary; however, if you have used a computer program please submit both the code and the output with your exam. If you have used a result from the literature, other than the textbook, please provide reference to the source and include complete derivation of the result in your solution.

The total score on this exam is 180 points. Of these, 30 are bonus points. A score of 150 points would result in a full credit towards the course grade. Scores above 150 points will be prorated to offset any deficit you might have in the homework grades.

Good luck!

Problem 1. (30 points)

A binary vector $x = (x_1, x_2, \ldots, x_n)$ is chosen uniformly at random from $\{0, 1\}^n$ and then transmitted over $n$ channels $C_1, C_2, \ldots, C_n$. For $i = 1, 2, \ldots, n$, the channel $C_i$ erases the $i$-th bit of $x$ while transmitting all other bits as is. For example, for $n = 7$, the outputs of $C_1, C_2, \ldots, C_7$ are given by

$$(\epsilon, x_2, x_3, x_4, x_5, x_6, x_7), (x_1, \epsilon, x_3, x_4, x_5, x_6, x_7), (x_1, x_2, \epsilon, x_4, x_5, x_6, x_7),$$
$$(x_1, x_2, x_3, \epsilon, x_6, x_7), (x_1, x_2, x_3, x_4, x_5, x_7), (x_1, x_2, x_3, x_4, x_5, x_7, \epsilon)$$

where $\epsilon$ denotes the erasure symbol, which conveys no information about the transmitted bit. The outputs of the channels $C_1, C_2, \ldots, C_n$ are observed by the decoders $D_1, D_2, \ldots, D_n$, respectively. Your task in this problem is to design these decoders.

Each decoder $D_i$ must operate as follows. Upon observing the output of $C_i$ (and nothing else), the decoder can either declare a decoding failure $F$ or produce an estimate $\hat{x}_i \in \{0, 1\}^n$ of the transmitted vector $x$. The outputs of the $n$ decoders are then aggregated. Those decoders that declare a decoding failure are ignored. Let $S \subseteq \{1, 2, \ldots, n\}$ denote the index set of those decoders that do produce an estimate of $x$. If all such estimates agree, that is $\hat{x}_i = \hat{x}_j$ for all $i, j \in S$, then this common estimate is taken as the overall system output $\hat{x}$. If there exist $i, j \in S$ such that $\hat{x}_i \neq \hat{x}_j$ or if all $n$ decoders declare a failure, then the overall system output is decoding failure $F$. Define

$$P_f = \text{ probability that the system output is a decoding failure } F$$
$$P_e = \text{ probability that the system output is } \hat{x} \text{ for some } \hat{x} \neq x$$
$$P_c = \text{ probability that the system output is } \hat{x} \text{ with } \hat{x} = x$$
where all the probabilities are with respect to the uniformly random choice of the vector \( x \) from \( \{0, 1\}^n \) (the decoders \( D_1, D_2, \ldots, D_n \) are deterministic functions from \( \{0, 1\}^{n-1} \) to \( \mathcal{F} \cup \{0, 1\}^n \) and the channels \( C_1, C_2, \ldots, C_n \) are also deterministic). Clearly \( P_f + P_c + P_e = 1 \).

a. For \( n = 7 \), design the decoders \( D_1, D_2, \ldots, D_7 \) to maximize the probability \( P_c \) that the system output is correct. What is this probability?

b. Show how to design the decoders \( D_1, D_2, \ldots, D_n \) so that \( P_c \rightarrow 1 \) as \( n \rightarrow \infty \).

c. For \( n = 2^m - 1 \), prove that your design in part (b) is optimal. That is, your design of the decoders \( D_1, D_2, \ldots, D_n \) yields the highest possible probability \( P_c \) for all \( n = 2^m - 1 \) with \( m \geq 2 \).

**Hint:** Hamming codes may be helpful in this problem.

**Problem 2.** (30 points)

a. Let \( p \) be a prime. Prove that the polynomial \( f(x) = x^p - x + 1 \) is irreducible over \( GF(p) \).

b. Let \( \alpha \in GF(q) \) be an element of multiplicative order \( s \). If it is known that \( s \) and \( (q - 1)/s \) are relatively prime, prove that the polynomial \( f(x) = x^s - \alpha \) is irreducible over \( GF(q) \).

