CSE522/Math581EB Coding Theory **Fall 2001**

Exercise 2: October 24

The exercises are for bonus points. Try to solve the ones which you find interesting.

2.1 Duality

- Consider the following slight modification of the $[2^k, k, 2^{k-1}]_2$ Hadamard code given by the encoding function:
$$E(m_1, m_2, \ldots m_k) = \left(\sum_{i=1}^{k} m_i x_i\right)_{(x_1,x_2,\ldots x_k)\in\mathcal{F}_2^k\setminus\{\vec{0}\}}.$$
Show that the dual of this code is the Hamming code.
- Recall that a Maximum Distance Seperable (MDS) code is a code that meets the Singleton Bound. Show that the dual of a MDS code is MDS.

2.2 Justesen Codes

- Show that for all $\epsilon > 0$, at least a $1-\epsilon$ fraction of subspaces in the Wozencraft ensemble are $[n, n/2, (H^{-1}(1/2)-\epsilon)n]_2$ codes.
- Let $E_1, E_2, \ldots, E_{n_1}$ be mappings from $\mathcal{F}_q^{k_2}$ into $F_q^{n_2}$ whose images are linear subspaces of $\mathcal{F}_q^{n_2}$, let C_1 be an $[n_1, k_1, d_1]_{q^{k_2}}$ code, and let π be the natural mapping from $\mathcal{F}_{q^{k_2}}$ to the vectorspace $\mathcal{F}_q^{k_2}$. Show that if
$$\Pr_i[E_i \text{ is a } [n_2, k_2, d_2]_q \text{ code}] \geq 1-\epsilon$$
then
$$C = \{((E_1(\pi(x_1)), E_2(\pi(x_2)), \ldots, E_{n_1}(\pi(x_{n_1}))) : (x_1, x_2, \ldots x_{n_1}) \in C_1\}$$
is an $[n_1 n_2, k_1 k_2, (d_1 - \epsilon n_1)d_2]_q$ code.
- Show that applying the above operation to Reed-Solomon codes (using the Wozencraft ensemble for the inner codes) yields a family of $[n, n/4, (1/2)(H^{-1}(1/2)-\epsilon)n]_2$ codes (called *Justesen Codes*).
- Generalize the above construction to produce a family of codes with rate $c/2$ and relative distance $(1/2)(H^{-1}(1-1/c)-\epsilon)$ for every integer $c \geq 2$ and $\epsilon > 0$. (Hint: generalize the Wozencraft ensemble, and use the new ensemble in the same concatenation-type operation with Reed-Solomon codes).

2.3 Secret Sharing

We are looking for a probabilistic protocol for sharing a secret $a \in \mathcal{F}_q$ among n parties, in such a way that any set of $< k$ parties can infer no information on the secret, and and set of $\geq k$ parties can recover the secret. Formally a *secret sharing protocol* is a randomized function $f : \mathcal{F}_q \times [n] \to \mathcal{F}_q$ (in other words $f : \mathcal{F}_q \times [n] \times \Omega \to \mathcal{F}_q$, where Ω is some probability space) such that

- For every set $S \subset [n]$ of size $|S| < k$, any vector $a_1, \ldots, a_{|S|}$ and any $a \in \mathcal{F}$,

$$\mathbf{P}[\forall i \in S, f(i, a) = a_i] = q^{-1}.$$

- For every set $S \subset [n]$ of size $|S| \geq k$, and any vector $a_1, \ldots, a_{|S|}$,

$$\#\{a : \mathbf{P}[\forall i \in S, f(i, a) = a_i] > 0\} \leq 1.$$

(both probabilities are taken over Ω). Let $C = [n + 1, k, n - k + 2]_q$ be a maximum-distance-separable (MDS) code. For each a and $1 \leq i \leq n$, let $f(i, a) = a_i$ where $(a_0, \ldots, a_n)$ is chosen uniformly among all the codewords such that a_0 is the secret a. Prove that f is a secret sharing protocol. This construction is originally due to Shamir where he used Reed-Solomon codes.