Homework Set #5

Due 17 November 2009, 6 pm, in INR036

Problem 1 (There are almost no perfect codes)

Let $\mathcal{C}$ be a linear binary *perfect code* consisting of binary sequences of length N. Assume that for the rate of code $\mathcal{C}$ we have $R_{\mathcal{C}} > 0$ where $R_{\mathcal{C}} \triangleq \frac{\log_2 |\mathcal{C}|}{N}$.

In this problem we would like to show that useful perfect codes do not exist (here, "useful" means having large block-length N, and rate close neither to 0 nor 1).

Let $\alpha \in (1/3, 1/2)$ be a parameter. In this problem we will show that there is no large perfect code that is αN-error-correcting.

Remember that a code is *perfect αN-error-correcting code* if the set of αN-spheres centered on the codewords of the code fill the Hamming space without overlapping.

Let us suppose that such a code has been found.

(a) Knowing that the code is αN-error-correcting code, what can we say about its minimum distance?

(b) Let us focus just on three codewords of this code. (Remember that the code has rate $R_{\mathcal{C}} > 0$, so it should have $2^{NR_{\mathcal{C}}}$ codewords which is a large number if N grows.) Without loss of generality, we choose one of the codewords to be the all-zero codeword and define the other two to have overlaps with it as shown in the following

$$\begin{aligned}
c_0 &= 000000 \quad 0000000000000 \quad 000000 \quad 0000\\
c_1 &= 111111 \quad 1111111111111 \quad 000000 \quad 0000\\
c_2 &= \underbrace{000000}_{uN} \quad \underbrace{1111111111111}_{vN} \quad \underbrace{111111}_{wN} \quad \underbrace{0000}_{xN}
\end{aligned}$$

where $u + v + w + x = 1$.

Use the distance property of code $\mathcal{C}$ to show that it cannot even have three codewords c_0, c_1, and c_2 (let alone $2^{NR_{\mathcal{C}}}$ codewords).

Problem 2 (Reed-Solomon Codes)

(a) Show that if H is the parity check matrix of a code of length n, then the code has minimum distance at least d if every $d-1$ columns of H are linearly independent.

(b) Consider a linear code defined over a finite field $\mathbb{F}$ with the parity check matrix

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{bmatrix}_{(n-k)\times n},$$

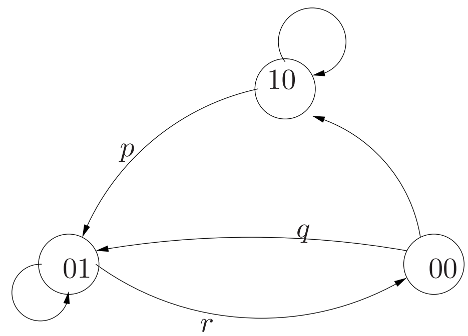

Figure 1: Problem 3

where $k \leq n \leq |\mathbb{F}|$ and $\alpha_i \in \mathbb{F}$ such that $\alpha_i \neq \alpha_j$ if $i \neq j$. A matrix with this form called a *Vandermonde matrix*. It can be shown that the parity check matrix of a Reed-Solomon code is in fact a Vandermonde matrix.

Show that every $n-k$ columns of H are linearly independent.
Hint: For a square $n \times n$ Vandermonde matrix

$$V = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{bmatrix}_{n\times n},$$

we have

$$\det(V) = \prod_{1\leq i<j\leq n} (\alpha_j - \alpha_i).$$

(c) From part (b) and the Singelton bound conclude that the Reed-Solomon codes are maximum distance seperable codes.

Problem 3

We have a source that produces a sequence of bits with the following two properties:

- A "1" is always followed by a "0",
- No more than three "0"s come in a row.

Assume that this source can be modeled by a first order Markov chain as shown in Fig 1

(a) Choose p, q, and r such that the entropy rate of this Markov process is maximized.

(b) Construct a 2-state FSM that receives the source outputs as its input and maximally compresses it.

(c) Is this finite state machine uniquely decodable?

(d) Is this finite state machine information lossless?

Problem 4 (Lempel-Ziv Algorithm is Asymptotically Optimal)

Consider a first order Markov process $X_0, X_1, \cdots$ with the stationary distribution $[p_0, p_1, \cdots, p_m]$, where p_i denotes the stationary distribution of being in state $i \in \{0, \cdots, m\}$. Assume that the Markov process is in state 0. We define T_0 as the number of steps it takes for the process to return to state 0 again.

(a) Calculate $\mathbb{E}T_0$ for a 2-state Markov process in terms of p_0 and p_1.

(b) Define s_i as the expected number of visits to state i before returning from 0 to state 0. i.e.,

$$s_i = \mathbb{E}_0[\sum_{n\geq 1} 1_{\{X_n=i\}} 1_{\{n\leq T_0\}}],$$

where the index 0 of $\mathbb{E}_0$ shows the fact that we are considering the chain from the time it has left state 0. Show that

$$p_i = \frac{s_i}{\sum_j s_j}$$

and conclude that $p_0 = \frac{1}{\mathbb{E}(T_0)}$.

(c) Take the Markov process $X_0, X_1, \cdots$ and form the following extended Markov process from it: $X_0^{n-1}, X_1^n, X_2^{n+1}, \cdots$. How many steps does it take on average for this extended process to return for the first time to the state $00\cdots 0$ (after it left it).

In the LZ77 algorithm with infinite-length sliding window, in order to encode the block $x_0 x_1 \cdots x_{n-1}$, one finds and communicates the last time the n symbols have been seen. Call it $R_n(x_0 x_1 \cdots x_{n-1})$. If we denote the length of description of $R_n(X_0 X_1 \cdots X_{n-1})$ by $l(X_0 X_1 \cdots X_{n-1})$, it can easily be shown that

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{E} l(X_0 X_1 \cdots, X_{n-1}) = H(\mathcal{X})$$

and this is the basic idea of the proof of optimality of LZ77 algorithm. Refer to Homework 5 of last year's homeworks for details of proof.