# 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

References for this topic are [Yek12]

**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 $(r, \delta, \epsilon)$-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 $LDC$s that for a given message length $k$ and algphabet size $q$ have small values of $r$, $N$ and $\epsilon$ and a large value of $\delta$. 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 $\epsilon$ 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 $(r, \delta, \epsilon)$-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 $(r, \delta, \epsilon)$-locally correctable code that is a linear subspace; then there exists a $q-ary$ $(r, \delta, \epsilon)$-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 $(r, \delta, \epsilon)$-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.

# Chapter 2

# Multiplicity Code

References for this topic are [KSY11], [Kop15]
**Notation:**

- For a vector $\bar{i} = \langle i_1, i_2, \ldots, i_m \rangle$ of non-negative integers its ***weight*** denoted $wt(\bar{i}) := \sum_{j=1}^{m} i_j$
- $\mathbb{F}[\overline{X}] = \mathbb{F}[X_1, \ldots, X_m]$
- For a vector of non-negative integers $\bar{i}$, $\overline{X}^{\bar{i}} := \prod_{j=1}^{m} X_j^{i_j}$

## 2.1 Hasse Derivative

**Definition 2.1.1** ((Hasse) Derivative). *For $P(\overline{X}) \in \mathbb{F}[\overline{X}]$ and non-negative vector $\bar{i}$, the $\bar{i}$th (Hasse) derivative of $P$ denoted $P^{(\bar{i})}(\overline{X})$ is the coefficient of $\overline{Z}^{\bar{i}}$ in the polynomial $\widetilde{P}(\overline{X}, \overline{Z}) \stackrel{\Delta}{=} P(\overline{X} + \overline{Z}) \in \mathbb{F}[\overline{X}, \overline{Z}]$. Thus*

$$P(\overline{X} + \overline{Z}) = \sum_{\bar{i}} P^{(\bar{i})}(\overline{X}) \overline{Z}^{\bar{i}}$$

### 2.1.1 Basic Properties of Hasse Derivatives

**Proposition 2.1.1** ( [HKT08],[Dvi+09]). *Let $P(\overline{X}), Q(\overline{X}) \in \mathbb{F}[\overline{X}]$ and let $\bar{i}, \bar{j}$ be vectors of nennegative integers. Then:*

1. $P^{(\bar{i})}(\overline{X}) + Q^{(\bar{i})}(\overline{X}) = (P+Q)^{(\bar{i})}(\overline{X})$
2. $(P \cdot Q)^{(\bar{i})}(\overline{X}) = \sum_{0 \leq \bar{e} \leq \bar{i}} P^{(\bar{e})}(\overline{X}) \cdot Q^{(\bar{i}-\bar{e})}(\overline{X})$
3. $\left(P^{(\bar{i})}\right)^{(\bar{j})}(\overline{X}) = \binom{\bar{i}+\bar{j}}{\bar{i}} P^{(\bar{i}+\bar{j})}(\overline{X})$

***Proof*:**

- 
- 

- We will expand $P(\overline{X}+\overline{Z}+\overline{W})$ in two ways.

$$P(\overline{X}+(\overline{Z}+\overline{W}))=\sum_{\bar{k}}P^{(\bar{k})}(\overline{X})(\overline{Z}+\overline{W})^{\bar{k}}=\sum_{\bar{k}}P^{(\bar{k})}(\overline{X})\sum_{\bar{i}+\bar{j}=\bar{k}}\binom{\bar{k}}{\bar{i}}\overline{Z}^{\bar{j}}\overline{W}^{\bar{i}}=\sum_{\bar{i},\bar{j}}P^{(\bar{i}+\bar{j})}(\overline{X})\binom{\bar{i}+\bar{j}}{\bar{i}}\overline{Z}^{\bar{j}}\overline{W}^{\bar{i}}$$

$$P((\overline{X}+\overline{Z})+\overline{W})=\sum_{\bar{i}}P^{(\bar{i})}(\overline{X}+\overline{Z})\overline{W}^{\bar{i}}=\sum_{\bar{i}}\sum_{\bar{j}}\left(P^{(\bar{i})}\right)^{(\bar{j})}(\overline{X})\overline{Z}^{\bar{j}}\overline{W}^{\bar{i}}$$

