Tutorial XIV: More on Codes

Homework

1 Constructing good codes

The objective of this problem is to explicitly construct a family of binary linear codes with dimension $k = \Omega(n)$ and minimum distance $d = \Omega(n)$.

1. We will define a family of codes with blocklength $2k$ and dimension k. Recall that we can view the set $\{0,1\}^k$ as a field $\mathbb{F}_{2^k}$ (the only thing needed for this problem is that it is a field). More formally, we assume that $\sigma : \mathbb{F}_2^k \to \mathbb{F}_{2^k}$ is a bijection and satisfies the properties $\sigma(0) = 0$, $\sigma(x+y) = \sigma(x) + \sigma(y)$ for any $x, y \in \mathbb{F}_2^k$ and also $\sigma^{-1}(u+v) = \sigma^{-1}(u) + \sigma^{-1}(v)$ for $u, v \in \mathbb{F}_{2^k}$. For every $\alpha \in \mathbb{F}_{2^k}$ nonzero, let $C_\alpha : \{0,1\}^k \to \{0,1\}^{2k}$ be defined by $C_\alpha(x) = (x, \sigma^{-1}(\alpha \cdot \sigma(x)))$. Here $\cdot$ denotes the multiplication in the field $\mathbb{F}_{2^k}$.
   (a) Show that for any α, C_α is a linear code. For $\alpha = 1$ (the unit for the field $\mathbb{F}_{2^k}$), what is the minimum distance of C_1?
   (b) Show that for $\alpha \neq \beta$, $C_\alpha \cap C_\beta = \{0\}$.
   (c) Show that the fraction of codes C_α with minimum distance $\leq d-1$ is at most $\frac{\sum_{i=1}^{d-1} \binom{2k}{i}}{2^k - 1}$. Recall that for large enough k, $\sum_{i=0}^{d-1} \binom{2k}{i} \leq 2^{2kH_2(\frac{d}{2k})}$. Let $\epsilon > 0$ and $d = H_2^{-1}(\frac{1}{2} - \frac{\epsilon}{2})2k$. Show that the fraction of codes with minimum distance $\geq d$ is at least $1 - 2^{-\epsilon k}$.
2. The problem in this family is that we do not know which value of α leads to a good code. Let RS be a Reed Solomon $[2^k - 1, 2^{k-1}, 2^{k-1}]_{2^k}$ code.
   (a) Give a generator matrix for the code RS.
   (b) Consider the concatenation of the code RS and use as inner codes the codes C_α, i.e., the block labeled α is encoded using the code C_α. The resulting code is a binary code. What is the blocklength and the dimension of the resulting code? Give a lower bound on the minimum distance that is linear in the blocklength.

2 Hardness on Linear Codes

Definition 2.1. *Given a generator $\mathcal{G}$ for a linear code C with a minimum distance r, and a received word y. The output of MLD is 1 if there exists a codeword $c \in C$ such that $\Delta(c, y) \leq r$, and 0 otherwise.*

Problem 2.2. *Let $G = (V, E)$ be a graph, and let $U_x, U_y \subseteq V$. Show that $\partial_E(U_x) \triangle \partial_E(U_y) = \partial_E(U_x \triangle U_y)$.*

Here, $\triangle$ denotes the symmetric difference between two sets, and $\partial_E(U) = \{(u,v) \in E : u \in U, v \notin U\}$ for some $U \subseteq V$.

Problem 2.3. *Show that MLD is NP-complete.*

Problem 2.4. *There exists a family of codes $C_1, C_2, \ldots$ with $C_i \in \{0,1\}^i$ for all $i \geq 1$ such that if there is a polynomial time algorithm solving MLD for all codes in the family, then $P = NP$.*