# Math 342 Problem set 9 (due 20/3/09)

## The Parity Code

Let $p\colon \mathbb{F}_2^n \to \mathbb{F}_2$ 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: $00110101, 01101011, 11011111, 00000000$.

2. Show that $p$ is a linear transformation. By Lemma 4.6 of the notes, $P = \{\underline{v} \in \mathbb{F}_2^n \mid p(\underline{v}) = 0\}$ is a subspace. Call it the *parity code*.

3. 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 $G\colon \mathbb{F}_2^7 \to \mathbb{F}_2^8$. 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 $\underline{v}' \in \mathbb{F}_2^8$ and *two* distinct vectors $\underline{u}, \underline{v} \in P$ both at distance 1 from $\underline{v}'$. 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 (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 so on. This gives an element of $C_m$, as does the reverse fillling (starting with 1). Here's the example with $m = 3$, $n = 8$:

$k = 3$: $00000000, 11111111$; $k = 2$: $00001111, 00001111$; $k = 1$: $00110011, 11001100$, $k = 0$: $01010101, 10101010$.

6. For any distinct $\underline{x}, \underline{y} \in C_m$, we have $d_H(\underline{x}, \underline{y}) \geq \frac{n}{2}$.
   *Hint*: Start with the case $m = 3$ as in the problem, but you need to address the case of general $m$.

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

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

9. Show that $C_m \subset \mathbb{F}_2^n$ is *not* a subspace of $\mathbb{F}_2^n$. Thus this code is not linear.