**Math 342 Problem set 9 (due 8/11/11)**

**The Parity Code**

Let \( p: \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) be the parity map \( p(v_1, \ldots, v_n) = \sum_{i=1}^{n} v_i \) where the addition is in \( \mathbb{F}_2 \).

1. Calculate the parity of the following bit vectors: 00110101, 01101011, 11011111, 00000000.

   - We saw in class that \( p \) is a linear transformation. By Lemma 100 of the notes, \( P = \{ v \in \mathbb{F}_2^n | p(v) = 0 \} \) is a subspace. Call it the *parity code*.

3. The *weight* of a vector is its number of non-zero entries, equivalently its Hamming distance from the zero vector. The weight of a linear code is the smallest weight of a non-zero vector. What are the possible weights of elements of \( P \)? Show that the code \( P \) has weight 2.

4. Say \( n = 8 \). Take the following 7-bit vectors and extend them to vectors in \( P \): 0011010, 0110101, 1101111, 0000000.

5. Show that for any 7-bit vector there is a unique 8-bit extension with even parity. Let the extension map be \( G: \mathbb{F}_2^7 \rightarrow \mathbb{F}_2^8 \). Write down the matrix for this map – the *generator matrix* of the code \( P \).

6. It is often said that parity can detect one error, but cannot correct any. Give an example of a bit vector \( v' \in \mathbb{F}_2^8 \) and two distinct vectors \( u, v \in P \) both at distance 1 from \( v' \). Explain why your example validates the saying.

**A non-linear code**

Let \( m \geq 1 \), and let \( n = 2^m \). Construct a subset \( C_m \subset \mathbb{F}_2^{2^m} \) of size \( 2(m+1) \) as follows: for every \( k, 0 \leq k \leq m \), divide the \( 2^m \) co-ordinates into \( 2^{m-k} \) consecutive blocks of length \( 2^k \) (so if \( k = m \) you get only one block, if \( k = m-1 \) you get two blocks each with half the co-ordinates, with \( k = 0 \) every block has size 1). Now fill the first block with all zeros, the second block with all ones and keep alternating. Put the resulting vector in \( C_m \), as well as the one obtained by the reverse procedure (i.e. by starting with 1). Here’s the example with \( m = 3, n = 8 \):

\[
\begin{align*}
  k=3: & 00000000, 11111111; \\
  k=2: & 00001111, 00011111; \\
  k=1: & 00110011, 11001100, 0: 01010101, 10101010.
\end{align*}
\]

7. For any distinct \( x, y \in C_m \), should that \( d_H(x, y) \geq \frac{n}{2} \).

   *Hint:* First work out the case \( m = 3 \) from the example, but you need to address the case of general \( m \).

8. How many errors can this code correct? How many errors can it detect?

9. For the case \( m = 3 \), find the nearest codeword to the received words 00010101, 11010000, 10101010 (prove that you found the right codeword!).

10. For \( m \geq 2 \), show that \( C_m \subset \mathbb{F}_2^n \) is *not* a subspace of \( \mathbb{F}_2^n \). Thus this code is not linear.