**Hint:** If \( g(x) \) is an irreducible factor of \( f(x) \) of degree \( d < s \), use it to construct \( GF(q^d) \).

**Problem 3.** (20 points)

Let \( F_q \) be the finite field of order \( q \). Let \( 1 \) denote the vector \((111\cdots111)\) of length \( n \). Given a code \( C \) (linear or nonlinear) of length \( n \) over \( F_q \) and a set \( E \subseteq F_q^n \) of potential error vectors, we say that \( C \) corrects all the errors in \( E \) if \( \xi_1 + \xi_2 \neq \xi_2 + \xi_2 \) for all distinct \( \xi_1, \xi_2 \in C \) and all \( \xi_1, \xi_2 \in E \).

a. Let \( C \) be a linear code of length \( n \) over \( F_q \). Prove that \( C \) corrects all the errors in \( \{ \alpha \cdot 1 : \alpha \in F_q \} \) if and only if \( 1 \notin C \) (here, \( \alpha \cdot 1 \) is the the vector \((\alpha \alpha \cdots \alpha \alpha)\) of length \( n \) over \( F_q \)).

b. What is the highest possible dimension for a linear code \( C \) of length \( n \) over \( F_q \) that corrects all the errors in \( \{ \alpha \cdot 1 : \alpha \in F_q \} \)? Explain how a generator matrix for such a code can be obtained.

Now assume that errors are of the form \( \xi = \xi_1 + \xi_2 \), where \( \xi_1 = \alpha \cdot 1 \) for some \( \alpha \in F_q \) while \( \xi_2 \) is a vector of weight \( \leq t \). That is, consider the set of errors \( E = \{ \alpha \cdot 1 + \xi : \alpha \in F_q, \xi \in F_q^n, \text{wt}(\xi) \leq t \} \).

c. Let \( C \) be a linear code of length \( n \) over \( F_q \). Prove that \( C \) corrects all the errors in \( E \) if and only if \( 1 \notin C \) and the minimum distance of the code \( C^* = \{ \xi + \alpha \cdot 1 : \xi \in C, \alpha \in F_q \} \) is at least \( 2t + 1 \).

d. Let \( C \) be a linear code of length \( n \) over \( F_q \) that corrects all the errors in \( E \). Prove that the dimension \( k \) of \( C \) satisfies \( k \leq n - 2t - 1 \).

e. Assume that \( 2t + 1 \leq n \leq q \). Write-down a generator matrix for a linear code \( C \) of length \( n \) and dimension \( k = n - 2t - 1 \) over \( F_q \) that corrects all the errors in \( E \).
Problem 4. (30 points)

Given a binary vector \( a = (a_1, a_2, \ldots, a_n) \), let \( C(a) \) denote the binary linear code of length \( 2n \) and dimension \( n \) defined by the following parity-check matrix:

\[
H = \begin{bmatrix}
  1 & a_1 & a_2 & \cdots & a_{n-1} & a_n \\
  1 & a_n & a_1 & \cdots & a_{n-2} & a_{n-1} \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
  1 & a_3 & a_4 & \cdots & a_n & a_1 \\
  & a_2 & a_3 & \cdots & a_n & a_1
\end{bmatrix}
\]  

That is, \( H = [I \mid A] \) where \( I \) is the \( n \times n \) identity matrix and \( A \) is the \( n \times n \) matrix whose rows are the \( n \) cyclic shifts of the vector \( a = (a_1, a_2, \ldots, a_n) \).

a. Let \( \pi \) be a permutation in \( S_{2n} \) that takes a vector \( x = (x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{2n}) \) into the vector

\[
\pi(x) = (x_n, x_1, \ldots, x_{n-1}, x_{2n}, x_{n+1}, \ldots, x_{2n-1})
\]

That is, \( \pi \) effects a cyclic shift of the first \( n \) positions in \( x \) and a cyclic shift of the last \( n \) positions in \( x \). Prove that the code \( C(a) \) is invariant under this permutation. In other words, show that for all \( c \in C(a) \), the vector \( \pi(c) \) is also a codeword of \( C(a) \).

