ECE 259A: Solutions to the Midterm Exam

Problem 1.

For a codeword \( x \in C \), define its decoding region as the set of all vectors \( y \in \mathbb{F}_2^n \) such that \( D(y) = x \). Clearly, such decoding regions are disjoint, forming a partition of \( \mathbb{F}_2^n \). Now, assume to the contrary that

\[
D(x + e) = x \quad \text{whenever} \quad \text{wt}(e) \leq t + 1
\]

In other words, for all \( x \in C \), the Hamming sphere of radius \( t + 1 \) about \( x \) belongs to the decoding region of \( x \). Since decoding regions are disjoint, this implies that Hamming spheres of radius \( t + 1 \) about the codewords of \( C \) are disjoint. But if \( x \) and \( x' \) are codewords with \( d(x, x') = d \), then Hamming spheres of radius \( t + 1 \) about \( x \) and \( x' \) clearly intersect.

Here is another proof, which is somewhat shorter. Suppose that \( d = 2t + 2 \). Let \( x, x' \in C \) be two codewords at distance \( d = (t+1) + (t+1) \) from each other. Then there is a vector \( y \in \mathbb{F}_2^n \) such that

\[
y = x + e = x' + e' \quad \text{with} \quad \text{wt}(e) = \text{wt}(e') = t + 1
\]

If \( D(y) = x \) then the decoder fails to correct \( x' + e' \), while if \( D(y) = x' \) then \( D(x + e) \neq x \). In case \( d = 2t + 1 \), a similar argument applies.

Problem 2.

a. Let \( C = C_1 \otimes C_2 \). It follows from the definition of \( C_1 \otimes C_2 \) that the codewords of \( C \) take the form \( (u_1 G_1 | u_1 G_1 + u_2 G_2) \), where \( G_1 \) and \( G_2 \) are generator matrices for \( C_1 \) and \( C_2 \), respectively, \( u_1 \) takes values in \( \mathbb{F}_2^{k_1} \) and \( u_2 \) takes values in \( \mathbb{F}_2^{k_2} \). But the linear span of the rows of the matrix \( G \) is of precisely the same form. Moreover, it is easy to see that the rows of \( G \) are linearly independent. Hence \( G \) is a generator matrix for \( C \).

b. Let \( C = C_1 \otimes C_2 \) as before, and let \( v = (v_1 | v_2) \) be a binary vector of length \( 2n \), with \( v_1, v_2 \in \mathbb{F}_2^n \). Then \( v \in C \) if and only if \( v_1 \in C_1 \) and \( v_2 - v_1 = v_2 + v_1 \) belongs to \( C_2 \). Equivalently, \( v \in C \) if and only if \( H_1 v_1^t = 0 \) and \( H_2(v_1 + v_2)^t = 0 \). Equivalently, \( v \in C \) if and only if

\[
\begin{pmatrix}
H_1 & 0 \\
H_2 & H_2
\end{pmatrix}
\begin{pmatrix}
v_1 \\
v_2
\end{pmatrix} = 0
\]

c. Let \( c_1 \) be a codeword of weight \( d_1 \) in \( C_1 \) and let \( c_2 \) be a codeword of weight \( d_2 \) in \( C_2 \). Then both \( (c_1|c_1) \) and \( (0|c_2) \) are codewords of \( C_1 \otimes C_2 \). This implies that \( d \leq \min\{2d_1, d_2\} \). To prove the inequality in the opposite direction, consider a codeword \( v = (v_1 | v_2) \) in \( C_1 \otimes C_2 \) and suppose that \( \text{wt}(v) < d_2 \). Notice that \( v_1 + v_2 \) is a codeword of \( C_2 \), by construction. But we have

\[
\text{wt}(v_1 + v_2) = \text{wt}(v_1) + \text{wt}(v_2) - 2\text{wt}(v_1 \wedge v_2) \leq \text{wt}(v_1) + \text{wt}(v_2) = \text{wt}(v) < d_2
\]

