

## TABLE OF CONTENTS

	Page
List of Figures . . . . .	v
List of Tables . . . . .	vi
Chapter 1: Introduction . . . . .	1
1.1 Basics of Error Correcting Codes . . . . .	2
1.1.1 Historical Background and Modeling the Channel Noise . . . . .	3
1.2 List Decoding . . . . .	4
1.2.1 Going Beyond Half the Distance Bound . . . . .	6
1.2.2 Why is List Decoding Any Good ? . . . . .	8
1.2.3 The Challenge of List Decoding (and What Was Already Known) . . . . .	9
1.3 Property Testing of Error Correcting Codes . . . . .	9
1.3.1 A Brief History of Property Testing of Codes . . . . .	10
1.4 Contributions of This Thesis . . . . .	11
1.4.1 List Decoding . . . . .	11
1.4.2 Property Testing . . . . .	13
1.4.3 Organization of the Thesis . . . . .	14
Chapter 2: Preliminaries . . . . .	15
2.1 The Basics . . . . .	15
2.1.1 Basic Definitions for Codes . . . . .	15
2.1.2 Code Families . . . . .	16
2.1.3 Linear Codes . . . . .	17
2.2 Preliminaries and Definitions Related to List Decoding . . . . .	18
2.2.1 Rate vs. List decodability . . . . .	19
2.2.2 Results Related to the $q$ -ary Entropy Function . . . . .	22
2.3 Definitions Related to Property Testing of Codes . . . . .	25
2.4 Common Families of Codes . . . . .	26

2.4.1	Reed-Solomon Codes . . . . .	26
2.4.2	Reed-Muller Codes . . . . .	27
2.5	Basic Finite Field Algebra . . . . .	27
Chapter 3:	List Decoding of Folded Reed-Solomon Codes . . . . .	29
3.1	Introduction . . . . .	29
3.2	Folded Reed-Solomon Codes . . . . .	30
3.2.1	Description of Folded Reed-Solomon Codes . . . . .	31
3.2.2	Why Might Folding Help? . . . . .	32
3.2.3	Relation to Parvaresh Vardy Codes . . . . .	33
3.3	Problem Statement and Informal Description of the Algorithms . . . . .	34
3.4	Trivariate Interpolation Based Decoding . . . . .	36
3.4.1	Facts about Trivariate Interpolation . . . . .	37
3.4.2	Using Trivariate Interpolation for Folded RS Codes . . . . .	38
3.4.3	Root-finding Step . . . . .	40
3.5	Codes Approaching List Decoding Capacity . . . . .	42
3.6	Extension to List Recovery . . . . .	47
3.7	Bibliographic Notes and Open Questions . . . . .	49
Chapter 4:	Results via Code Concatenation . . . . .	52
4.1	Introduction . . . . .	52
4.1.1	Code Concatenation and List Recovery . . . . .	53
4.2	Capacity-Achieving Codes over Smaller Alphabets . . . . .	54
4.3	Binary Codes List Decodable up to the Zyablov Bound . . . . .	57
4.4	Unique Decoding of a Random Ensemble of Binary Codes . . . . .	58
4.5	List Decoding up to the Blokh Zyablov Bound . . . . .	59
4.5.1	Multilevel Concatenated Codes . . . . .	61
4.5.2	Linear Codes with Good Nested List Decodability . . . . .	63
4.5.3	List Decoding Multilevel Concatenated Codes . . . . .	66
4.5.4	Putting it Together . . . . .	69
4.6	Bibliographic Notes and Open Questions . . . . .	70
Chapter 5:	List Decodability of Random Linear Concatenated Codes . . . . .	72
5.1	Introduction . . . . .	72