Henceforth, let us assume that \( n \) is prime, and consider the following random experiment. The experiment consists of selecting a vector \( a \) uniformly at random from \( \mathbb{F}_2^n \) and generating the corresponding code \( C(a) \) according to (1). You can think of these codes \( C(a) \) as the outcomes of the random experiment. Since each such code \( C(a) \) is uniquely determined by the underlying vector \( a \), there are \( 2^n \) possible outcomes, all of them equally likely. All the probabilities below are with respect to this experiment.

b. Let \( X_w \) denote the random variable that counts the number of nonzero codewords of weight at most \( w \) in \( C(a) \). Let \( E[X_w] \) denote the expected value of \( X_w \). Prove that for \( w < n \), we have

\[
\Pr\{X_w > 0\} \leq \frac{E[X_w]}{n}
\]

**Hint:** For prime \( n \), the \( n \) cyclic shifts of a vector \( x \in \mathbb{F}_2^n \) are all distinct, unless \( x = 0 \) or \( x = 1 \).

c. Let us write binary vectors of length \( 2n \) as \( (u \mid v) \) with \( u, v \in \mathbb{F}_2^n \). Furthermore, for every \( v \in \mathbb{F}_2^n \), let \( \langle v \rangle \) denote the smallest binary linear cyclic code of length \( n \) that contains \( v \). Prove that

\[
\Pr\{(u \mid v) \in C(a)\} = \begin{cases} 
1 & \text{if } u \in \langle v \rangle \\
\frac{1}{|\langle v \rangle|} & \text{otherwise}
\end{cases}
\]

**Hint:** Prove that if \( a \) is uniformly random in \( \mathbb{F}_2^n \), then \( vA \) is uniformly random in \( \langle v \rangle \).

Henceforth, let us further assume the prime \( n \) is such that \( 2 \) is primitive in \( \mathbb{Z}_n \), the prime field of integers modulo \( n \). In this case, the polynomial \( p(x) = x^{n-1} + x^{n-2} + \cdots + x + 1 \) is irreducible over \( \mathbb{F}_2 \) (you can assume this fact as a given, you do not need to prove this).

d. How many binary linear cyclic codes of length \( n \) are there? Describe all these codes.
e. Let \( V(2n, w) = \sum_{i=0}^{w} \binom{2n}{i} \) be the volume of a Hamming sphere of radius \( w \) in \( \mathbb{F}_2^{2n} \). Prove that for \( w < n \), we have
\[
\Pr\{ X_w > 0 \} < \frac{V(2n, w)}{n2^{n-1}}
\] (2)

Finally, use (2) to conclude that if \( n \) is a prime such that 2 is primitive in \( \mathbb{Z}_n \), there exist binary linear codes with parameters \((2n, n, d)\) whenever \( d \leq n \) and \( V(2n, d-1) \leq n2^{n-1} \).

Research Problem. The result proved in (2) implies that, under certain conditions on \( n \) and \( k \), there exist \((n, k, d)\) binary linear codes such that \( k \geq n - \log_2 V(n, d-1) + \log_2 n - 2 \). Can you improve this by replacing the \( \log_2 n \) term by any function that grows faster than \( \log_2 n \)?

Problem 5. (15 points)

Let \( \mathbb{F} \) denote the finite field \( \text{GF}(q) \), and let \( C \) be an \((n, k)\) linear code over \( \mathbb{F} \) with \( k \geq 1 \). As usual, we associate with a codeword \((c_0, c_1, \ldots, c_{n-1}) \in C\) the polynomial \( c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \) in \( \mathbb{F}[x] \). In this problem, it is known that the code \( C \) satisfies the following property:
\[
(c_0, c_1, \ldots, c_{n-1}) \in C \quad \Rightarrow \quad (-c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C
\] (3)

Note that this code \( C \) is not cyclic, since the first position is negated after the cyclic shift in (3). Nevertheless, you are asked to show that some of the properties of \( C \) are similar to those of cyclic codes.

a. Prove that there is a unique monic polynomial \( g(x) \) in \( C \) with the property that \( c(x) \in C \) if and only if \( \deg c(x) \leq n - 1 \) and \( g(x) \) divides \( c(x) \). Thus we say that \( g(x) \) generates the code \( C \).

b. Prove that \( \deg g(x) = n - k \).

c. Prove that \( g(x) \) divides the polynomial \( x^n + 1 \).

d. Prove that any polynomial \( g'(x) \in \mathbb{F}[x] \) that divides \( x^n + 1 \) generates a linear code \( C' \) of length \( n \) over \( \mathbb{F} \) that satisfies (3). Moreover, show that the dimension of \( C' \) is \( n - \deg g'(x) \).

