CSE522/Math581EB Coding Theory **Fall 2001**

Exercise 3: November 13

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

3.1 Comparing bounds

Draw all the bound that we've seen so far for binary codes, and compare them:

- Singleton: $R + \delta \leq 1$,
- Hamming: $R + H(\delta/2) \leq 1$,
- Plotkin: $R + 2\delta \leq 1$,
- Elias-Bassylago: $R + H(1/2(1 - \sqrt{1 - 2\delta})) \leq 1$,
- GV: Codes exit if $R + H(\delta) \leq 1$.

3.2 q-ary Johnson and Elias-Bassylago bounds

- Prove that an $(n, k, \delta n)_q$ code is $(\tau n - 1, (q-1)n)$ error correcting for

$$\tau = \frac{q-1}{q}\left(1 - \sqrt{1 - \frac{q}{q-1}\delta}\right).$$

  Use the following map $\widehat{\ }$ from F_q to $\mathbb{R}^q$ which maps $a \in F_q$ to the vector $e_a - (1/q, \ldots, 1/q)$, where e_a is the a'th unit vector, and extend this map to vectors.

- Deduce the asymptotic Elias-Bassalygo bound.
- Prove Plotkin bound: an $(n, k, d)_q$ code satisfies

$$k \leq n - \frac{qd}{q-1} + \log_q\left(\frac{q^2}{q-1}d\right).$$

  Hints:

  - By restriction it suffice to prove the claim when $d \geq n(q-1)/q$.
  - Let C' be obtained from C by removing all codewords which begin with the least occuring coordinate α.
  - If $x_1, \ldots, x_m$ are the codewords of C', consider the vectors $\overline{x_1}, \ldots, \overline{x_m}$ and $\overline{y} = \overline{(\alpha, 0, \ldots, 0)}$.

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

Prove that for every $\epsilon > 0$, there exists an exponential number m of unit vectors in $\mathbb{R}^n$, $x_1, \ldots, x_m$ such that for all i, j it holds that $< x_i, x_j > \leq \epsilon$.

3.4 Discrete Fourier transforms

Consider the space of all functions $f : \{0,1\}^n \to \mathbb{R}$ with the inner product, $< f, g >= 2^{-n} \sum_{x \in \{0,1\}^n} f(x)g(x)$. Let $U_y(x) = (-1)^{<y,x>}$.

- Prove that $U_y \times U_z = U_{y+z}$, and conclude that $\{U_y\}_{y \in \{0,1\}^n}$ is an orthogonal basis for this set of functions.
- Consider a random walk X_t on $\{0,1\}^n$, so that $\mathbf{P}[X_{t+1} = x + e_i | X_t = x] = 1/n$ for all i. This defines a $2^n \times 2^n$ matrix: $(\mathbf{P}[X_{t+1} = v | X_t = w])_{v,w \in \{0,1\}^n}$. Find the eigenvalues and eigenvectors of this matrix.
- Suppose Alice holds a sequence of i.i.d. bits $b_1, \ldots, b_n$ and Bob holds a noisy version of these bits $c_1, \ldots, c_n$: it holds that $\mathbf{P}[b_i = c_i] = 1 - \epsilon$, independently for all i. Alice and Bob want to toss the same coin using the bits b_i and c_i. So they want functions $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ such that $\mathbf{P}[f(b_i) = 1] = \mathbf{P}[g(c_i) = 1] = 1/2$, and $\mathbf{P}[f(b_i) = g(c_i)]$ is maximized.

  What is the best they can do?

3.5 List-decoding of Reed-Muller codes

Generalize the Guruswami-Sudan list-decoding algorithm to Reed-Muller codes. For rate R Reed-Solomon codes, the GS algorithm decodes from relative agreement $\tau \geq \sqrt{R}$. What agreement does the generalized algorithm require in the Reed-Muller case? Is this comparable performance?