Introduction to Coding Theory 89-662

Final Exam, Moed Bet 2008

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

Question 1 (20 points): Prove the Gilbert-Varshamov lower bound: Let $n, k$ and $d$ be natural numbers such that $2 \leq d \leq n$ and $1 \leq k \leq n$. If $V_q^{n-1}(d-2) < q^{n-k}$ then there exists a linear code $[n, k]$ over $F_q$ with distance at least $d$.

Question 2 (25 points): The heaviest codeword problem is defined as follows: Upon receiving a parity check matrix $H$ that fully defines a binary linear code $C$, find the codeword $c \in C$ with the maximum weight (i.e., find $c$ such that $wt(c) \geq wt(c')$ for all $c' \in C$). Give an efficient (polynomial-time) algorithm for this problem or show that it is NP-complete.

Question 3 (25 points):
1. Show that there exists no binary linear code with parameters $[2^m, 2^m - m, 3]$ for any $m \geq 2$.
2. Let $C$ be a binary linear code with parameters $[2^m, k, 4]$ for some $m \geq 2$. Show that $k \leq 2^m - m - 1$.
3. Let $\delta$ and $R$ be such that $R = 1 - H(\delta)$. Is it possible to construct a code with rate $R = \frac{k}{n}$ that can correct more than $\delta n$ errors?

You can use any of the bounds that we learned in class (but you must state exactly what you are using and what it states).

Question 4 (30 points): A burst error of length $t$ has the property that all errors are within distance $t$ from each other. More formally, a vector $e \in F^n_2$ is a burst error of length $t$ if there exist $i < j$ such that $e_1 = \cdots = e_{i-1} = 0$, $e_{j+1} = \cdots = e_{n} = 0$ and $j - i < t$.

Let $C$ be a linear code $[n, k]$ over $F_q$ such that there exists a decoder for $C$ that corrects every burst of length $t$ or less.

1. Show that in every nonzero codeword $c \in C$, the locations $i$ and $j$ of the first and last nonzero entries in $c$ must satisfy $j - i \geq 2t$ (i.e., they must be at least $2t$ far apart).
2. Show that all of the burst errors of length $t$ of a codeword $c$ lie in distinct cosets of $C$. 
3. Show that $n - k \geq 2t$.

Hint: recall that if there are $d$ linear dependent columns of the parity check matrix, then there exists a codeword of weight $d$. Combine this with item (1) of this question to conclude that no consecutive $2t$ columns can be linearly dependent. Now consider what it would mean if $n - k < 2t$. 