Algorithmic Coding Theory - Amit Kumar Sinhababu

Scribed: Soham Chatterjee

sohamchatterjee999@gmail.com
Website: sohamch08.github.io

2023

Contents

Chapter 1

Locally Decodable Codes

1.1 Introduction

Definition 1.1.1 (Locally Decodable Codes)**.** *A q-ary code $C : \mathbb{F}_q^k \to \mathbb{F}_q^N$ is said to be (r, δ, ϵ)-locally decodable if there exists a randomized decoding algorithm $\mathcal{A}$ such that*

1. *For all $\overline{x} \in \mathbb{F}_q^k$, $i \in [k]$ and all vectors $\overline{y} \in \mathbb{F}_q^N$ such that $\Delta(C(\overline{x}), \overline{y}) \leq \delta$:*

$$Pr[\mathcal{A}^{\overline{y}}(i) = \overline{x}(i)] \geq 1 - \epsilon$$

   where the probability is taken over the random coin tosses of the alforithm $\mathcal{A}$

2. *$\mathcal{A}$ makes at most r queries to $\boldsymbol{y}$*

We would like to have LDCs that for a given message length k and algphabet size q have small values of r, N and ϵ and a large value of δ. The exact value of r is not very important provided that it is muxh smaller than k. Similarly the exact value of $\epsilon < \frac{1}{2}$ is not the important since one can easily amplify ϵ to be close to 0 by running the decoding procedure few times and taking a majority vote.

A locally decodable code allows to probabilistically decode any coordinate of a message by probing only few coordinates of its corrupted encoding. A stronger property that is desirable in certain application is that of local correctability allowing to efficiently recover not only coordinates of the message but also arbitrary coordinates of the encoding.

Definition 1.1.2 (Locally Correctable Codes)**.** *A q-ary code C in the space $\mathbb{F}_q^N$ is (r, δ, ϵ)-locally decodable if there exists a randomized decoding algorithm $\mathcal{A}$ such that*

1. *For all $\overline{c} \in C$, $i \in [N]$ and all vectors $\overline{y} \in \mathbb{F}_q^N$ such that $\Delta(\overline{c}, \overline{y}) \leq \delta$:*

$$Pr[\mathcal{A}^{\overline{y}}(i) = \overline{c}(i)] \geq 1 - \epsilon$$

   where the probability is taken over the random coin tosses of the alforithm $\mathcal{A}$

2. *$\mathcal{A}$ makes at most r queries to $\boldsymbol{y}$*

Lemma 1.1.1. *Let q be a prime power. Suppose $C \subseteq \mathbb{F}_q^N$ is a (r, δ, ϵ)-locally correctable code that is a linear subspace; then there exists a $q-$ary (r, δ, ϵ)-locally decodable code C' encoding messages of length $\dim C$ to codewords of length N*

Proof: Let $I \subseteq [N]$ be a set of $k := \dim C$ coordinates of C whose values uniquely determine an element of C. For $\boldsymbol{c} \in C$ let $\boldsymbol{c}|_I \in \mathbb{F}_q^k$ denote the restriction of $\boldsymbol{c}$ to coordinates of I. Given a message $\boldsymbol{x} \in \mathbb{F}_q^k$ we define $C'(\boldsymbol{x})$ to be the unique element $\boldsymbol{c} \in C$ such that $\boldsymbol{c}|_I = \boldsymbol{x}$. Now C' is a (r, δ, ϵ)-locally decodable code ■

1.2 Reed Muller Locally Decodable Codes

The key idea begind early locally decodable codes is that of polynomial interpolation. Local decodability is achived through reliance on the rich structure of short lical dependencies between such evaluations at multiple points. We cibsider three local correctors for RM codes of increasing level of sophistication.

1.2.1 Basic Decoding on Lines

To recover the value of a degree d polynomial $f \in \mathbb{F}_q[x_1 \ldots, x_n]$ at a point $\boldsymbol{w} \in \mathbb{F}_q^n$ it shoots a random affine line through $\boldsymbol{w}$ and then relies on the local dependency between the calies of f at some $d+1$ points along the line.