TUTORIAL XII

1 Homework 7

1. Give an example of a nontrivial (i.e., $C \neq \{0\}$) linear code C such that $C^\perp = C$.

2. By constructing the columns of a parity check matrix in a greedy fashion, show that there exists a binary linear code $[n, k, d]_2$ provided that

$$2^{n-k} > 1 + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2}. \tag{1}$$

   This is a small improvement compared to the general Gilbert-Varshamov bound. In particular, it is tight for the $[7, 4, 3]_2$ Hamming code.

3. (Bonus question) The Hadamard code has a nice property that it can be locally decoded. Let $x \in C_{Had,r}$ and suppose you are interested only in the i-th bit x_i of x ($i \in \{0, 1, \ldots, 2^r - 1\}$). The challenge is that you only have access to y such that $\Delta(x, y) \leq \frac{n}{10}$ and you would like to look only at a few bits of y. Show that by querying only 2 well-chosen positions (the choice will involve some randomisation) of y, you can determine x_i correctly with probability $4/5$ (the probability here is over the choice of the queries, in particular x, y and i are fixed). *Hint:* You might want to query y at the position labelled by $u \in \{0, 1\}^r$ at random and the position $u + e_i$ where $e_i \in \{0, 1\}^r$ has a 1 at position i and 0 elsewhere.

2 Homework 8

We use the notation introduced in class for Reed-Solomon codes.

1. Consider a $[4, 2]_5$ Reed-Solomon code over $\mathbb{F}_5$ with $\alpha_i = 2^{i-1}$. Compute a generator matrix and a parity check matrix for this code (you may use an exercise from the tutorial for that, but you can also do it without). What is the minimum distance of this code? Check that your answer is consistent with the parity check matrix.

2. A well-studied family of codes is called cyclic codes. Their defining property is that if $(c_0, \ldots, c_{n-1}) \in C$ then $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. Show that if β is a generator of $\mathbb{F}_q^*$ and $\alpha_i = \beta^{i-1}$ with $n = q - 1$, then the $[n, k]_q$ Reed-Solomon code is cyclic.

3. Prove that any $[n, k]_q$ Reed-Solomon code C has the following property: for any $\mathbf{v} \in \mathbb{F}_q^k$ and any subset $S \subseteq \{1, \ldots, n\}$ of size k, there exists $\mathbf{c} \in C$ such that $c_S = \mathbf{v}$ where $\mathbf{c}_S \in \mathbb{F}_q^k$ corresponds to the vector $\mathbf{c}$ projected on the coordinates labelled by S.

3 Secret Sharing

Secret sharing is a cryptographic problem of splitting a *secret* among several participants/players in such a way that the secret cannot be reconstructed unless a sufficient number of *shares* are combined. More formally, an (ℓ, m)-secret sharing scheme takes as input a set of n players $P_1, \ldots, P_n$ and a secret $s \in \mathcal{X}$ to be shared among them. The output is a set of shares $s_1, \ldots, s_n$ where s_i corresponds to P_i. The scheme must satisfy the following properties.

1. For all $A \subseteq \{1, \ldots, n\}$ with $|A| \geq m$, $\{P_i\}_{i \in A}$ can recover s from $\{s_i\}_{i \in A}$.

2. For all $B \subseteq \{1, \ldots, n\}$ with $|B| < \ell$, $\{P_i\}_{i \in B}$ *cannot* recover s from $\{s_i\}_{i \in B}$. By *cannot recover*, we mean that s is information theoretically hidden to all parties in B or equivalently, s is equally likely to take on any value in $\mathcal{X}$.

Shamir's $(\ell, \ell+1)$-secret sharing scheme: Let $\mathcal{X} = \mathbb{F}_q$ with $q \geq n$ and $1 \leq \ell \leq n-1$. Pick a random polynomial $f(x) \in \mathbb{F}_q[X]$ of degree $\leq \ell$ such that $f(0) = s$. Choose distinct $\alpha_i \in \mathbb{F}_q$ and set $s_i = (f(\alpha_i), \alpha_i)$.

1. Show that the properties 1 and 2 hold for this scheme.

Linear codes and secret sharing: Consider $\mathcal{X} = \mathbb{F}_q$ with $q \geq n$. Let C be an $[n+1, k, d]_q$-code and $C^\perp$ be its dual $[n+1, n+1-k, d^\perp]_q$-code. Consider the following secret sharing scheme: pick a random codeword $\mathbf{c} = (c_0, c_1, \ldots, c_n) \in C$ and set $s = c_0$ and $s_i = c_i$ for $i \in [1, n]$.

1. Argue that the scheme is correct (that is, any $s \in \mathbb{F}_q$ corresponds to some codeword).
2. Show that it is an (ℓ, m)-secret sharing scheme with $\ell \leq d^\perp - 2$ and $m \geq n - d + 2$.

Correspondence to Reed-Solomon?

1. Show that $RS[n, k]^\perp = RS[n, n-k]$.
2. Can you represent Shamir's $(\ell, \ell+1)$-scheme as a linear code-based scheme with $C = RS[n', k']_q$ for some n', k'?