Hence comparing the coefficients of $\overline{Z}^{\bar{j}}\overline{W}^{\bar{i}}$ we obtain $\left(P^{(\bar{i})}\right)^{(\bar{j})}(\overline{X})=\binom{\bar{i}+\bar{j}}{\bar{i}}P^{(\bar{i}+\bar{j})}(\overline{X})$

■

## 2.2 Multiplicity

Now we will define the notion of the multiplicity of a polynomial.

**Definition 2.2.1** (Multiplicity). *For $P(\overline{X})\in\mathbb{F}[\overline{X}]$ and $\bar{a}\in\mathbb{F}^m$ the multiplicity of $P$ at $\bar{a}\in\mathbb{F}^m$ denoted $mult(P,\bar{a})$ id the largest integer $M$ such that for every non-negative vector $\bar{i}$ with $wt(\bar{i})<M$ we have $P^{(\bar{i})}(\bar{a})=0$ (If $M$ may be taken arbitrarily large we set $mult(P,\bar{a})=\infty$)*

Note that $mult(P,\bar{a})\geq 0$ for all $\bar{a}\in\mathbb{F}^m$.

### 2.2.1 Basic Properties of Multiplicity

We now translate some of the properties of the Hasse derivative into properties of the multiplicities. We will discuss the properties of multiplicities from [Dvi+09]

**Proposition 2.2.1.** *If $P(\overline{X})\in\mathbb{F}[\overline{X}]$ and $\bar{a}\in\mathbb{F}^m$ are such that $mult(O,\bar{a})=n$ then $mult(P^{(\bar{i})},\bar{a})\geq n-wt(\bar{i})$*

***Proof:*** By assumption, for any $\bar{k}$ with $wt(\bar{k})<n$, we have $P^{(\bar{k})}(\bar{a})=0$. Now take any $\bar{j}$ such that $wt(\bar{j})<n-wt(\bar{i})$. Using Theorem 2.1.1 (3) we have

$$\left(P^{(\bar{i})}\right)^{(\bar{j})}(\bar{a})=\binom{\bar{i}+\bar{j}}{\bar{i}}P^{(\bar{i}+\bar{j})}(\bar{a})$$

Since $wt(\bar{i}+\bar{j})=wt(\bar{i})+wt(\bar{j})<m$, hence $\left(P^{(\bar{i})}\right)^{(\bar{j})}(\bar{a})=0$. Thus $mult(P^{(\bar{i})},\bar{a})\geq n-wt(\bar{i})$ ■

We will now discuss the behavior of multiplicites under composition of polynomial tuples. Let $\overline{X}=(X_1,X_2,\ldots,X_m)$ and $\overline{Y}=(Y_1,Y_2,\ldots,Y_n)$ be formal variables. Let $P(\overline{X})=(P_1(\overline{X}),\ldots,P_k(\overline{X}))\in\mathbb{F}[\overline{X}]^k$ and also $Q(\overline{Y})=(Q_1(\overline{Y}),\ldots,Q_m(\overline{Y}))\in\mathbb{F}[\overline{Y}]^m$. We define the composition polynomial $P\circ Q(\overline{Y})\in\mathbb{F}[\overline{Y}]^k$ to be the polynomial $P(Q_1(\overline{Y}),\ldots,Q_m(\overline{Y}))$. In this situation we have the following proposition:

**Proposition 2.2.2.** *Let $P(\overline{X}),Q(\overline{Y})$ be defined as above. Then for any $\bar{a}\in\mathbb{F}^n$*

$$mult(P\circ Q,\bar{a})\geq mult(P,Q(\bar{a}))\cdot mult(Q-Q(\bar{a}),\bar{a})$$

