CSE522/Math581EB Coding Theory **Fall 2001**

Final Exam: December 11

Please answer as much of the following as you can, but don't kill yourself trying to get absolutely everything. There are 7 questions on 2 pages. As we agreed, you may use your own notes and the online scribe notes (including the algebra notes) from this class, and the references listed on the syllabus, but no other resources. Please write clear and concise answers, and leave them in our mailbox in the Math building by Thursday, December 13 at 5pm. If you have questions on the exam, we will answer them by email assuming they are received before 5pm Wednesday. Please also sign the statement at the end of the exam indicating that you have consulted only the allowed notes and references, and include the signed exam with your answers. Good luck!

1 The binary erasure channel capacity

Consider the *binary erasure channel* in which bits may be erased, but not flipped. Formally, $\Sigma_{in} = \{0,1\}$, $\Sigma_{out} = \{0,1,?\}$ and $P_{i,i} = 1-p$, $P_{i,?} = p$ for $i = 0,1$. Prove that this channel has capacity $1-p$; i.e., prove that

- for all $R < 1-p$ there exist a pair of functions $E : \{0,1\}^k \to \Sigma_{in}^{k/R}$ and $D : \Sigma_{out}^{k/R} \to \{0,1\}^k$, with the following property: If we pick a message uniformly at random from $\{0,1\}^k$, encode it with E, send the result through the channel and decode the result, then we recover the original message with probability $1-o(1)$. Formally,
$$\mathbf{P}[D(\mathcal{C}(E(x))) = x] = 1 - o(1).$$
- for all $R > 1-p$ and all functions $E : \{0,1\}^k \to \Sigma_{in}^{k/R}$ and $D : \Sigma_{out}^{k/R} \to \{0,1\}^k$, it holds that if we pick a message at random from $\{0,1\}^k$, encode it with E, send the result through the channel and decode the result, then we recover the original message with probability $o(1)$. Formally,
$$\mathbf{P}[D(\mathcal{C}(E(x))) = x] = o(1).$$

2 Errors and erasures

Express the number of errors e and erasures s an $[n,k,d]_q$ code can *simultaneously* tolerate (and still be unambiguously decodable) in terms of the parameters of the code. For Reed-Solomon codes, describe how to adapt the algorithms for unique-decoding and list-decoding to handle a mixture of e errors and s erasures. Express the mixtures of errors and erasures (e and s) each of the adapted algorithms can handle in terms of the parameters of the code.

3 Duality of Hamming and Hadamard codes

The *punctured Hadamard code* is a $[2^k - 1, k, 2^{k-1} - 1]_2$ code given by the following encoding function:

$$E(m_1, m_2, \ldots m_k) = \left(\sum_{i=1}^{k} m_i x_i \right)_{(x_1, x_2, \ldots x_k) \in \mathbb{F}_2^k \setminus \{\vec{0}\}}.$$

Show that the dual of this code is the Hamming code.

4 Vectors in $\mathbb{R}^n$

In the following problem, $x_1, x_2, \ldots x_m$ are m unit vectors in $\mathbb{R}^n$. Recall that $\langle x_i, x_j \rangle$ denotes the inner product of x_i and x_j.

- Suppose that for all $i \neq j$, we have $\langle x_i, x_j \rangle \leq -\epsilon$, for some $\epsilon > 0$. Prove that $m \leq 1 + \frac{1}{\epsilon}$.
- For $\epsilon > 0$, prove that there *exist* $m = c_1 2^{c_2 n}$ unit vectors $x_1, x_2, \ldots, x_m$ in $\mathbb{R}^n$ such that $\langle x_i, x_j \rangle < \epsilon$, where $c_1 > 0$ and $c_2 > 0$ depend on ϵ (but not on n).

5 k-wise independence

A collection of n-bit binary strings $S = \{s_1, \ldots, s_m\}$ has the *k-wise independence* property, if for all $i_1 < \ldots < i_k$ and all $r \in \{0,1\}^k$ it holds that

$$\mathbf{P}[(s(i_1), \ldots, s(i_k)) = r] = 2^{-k},$$

where s is chosen uniformly at random from S, and $s(i)$ denotes the i-th bit of string s. Prove that the collection of codewords of a linear binary code $\mathcal{C}$ has the k-wise independence property if and only if the distance of the dual code, $\Delta(\mathcal{C}^\perp)$, satisfies $\Delta(\mathcal{C}^\perp) \geq k$.

6 Design a code

Describe an $[16, 10, d]_2$ code with d maximum. Be sure to prove that the distance is indeed d and that no larger d is possible.

7 A polynomial code

Given integer parameters d and $\ell_1, \ell_2, \ldots, \ell_d$ (with $\ell_i < q$ for all i), define the q-ary code $\mathcal{C}$ as follows:

$$\mathcal{C} = \left\{ (f(x_1, x_2, \ldots x_d))_{(x_1, x_2, \ldots x_d) \in \mathbb{F}_q^d} : f \text{ is a } d\text{-variate polynomial with } x_i\text{-degree at most } \ell_i \text{ for all } i \right\}.$$

Give the blocklength n, the message length k, and the distance d of this code. Be sure to argue that your distance is exact and not just a lower bound on the actual distance.

By signing here I certify that I have consulted only the allowed notes and references, and no other resources or people. Signature: _____