# TUTORIAL XII

## 1 Codes Achieving the Gilbert-Varshamov Bound

The purpose of this exercise is to use the probabilistic method to show that a random linear code lies on the Gilbert-Varshamov bound, with high probability.

1. Given a non-zero vector $\mathbf{m} \in \mathbb{F}_q^k$ and a uniformly random $k \times n$ matrix $\mathbf{G}$ over $\mathbb{F}_q$, show that the vector $\mathbf{mG}$ is uniformly distributed over $\mathbb{F}_q^n$.
2. Let $k = (1 - H_q(\delta) - \varepsilon)n$, with $\delta = d/n$. Show that there exists a $k \times n$ matrix $\mathbf{G}$ such that

   $$\text{for every } \mathbf{m} \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}, wt(\mathbf{mG}) \geq d$$

   where $wt(\mathbf{m})$ is the Hamming weight of the vector $\mathbf{m}$.
3. Show that $\mathbf{G}$ has full rank (i.e., it has dimension at least $k = (1 - H_q(\delta) - \varepsilon)n$)

## 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 $\alpha$ 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 $(\ell, m)$-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 $(\ell, m)$-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 $n', k'$?