*In particular, since $mult(Q-Q(\bar{a}),\bar{a})\geq 1$, we have $mult(P\circ Q,\bar{a})\geq mult(P,Q(\bar{a}))$*

***Proof:*** Let $m_1 = mult(P, Q(\bar{a}))$ and $m_2 = (Q - Q(\bar{a}), \bar{a})$. Clearly $m_2 > 0$. If $m_1 = 0$ the result is obvious. Now assume $m_1 > 0$ (so that $P(Q(\bar{a})) = 0$). Now

$$\begin{aligned}
P(Q(\bar{a}+\overline{Z})) &= P\left(Q(\bar{a}) + \sum_{\bar{i}\neq 0} Q^{(\bar{i})}(\bar{a})\overline{Z}^{\bar{i}}\right) \\
&= P\left(Q(\bar{a}) + \sum_{wt(\bar{i})\geq m_2} Q^{(\bar{i})}(\bar{a})\overline{Z}^{\bar{i}}\right) && [\text{Since } mult(Q - Q(\bar{a}), \bar{a}) = m_2 > 0] \\
&= P(Q(\bar{a}) + h(\overline{Z})) && \left[\text{where } h(\overline{Z}) = \sum_{wt(\bar{i})\geq m_2} Q^{(\bar{i})}(\bar{a})\overline{Z}^{\bar{i}}\right] \\
&= P(Q(\bar{a})) + \sum_{\bar{j}\neq 0} P^{(\bar{j})}(Q(\bar{a}))h(\overline{Z})^{\bar{j}} \\
&= \sum_{wt(\bar{j})\geq m_1} P^{(\bar{j})}(Q(\bar{a}))h(\overline{Z})^{\bar{j}} && [\text{since } mult(P, Q(\bar{a})) = m_1 > 0]
\end{aligned}$$

Since each monomial $\overline{Z}^{\bar{i}}$ appearing in $h$ has $wt(\bar{i}) \geq m_2$ and each occurrence of $h(\overline{Z})$ in $P(Q(\bar{a}+\overline{Z}))$ is raised to the power $\bar{j}$ with $wt(\bar{j}) \geq m_1$ we conclude that $P(Q(\bar{a}+\overline{Z}))$ is of the form $\sum_{wt(\bar{k})\geq m_1\cdot m_2} c_{\bar{k}}\overline{Z}^{\bar{k}}$. This shows that $(P \circ Q)^{(\bar{k})}(\bar{a}) = 0$ for each $\bar{k}$ with $wt(\bar{k}) < m_1 \cdot m_2$. And hence we get the result. ■

**Corollary 2.2.3.** *Let $P(\overline{X}) \in \mathbb{F}[\overline{X}]$. Let $\bar{a}, \bar{b} \in \mathbb{F}^m$. Let $P_{\bar{a},\bar{b}}(T)$ be the polynomial $P(\bar{a} + T \cdot \bar{b}) \in \mathbb{F}[T]$. Then for any $t \in \mathbb{F}$,*

$$mult(P_{\bar{a},\bar{b}}, t) \geq mult(P, \bar{a} + t \cdot \bar{b})$$

***Proof:*** Let $Q(T) = \bar{a} + T \cdot \bar{b} \in \mathbb{F}[T]^m$. Applying Proposition 2.2.2 and $Q(T)$ we get the desired claim. ■

### 2.2.2 Strengthening of the Schwartz-Zippel Lemma

**Theorem 2.2.4** (Schwartz-Zippel Lemma)**.** *Let $P(\overline{X}) \in \mathbb{F}[\overline{X}]$ be a non-zero polynomial with degree $d$. Let $S$ be a finite subset of $\mathbb{F}$ with at least $d$ elements in it. If we take $\bar{a} \in S^m$ independently and uniformly at random then*

$$Pr_{\bar{a}\in S^m}[P(\bar{a}) = 0] \leq \frac{d}{|S|}$$

We will prove the strengthening of this lemma using $mult$.

