Introduction to Coding Theory 89-662

Final Exam, Moed Aleph 2009

Exam instructions: The exam is closed book: no material is allowed! Answer all questions and *formally prove all of your answers.* The exam time is 2.5 hours.

Question 1 (25 points):

1. Formally define the notion of local decodability, and show that the Walsh-Hadamard code is 2-locally decodable with $\delta \leq \frac{1}{4}$.
2. Prove that if C is an $[n, k]$ code such that $C^{\perp}$ has distance $d \geq \ell+1$, then C is not $(\ell-1)$-locally decodable.
3. Prove that there exists a code of length n that is 1-locally decodable for $\delta < \frac{1}{2}$.

Question 2 (15 points): Show that if there exists a linear code C with parameters $[n, k, d]$ where d is *even*, then there exists a linear code C' with parameters $[n, k, d]$ such that *every* codeword has even weight.

Question 3 (30 points): Let C be a *binary linear code* and denote by $\overline{C}$ the code derived by taking the complement of all words in C.

1. Show that if the word $(1, \ldots, 1) \in C$ then $C = \overline{C}$.
2. Prove or refute: $\overline{C}$ is a linear code.
3. Prove or refute: $C \cup \overline{C}$ is a linear code.

Question 4 (30 points):

1. Let C be a linear $[n, k, d]$ MDS code over $\mathbb{F}_q$, and let $I \subseteq \{1, \ldots, n\}$ be a subset of exactly k coordinates. Denote $I = \{i_1, \ldots, i_k\}$. Show that for all $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_q$ there exists a **unique** codeword $c \in C$ such that $c_{i_j} = \alpha_j$ (where $c = (c_1, \ldots, c_n)$).

   Hint: Define a linear transformation projecting the code onto the subset of k coordinates. Then, use the theorem from linear algebra stating that if $T : U \to V$ is a linear transformation from a vector subspace U to a vector subspace V, then $\mathsf{dim}(Im(T)) + \mathsf{dim}(Ker(T)) = \mathsf{dim}(U)$, where

   $$Im(T) = \{v \in V \mid \exists u \in U \text{ s.t. } T(u) = v\}$$

   and

   $$Ker(T) = \{u \in U \text{ s.t. } T(u) = 0\}$$

2. Use the above to calculate (with a proof) the number of codewords with weight *exactly* $n-k+1$ in any MDS code over a field $\mathbb{F}_q$ of exactly q elements.

   Hint: Look at the case of $\alpha_1, \ldots, \alpha_k$ where exactly one $\alpha_j \neq 0$ and consider what the other coordinates could be.