Introduction to Coding Theory 89-662

Final Exam, Moed Aleph 2008

Exam instructions:

1. Closed book: no material is allowed
2. Answer all questions
3. Time: 2.5 hours
4. Good luck!

Question 1 (15 points): Describe a binary linear code with parameters \([n, \log_2(n + 1), \frac{n+1}{2}]\) (equivalently, with parameters \([2^k - 1, k, 2^k - 1]\)). Provide a full proof that your construction is a binary linear code and that it meets these parameters.

Question 2 (30 points): Prove the following. Let \(\delta > 0\) and \(\epsilon > 0\) be any constants and let \(d\) be any natural number. Then, for large enough \(k\) and \(n\) fulfilling \(\frac{k}{n} = 1 - H(d/n) - \delta\), there exist a pair of functions \((E, D)\) where \(E: \{0, 1\}^k \rightarrow \{0, 1\}^n\) and \(D: \{0, 1\}^n \rightarrow \{0, 1\}^k\) such that for every vector \(e \in \{0, 1\}^n\) with \(wt(e) \leq d\) it holds that

\[
\Pr_{x \leftarrow \{0,1\}^k} [D(E(x) + e) \neq x] \leq \epsilon
\]

In what way does the above differ from Shannon’s theorem?

Question 3 (20 points): Let \(C_i\) be an \([n, k_i, d_i]\) linear code over \(F_q\) for \(i = 1, 2\). Define

\[ C = \{(a + c, b + c, a + b + c) \mid a, b \in C_1, c \in C_2\} \]

1. Show that \(C\) is a \([3n, 2k_1 + k_2]\) linear code
2. Find a generator matrix \(G\) of \(C\), given generator matrices \(G_1\) and \(G_2\) of \(C_1\) and \(C_2\) respectively.
3. Find a parity-check matrix \(H\) of \(C\) given \(H_1\) and \(H_2\).
4. What can you say about the minimum distance of \(C\)?

Question 4 (20 points): Show that any coset of a linear perfect code is a perfect code. When is the resulting code linear and when is it not linear?

Question 5 (15 points): A code \(C\) is cyclic if for every codeword \(c \in C\) it holds that a cyclic shift of \(c\) is also in \(C\). That is, let \(c = c_1 \cdots c_{n-1} c_n\), then \(c_n c_1 \cdots c_{n-1} \in C\). Show that the Reed-Solomon code is cyclic.