Soham Chatterjee
Email: sohamc@cmi.ac.in
Course: Algorithmic Coding Theory

Takehome Endsem
Roll: BMC202175
Date: November 24, 2023

Problem 1 List Decoding of RS Codes

In class we described a list deoding algorithm for RS codes that decoded from $n-2(k-1)\sqrt{n}$ errors where n is the block length of the code and k its dimension. In this problem we want you to improve this bound to correct $n-\sqrt{2kn}$ errors.
Recall that the algorithm from class involved two steps:

(1) Find a non-zero polynomial $Q(x,y)$ of degree at most $2\sqrt{n}$ such that $Q(\alpha_i,\beta_i)=0$ for every $i\in[n]$.

(2) Factor this polynomial and include P in the output if $y-P(x)$ divides $Q(x,y)$ and $|\{i,[n]\mid P(\alpha_i)=\beta_i\}|\geq t$

Our modification will be obtained by carefully picking a set of monomials $M\subseteq\{x^iy^i\mid i,j\geq 0\}$ and requiring that Q be only supported on the monomials of M. (I.e. if $Q(x,y)=\sum\limits_{i,j}c_{i,j}x^iy^j$ and $c_{ij}\neq 0$ for some i,j then $x^iy^j\in M$.)
Describe a set of monomials M that allows you to solve the list-decoding algorithm above with $t=\sqrt{2kn}$. (No need to write the details of all remaining steps.)

Solution:

□

Problem 2

Consider the following algorithm for converting errors to erasures in an expander code:
Given a codeword $c\in\mathbb{F}_2^n$ and a corrupted word $w\in\mathbb{F}_q^n$ with $\textsc{errors}:=\{i\in[n]\mid w_i\neq c_i\}$ satisfying $|\textsc{errors}|\leq rn$, let U be the set of constraints left unsatisfied by the assignment w. Initially the algorithm sets $\textsc{erase}=\emptyset$ and $\textsc{unhappy}=U$ ($\textsc{unhappy}$ for unHappy constraints). Then while there exists a variable $i\in[n]\setminus\textsc{erase}$ with more than 1/3rd of neighbors in $\textsc{unhappy}$, it sets $\textsc{erase}=\textsc{erase}\cup\{i\}$ and $\textsc{unhappy}=\textsc{unhappy}\cup N(i)$. When no such i exists it stops and outputs $\textsc{erase}$.
Prove that if the expander code is based on a (c,d)-regular (γ,δ)-expander with $\gamma>\frac{2c}{3}$ then for some $\tau>0$ the alforithm's output satisfies

(1) $|\textsc{erase}|<\delta n$

(2) $\textsc{errors}\subseteq\textsc{erase}$

Solution:

□

Problem 3

Fix a matrix $A\in\mathbb{F}_q^{m\times n}$ for $m\leq n$. Suppose you have oracle access to A: that is there is a magic box, M, so that in time $O(q)$, $M(i,j)$ returns $A_{i,j}$. Give a randomized streaming algorithm that takes in an input $y\in\mathbb{F}_q^n$ (in a straming fashionm so it sees y_q, then y_2, then y_3 and so on until y_m), and outputs its best guess about whether or not $Ay=0$.

Solution:

□

Problem 4 (Local) Decodability of Reed-Muller Codes:

Recall that $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$. Show that there exist polynomials $p_1, \ldots, p_m \in \mathbb{F}_{q^m}[X]$ of degree q^{m-1} such that the map $p : \mathbb{F}_{q^m} \to \left(\mathbb{F}_{q^m}\right)^m$ given by $p(x) = (p_1(x), \ldots, p_m(x))$ has image $\mathbb{F}_q^m$ and p is a bijection from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q^m$. Use this map to conclude that the Reed-Muller Code $RM(q, m, r)$ is a subcode of the reed solomon code obtained by evaluating polynomials of degree at most rq^{m-1} over all of $\mathbb{F}_{q^m}$

(a) Use this bijection to give a polynomial times (non-local) decoding algorithm for correcting Reed-Muller codes with $r < q$ up to half their minimum distance.

(b) Show how to correct $\epsilon_0 \left(1 - \frac{r}{q}\right)$ fraction of errors using a reduction to Reed-Solomon decoding with an $O(q)$ query algorithm. Your ϵ_0 should be an absolute constant.

Solution:

□