Problem set 13 - Introduction to ECC

out: 13/1/15
due: 9/2/15

This exercise contains a few basic questions on error correcting codes for those of you who haven't seen it before or want to refresh it. The hat puzzle may be of interest to everybody.

1. The Hamming $[7, 4]$ code is a subspace $C \subseteq \mathbb{F}_2^7$ generated b y the four basis vectors: $(1, 1, 1, 0, 0, 0, 0)$, $(1, 0, 0, 1, 1, 0, 0)$, $(0, 1, 0, 1, 0, 1, 0)$ and $(1, 1, 0, 1, 0, 0, 1)$.

   - Prove the code has distance 3.
   - Find an efficient encoding $E : \mathbb{F}_2^4 \to C$
   - Find an efficient decoding $D : \mathbb{F}_2^7 \to F_2^4$ that can correct any single error.

   The code has finite size, so efficient is not well defined. Yet..

2. Prove the $[7, 4]$ Hamming code is *perfect*, i.e., every word in $\mathbb{F}_2^7$ belongs to a unique ball of radius 1 around some codeword.

3. Prove the Hamming code is optimal, i.e., there are no $[7, 5, 3]_2$ or $[7, 4, 4]_2$ codes.

4. A hat puzzle (by Todd Ebert, PhD thesis, 1998, UC santa Barbara).

   There are N prisoners. The jailer decides to give them a test (and kill/free them accordingly). It has two stages:

   First stage: A random hat, either white or black, is placed on each of them. Each prisoner can see all hats except his own.

   Second stage: Each prisoner is taken to a separate cell and asked for the color of his hat. A prisoner can answer "Black", "White" or "don't know".

   If at least one prisoner guesses correctly and none guesses incorrectly, the prisoners win. Otherwise they lose. The prisoners can agree on a strategy before the test takes place.

   Show a strategy for $n = 7$ prisoners with winning probability 7/8.

5. (Continues the previous question, but requires more than the guided solution so far).

   - Show a strategy for $n = 127 = 2^7 - 1$ prisoners with winning probability 127/128.
   - Show the winning probability goes to one when the number of prisoners go to infinity.

6. (The Reed-Solomon code) Let q be a prime power and $\mathbb{F}_q$ the field with q elements $a_1, \ldots, a_q$. Let $1 \leq k \leq q$. Define the following code: For every polynomial $f \in \mathbb{F}_q[x]$ of degree less than k define the codeword $(f(a_1), \ldots, f(a_q)) \in \mathbb{F}_q^q$.

   Prove that this defines an $[q, k, n - k + 1]_q$ linear code.

7. (The Hadamard code) Let n be an integer. Define the following binary code: Suppose the elements of $\mathbb{F}_2^n$ are $a_1, \ldots, a_{2^n}$. For every linear function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ define the codeword $(f(a_1), \ldots, f(a_{2^n})) \in \mathbb{F}_2^{2^n}$.

   Prove that this defines an $[2^n, n, \frac{1}{2}]_2$ linear code.

8. (Concatenation) Suppose C_1 is an $[n_1, k_1, d_1]_q$ code for some q that is a power of 2 and C_2 is an $[n_2, k_2, d_2]_2$ code for $k_2 = \log_2 q$. We view C_2 as a linear mapping from $\mathbb{F}_q$ to $\mathbb{F}_2^{n_2}$ (How?). We define $\Phi : F_q^{n_1} \to F_2^{n_1 n_2}$ by $\Phi(x_1, \ldots, x_{n_1}) = (C_2(x_1), \ldots, C_2(x_{n_1}))$. We define the concatenated $C_1 \circ C_2$ to be $\{\Phi(c_1) \mid c_1 \in C_1\}$.

   - Prove that $C_1 \circ C_2$ is a $[n_1 n_2, k_1 k_2, d_1 d_2]_2$ linear code.
   - Let $k, \varepsilon > 0$. Concatenate the Reed-Solomon code with the Hadamard code to get an $[n = O((\frac{k}{\varepsilon})^2), k, \frac{1}{2} - \varepsilon]_2$ code.