TUTORIAL XIII

1 Homework 2

1. Let $A_q(n,d)$ be the largest k such that a code over alphabet $\{1,\dots,q\}$ of block length n, dimension k and minimum distance d exists (recall that this corresponds to the notation $(n,k,d)_q$). Determine $A_2(3,d)$ for all integers $d \geq 1$.

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. A well-studied family of codes is called cyclic codes. Their defining property is that if $(c_0,\dots,c_{n-1}) \in C$ then $(c_{n-1},c_0,\dots,c_{n-2}) \in C$. 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.

4. The Hadamard code has a nice property that it can be locally decoded. Let $C_{Had,r} : \{0,1\}^r \to \{0,1\}^{2^r}$ be the encoding function of the Hadamard code. Suppose you are interested only in the i-th bit x_i of the message $x \in \{0,1\}^r$. The challenge is that you only have access to $y \in \{0,1\}^{2^r}$ such that $\Delta(C_{Had,r}(x), y) \leq \frac{2^r}{10}$ 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 randomization) 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 $e_i \in \{0,1\}^r$ is the binary representation of i

2 Reed-Solomon codes

Consider the Reed-Solomon code over a field $\mathbb{F}_q$ and block length $n = q-1$ defined as

$$RS[n,k]_q = \{(p(1), p(\alpha), \dots, p(\alpha^{n-1})) \mid p \in \mathbb{F}_q[X] \text{ has degree } \leq k-1\}$$

where α is a generator of the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$

1. Show that for any $k \in [|1; n-1|]$, we have

$$\sum_{i=0}^{n-1} \alpha^{ki} = 0$$

2. Prove that

$$RS[n,k]_q \subseteq \left\{ (c_0,\dots,c_{n-1}) \in \mathbb{F}_q^n \mid \forall l \in [|1; n-k|], c(\alpha^l) = 0, \text{ where } c(X) = \sum_{i=0}^{n-1} c_i X^i \right\}$$

3. Prove that the following matrix is invertible, and compute its inverse.

$$W(\alpha) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \dots & \alpha^{2n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-1} & \dots & \alpha^{(n-1)(n-1)} \end{pmatrix}$$

4. Prove that

$$RS[n,k]_q \supseteq \left\{ (c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n \mid \forall l \in [|1; n-k|], c(\alpha^l) = 0, \text{ where } c(X) = \sum_{i=0}^{n-1} c_i X^i \right\}$$

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 $P_1, \dots, P_n$ and a secret $s \in \mathcal{X}$ to be shared among them. The output is a set of shares $s_1, \dots, s_n$ where s_i corresponds to P_i. The scheme must satisfy the following properties.

1. For all $A \subseteq \{1, \dots, n\}$ with $|A| \geq m$, $\{P_i\}_{i \in A}$ can recover s from $\{s_i\}_{i \in A}$.
2. For all $B \subseteq \{1, \dots, n\}$ with $|B| \leq \ell$, $\{P_i\}_{i \in B}$ *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 $\mathbf{c} = (c_0, c_1, \dots, c_n) \in C$ such that $c_0 = s$, and set $s_i = c_i$ 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 for all $\ell \leq d^\perp - 2$ 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'?