CS 599B: Math for TCS, Spring 2022

Exercise Set 9

Due: 10:00PM, Tuesday April 19, 2022 on Gradescope.

Instructions. You're encouraged to discuss these problems with other students as you solve them, but the written solutions you hand in must be in your own words. Don't worry about polishing the presentation of your solutions; these are primarily intended to keep you thinking about and engaged with the material.

Problem 1 (Codes vs. pseudorandom distributions)**.**

(a) An $(n, k, d)_q$ code is *maximum distance separable (MDS)* if $d = n - k + 1$. Note that Reed-Solomon codes are MDS. Show that if $C \subseteq \mathbb{F}_q^n$ is an MDS $[n, k]_q$-linear code, then the uniform distribution over C is k-wise independent.

(b) Let C be an $[n, k]_2$ code such that every nonzero codeword $v \in C$ has Hamming weight $wt(v) \in [(1 - \varepsilon)n/2, (1 + \varepsilon)n/2]$. Let $G \in \mathbb{F}^{k \times n}$ be a generator matrix for C. Show that the uniform distribution over the columns of G is an $O(\varepsilon)$-biased distribution over $\mathbb{F}_2^k$ with support size n.

Problem 2 (Systematic codes)**.** A systematic code is one for which the message appears as the first k symbols of the corresponding codeword. A generator matrix for a systematic $[n, k]_q$ linear code takes the form $(I_k|A)$ where I_k is the $k \times k$ identity matrix and A is some $k \times (n - k)$ matrix.

(a) Explain why if C is an $[n, k]_q$ linear code, then there exists an isomorphic systematic code C'. (Two vector spaces are isomorphic if there is a linear bijection between them.)

(b) Given a set of messages A, describe how to encode a message $x \in \mathbb{F}_q^k$ as a polynomial $p_x(\alpha)$ such that the resulting variant of a Reed-Solomon code is a sysematic code. That is, for every $x \in \mathbb{F}_q^k$, we should have $x = (p_x(\alpha_1), \ldots, p_x(\alpha_k))$.