**Theorem 2.2.5** ([Dvi+09])**.** *Let $P(\overline{X}) \in \mathbb{F}[\overline{X}]$ be a*

Now we need a bound on the number of points that a low-degree polynomial can vanish on with high multiplicity. We state a basic bound on the total number of zeroes (counting multiplicity) that a polynomial can have on a product set $S^m$.

**Theorem 2.2.6** ([Dvi+09])**.** *Let $P(\overline{X}) \in \mathbb{F}[\overline{X}]$ be a nonzero polynomial of total degree at most $d$. Then for any finite $S \subseteq \mathbb{F}$,*

$$\sum_{\bar{a}\in S^m} mult(P, \bar{a}) \leq d \cdot |S|^{m-1}$$

*In particular, for any integer $s > 0$*

$$Pr_{\overline{a} \in S^m}[mult(P, \overline{a}) \geq s] \leq \frac{d}{s|S|}$$

***Proof:*** We will prove this by induction on $m$. For the base case when $m = 1$ we will first show that if $mult(P, a) = k$ then $(X - a)^k$ divides $P(X)$. To see this, note that by definition of multiplicity, we have that $P(a + Z) = \sum_i P^{(i)}(a) Z^i$ and $P^{(i)}(a) = 0$ for all $i < k$ we conclude that $Z^k$ divides $P(a + Z)$. And thus $(X - a)^k$ divides $P(X)$. It follows that $\sum_{a \in S} mult(P, a)$ is at most the degree of $P$.

Now suppose $m > 1$. Let

$$P(\overline{X}) = \sum_{j=0}^{t} P_j(X_1, \ldots, X_{m-1}) X_m^j$$

where $0 \leq t \leq d$, $P_t(X_1, \ldots, X_{m-1}) \neq 0$ and $\deg(P_j) \leq d - j$. For any $a_1, \ldots, a_{n-1} \in S$ let $m_{a_1, \ldots, a_{n-1}} = mult(P_t, (a_1, \ldots, a_{n-1}))$. We will show that

$$\sum_{a_n \in S} mult(P, \overline{a}) \leq m_{a_1, \ldots, a_{n-1}} \cdot |S| + t$$

■

**Corollary 2.2.7.** *Let $P(\overline{X}) \in \mathbb{F}_q[\overline{X}]$ be a polynomial of total degree at most $d$. If*

$$\sum_{\overline{a} \in \mathbb{F}_q^m} mult(P, \overline{a}) > d \cdot q^{m-1}$$

*then $P(\overline{X}) = 0$*

# Chapter 3

# References


[HKT08] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic Curves over a Finite Field*. Princeton: Princeton University Press, 2008. ISBN: 9781400847419. DOI: doi:10.1515/9781400847419. URL: https://doi.org/10.1515/9781400847419.

[Dvi+09] Zeev Dvir et al. "Extensions to the Method of Multiplicities, with Applications to Kakeya Sets and Mergers". In: *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. 2009, pp. 181–190. DOI: 10.1109/FOCS.2009.40.

[KSY11] Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. "High-Rate Codes with Sublinear-Time Decoding". In: vol. 61. June 2011, pp. 167–176. DOI: 10.1145/1993636.1993660.

[Yek12] Sergey Yekhanin. "Locally Decodable Codes". In: *Foundations and Trends in Theoretical Computer Science* 6.3 (2012), pp. 139–255. ISSN: 1551-305X. DOI: 10.1561/0400000030. URL: http://dx.doi.org/10.1561/0400000030.

[Kop15] Swastik Kopparty. "Some remarks on multiplicity codes". In: *CoRR* abs/1505.07547 (2015). arXiv: 1505.07547. URL: http://arxiv.org/abs/1505.07547.