18.408 Topics in Theoretical Computer Science Fall 2022
Problem Set 1

1. Write down a generating matrix for the following codes:

   (a) Reed-Solomon code over $\mathbb{F}_q$ with $n = q$ and degree d.

   (b) The Hadamard code H_n.

2. In this problem, we will prove the Schwarz-Zippel Lemma for large fields, stating that for $q \geqslant d$, if $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ is a polynomial of total degree at most d not identically 0, then $\Pr_{x \in \mathbb{F}_q^n}[f(x) = 0] \leqslant \frac{d}{q}$.

   (a) Show that the statement of the Schwarz-Zippel Lemma holds for $n = 1$.

   (b) Prove the Schwarz-Zippel Lemma (hint: you may use induction on n). Conclude that the relative distance of $\mathrm{RM}_{m,d,q}$ is at least $1 - \frac{d}{q}$.

   (c) Show an example of a total degree d polynomial f for which the lemma is tight, i.e.

$$\Pr_{x \in \mathbb{F}_q^n}[f(x) = 0] = \frac{d}{q}.$$

3. Let $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ be a polynomial whose total degree is greater than d and at most $q-1$. Show that there is a line $\ell(t)$, i.e. $\ell\colon \mathbb{F}_q \to \mathbb{F}_q^m$ of the form $\ell(t) = a + tb$ for some $a, b \in \mathbb{F}_q^m$, such that the univariate polynomial $f|_\ell\colon \mathbb{F}_q \to \mathbb{F}_q$ has degree greater than d.

4. In this problem, we will analyze the Hadamard code shown in class. For each $v \in \mathbb{F}_2^n$, we define the function $h_v\colon \mathbb{F}_2^n \to \mathbb{F}_2$ by $h_v(x) = \langle v, x \rangle$, so that $H_n = \left\{ (h_v(x))_{x \in \mathbb{F}_2^n} \quad v \in \mathbb{F}_2^n \quad \right.$ is the Hadamard code.

   (a) Show that for all $v \neq \vec{0}$, $\Pr_{x \in \mathbb{F}_2^n}[h_v(x) = 1] = \frac{1}{2}$. Deduce that the relative distance of H_n is $\frac{1}{2}$.

   (b) Show that the rate of H_n is $\frac{n}{2^n}$.

5. The Quadratic Hadamard code is a variant of the Hadamard code defined above. For a vector $u, v \in \mathbb{F}_2^n$, we define $u \otimes v \in \mathbb{F}_2^{n \times n}$ as $(u \otimes v)_{i,j} = u_i v_j$. The Quadratic Hadamard code is then defined as

$$\mathrm{QH}_n = \left\{ (h_{v \otimes v}(x))_{x \in \mathbb{F}_2^{n \times n}} \quad v \in \mathbb{F}_2^n \right\}.$$

   (a) Show that the relative distance of QH_n is $\frac{1}{2}$ and that the rate is $\frac{n}{2^{n^2}}$.

   (b) Show that for all $x, y, u, v \in \mathbb{F}_2^n$ it holds that $\langle x \otimes y, z \otimes w \rangle = \langle x, z \rangle \langle y, w \rangle$.

6. (*) Show that there exist absolute constants $r \in \mathbb{N}$ and $\varepsilon_0 > 0$ such that the QH_n is $(r, O(\varepsilon), \varepsilon)$ locally testable for all $0 < \varepsilon \leqslant \varepsilon_0$.