Problem 6. (25 points)

In this problem, we let \( \mathbb{F} \) denote the finite field \( \text{GF}(p) \) and let \( \mathbb{K} \) denote its extension field \( \text{GF}(p^m) \) for some \( m \geq 2 \). The trace function from \( \mathbb{K} \) to \( \mathbb{F} \) is defined as follows. For all \( \alpha \in \mathbb{K} \),
\[
\text{Tr}(\alpha) \overset{\text{def}}{=} \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{m-1}}
\]

a. Prove that \( \text{Tr} \) is indeed a function from \( \mathbb{K} \) to \( \mathbb{F} \). In other words, show that \( \text{Tr}(\alpha) \) is in \( \mathbb{F} \) for all \( \alpha \in \mathbb{K} \). Further, prove that \( \text{Tr} \) is a surjective function. That is, show that for all \( a \in \mathbb{F} \), there exists an \( \alpha \in \mathbb{K} \) such that \( \text{Tr}(\alpha) = a \). Finally, show that \( \text{Tr} \) is an \( \mathbb{F} \)-linear function, namely prove that for all \( \alpha_1, \alpha_2 \in \mathbb{K} \) and \( a_1, a_2 \in \mathbb{F} \), we have \( \text{Tr}(a_1\alpha_1 + a_2\alpha_2) = a_1\text{Tr}(\alpha_1) + a_2\text{Tr}(\alpha_2) \).

b. Now let \( C \) be a linear code of length \( n \) over \( \mathbb{K} \) and let \( C^\perp \) denote its dual code. Consider the code \( \text{Tr}(C^\perp) = \{ (\text{Tr}(c_1), \text{Tr}(c_2), \ldots, \text{Tr}(c_n)) : (c_1, c_2, \ldots, c_n) \in C^\perp \} \). The subfield subcode of \( C \) is defined as \( C|_F = C \cap \mathbb{F}^n \). Prove that \( \text{Tr}(C^\perp) \) is the dual code of \( C|_F \).
Problem 7. (30 points)

Given binary vectors \( u = (u_1, u_2, \ldots, u_n) \) and \( v = (v_1, v_2, \ldots, v_n) \), we define their product componentwise, namely \( uv = (u_1v_1, u_2v_2, \ldots, u_nv_n) \), where \( u_1v_1, u_2v_2, \ldots, u_nv_n \) are computed in \( \text{GF}(2) \).

Given a binary code \( C \), consider the code \( C' \) spanned over \( \text{GF}(2) \) by the products of all the codewords of \( C \). Explicitly, \( C' \) is the smallest binary linear code that contains all vectors in the set \( \{uv : u, v \in C\} \).

Now suppose that \( C \) is a binary linear cyclic code of odd length \( n \) with generator polynomial \( g(x) \) and parity-check polynomial \( h(x) \). Let \( \alpha \) be a primitive \( n \)-th root of 1, and let \( H \) be the index set of zeros of the parity-check polynomial \( h(x) \). Thus \( h(\alpha^i) = 0 \) if and only if \( i \in H \) for \( i \in \{0, 1, \ldots, n-1\} \). Define

\[
H' \overset{\text{def}}{=} \{i + j \mod n : i, j \in H\}
\]

Show that \( H' \) is precisely the set of nonzeros of the code \( C' = \langle \{uv : u, v \in C\} \rangle \). In other words, prove that \( C' \) is the cyclic code of length \( n \) generated by the polynomial

\[
g'(x) = \frac{x^n - 1}{\prod_{i \in H'}(x - \alpha^i)}
\]

**Hint:** The previous problem may be helpful here.