This is only possible if \( v_1 + v_2 = 0 \), so that \( v_2 = v_1 \). But \( v_1 \) is a codeword of \( C_1 \). Hence, either \( v_1 = v_2 = 0 \) so that \( v = 0 \), or \( \text{wt}(v) = \text{wt}(v_1) + \text{wt}(v_2) = 2\text{wt}(v_1) \geq 2d_1 \).
d. We have \( n_1 = k_1 = 2 \) and \( d_1 = 1 \). The recursion \( C_m = C_{m-1} \oplus \{0,1\} \) doubles the length of the code and the number of codewords. Hence \( n_m = 2n_{m-1} \) and \( k_m = k_{m-1} + 1 \). It follows that

\[
n_m = 2^m \quad \text{and} \quad k_m = m + 1 \quad \text{for} \quad m = 1, 2, \ldots
\]

Clearly, the minimum distance of the code \( \{0,1\} \) of length \( n_{m-1} \) is \( 2^{m-1} \). Hence, part (e) of this problem implies that

\[
d_m = \min\{2d_{m-1}, 2^{m-1}\} = 2^{m-1} \quad \text{for} \quad m = 1, 2, \ldots
\]

where the second equality follows by induction on \( m \). For \( m = 3 \), we have \( n_3 = 8, k_3 = 4 \), and \( d_3 = 4 \). There is a unique binary linear code with these parameters — namely, the \((8,4,4)\) extended Hamming code.

e. We can prove this using, for example, the Plotkin bound. This bound asserts that for any \((n,k,d)\) binary linear code, we have

\[
d \leq \left\lfloor \frac{n2^{k-1}}{2^k - 1} \right\rfloor = \left\lfloor \frac{2^m}{2^{m+1} - 1} \right\rfloor = 2^{m-1}
\]

where the second equality follows by substituting the parameters \( n_m = 2^m \) and \( k_m = m + 1 \) from (1). Thus the code \( C_m \) achieves the Plotkin bound for all \( m \).

**Problem 3.**

This is a generalization of the sphere-packing bound. Let \( S_t \) denote the set of all bursts of length \( \ell \leq t \), and let \( x_1, x_2, \ldots, x_{2^k} \) be the codewords of \( C \). If \( D : F_2^n \to C \) is the decoder for \( C \) that corrects all bursts of length \( t \) or less, then

\[
D(x_i + e) = x_i \quad \text{whenever} \quad e \in S_t
\]

for all \( i = 1, 2, \ldots, 2^k \). It follows that the sets \( x_1 + S_t, x_2 + S_t, \ldots, x_{2^k} + S_t \) are disjoint, and therefore we have

\[
2^n \geq \left| \bigcup_{x \in C} (x + S_t) \right| = \sum_{x \in C} |x + S_t| = 2^k |S_t|
\]

as in the sphere-packing bound. In order to complete the proof, it remains to show that the cardinality of \( S_t \) is given by \( 1 + n + \sum_{\ell=2}^t (n-\ell+1)2^{\ell-2} \). Clearly, there is one “burst” of length zero, namely the vector \( 0 \), and \( n \) bursts of length 1. For a burst of length \( \ell \geq 2 \), there are \( n - \ell + 1 \) positions where the burst can start, and then \( 2^\ell - 2 \) different ways to complete the interior of the burst for each starting position.

**Problem 4.**

The \((24,12,8)\) binary Golay code \( C_{24} \) is an extended perfect code. As such, it is a quasiperfect code and has covering radius \( \rho = 4 \). Hence every vector in \( F_{2^{24}} \) is within distance \( \leq 4 \) from \( C_{24} \). On the other hand, if \( C_{24} \) were a subcode of the Wagner code \( C \), this would imply that at least some vectors in \( F_{2^{24}} \), namely those in \( C \setminus C_{24} \), are at distance \( \geq 6 \) from \( C_{24} \).