5.2	Preliminaries . . . . .	73
5.3	Overview of the Proof Techniques . . . . .	76
5.4	List Decodability of Random Concatenated Codes . . . . .	78
5.5	Using Folded Reed-Solomon Code as Outer Code . . . . .	84
5.5.1	Preliminaries . . . . .	84
5.5.2	The Main Result . . . . .	85
5.6	Bibliographic Notes and Open Questions . . . . .	88
Chapter 6:	Limits to List Decoding Reed-Solomon Codes . . . . .	90
6.1	Introduction . . . . .	90
6.2	Overview of the Results . . . . .	91
6.2.1	Limitations to List Recovery . . . . .	91
6.2.2	Explicit “Bad” List Decoding Configurations . . . . .	92
6.2.3	Proof Approach . . . . .	93
6.3	BCH Codes and List Recovering Reed-Solomon Codes . . . . .	93
6.3.1	Main Result . . . . .	93
6.3.2	Implications for Reed-Solomon List Decoding . . . . .	97
6.3.3	Implications for List Recovering Folded Reed-Solomon Codes . . . . .	98
6.3.4	A Precise Description of Polynomials with Values in Base Field . . . . .	99
6.3.5	Some Further Facts on BCH Codes . . . . .	101
6.4	Explicit Hamming Balls with Several Reed-Solomon Codewords . . . . .	102
6.4.1	Existence of Bad List Decoding Configurations . . . . .	102
6.4.2	Low Rate Reed-Solomon Codes . . . . .	102
6.4.3	High Rate Reed-Solomon Codes . . . . .	106
6.5	Bibliographic Notes and Open Questions . . . . .	108
Chapter 7:	Local Testing of Reed-Muller Codes . . . . .	111
7.1	Introduction . . . . .	111
7.1.1	Connection to Coding Theory . . . . .	111
7.1.2	Overview of Our Results . . . . .	112
7.1.3	Overview of the Analysis . . . . .	113
7.2	Preliminaries . . . . .	114
7.2.1	Facts from Finite Fields . . . . .	116

7.3	Characterization of Low Degree Polynomials over $\mathbb{F}_p$ . . . . .	118
7.4	A Tester for Low Degree Polynomials over $\mathbb{F}_p^n$ . . . . .	123
7.4.1	Tester in $\mathbb{F}_p$ . . . . .	123
7.4.2	Analysis of Algorithm <i>Test-<math>\mathcal{P}_t</math></i> . . . . .	124
7.4.3	Proof of Lemma 7.11 . . . . .	127
7.4.4	Proof of Lemma 7.12 . . . . .	131
7.4.5	Proof of Lemma 7.13 . . . . .	136
7.5	A Lower Bound and Improved Self-correction . . . . .	137
7.5.1	A Lower Bound . . . . .	137
7.5.2	Improved Self-correction . . . . .	137
7.6	Bibliographics Notes . . . . .	139
Chapter 8:	Tolerant Locally Testable Codes . . . . .	141
8.1	Introduction . . . . .	141
8.2	Preliminaries . . . . .	141
8.3	General Observations . . . . .	143
8.4	Tolerant Testers for Binary Codes . . . . .	145
8.4.1	PCP of Proximity . . . . .	145
8.4.2	The Code . . . . .	148
8.5	Product of Codes . . . . .	152
8.5.1	Tolerant Testers for Tensor Products of Codes . . . . .	152
8.5.2	Robust Testability of Product of Codes . . . . .	153
8.6	Tolerant Testing of Reed-Muller Codes . . . . .	156
8.6.1	Bivariate Polynomial Codes . . . . .	156
8.6.2	General Reed-Muller Codes . . . . .	157
8.7	Bibliographic Notes and Open Questions . . . . .	159
Chapter 9:	Concluding Remarks . . . . .	161
9.1	Summary of Contributions . . . . .	161
9.2	Directions for Future Work . . . . .	161
9.2.1	List Decoding . . . . .	162
9.2.2	Property Testing . . . . .	163
Bibliography	. . . . .	164

## LIST OF FIGURES

Figure Number	Page
1.1 Bad Example for Unique Decoding . . . . .	5
1.2 The Case for List Decoding . . . . .	6
2.1 The $q$ -ary Entropy Function . . . . .	23
3.1 Rate vs List decodability for Various Codes . . . . .	31
3.2 Folding of the Reed-Solomon Code with Parameter $m = 4$ . . . . .	32
3.3 Relation between Folded RS and Parvaresh Vardy Codes . . . . .	34
4.1 List Decodability of Our Binary Codes . . . . .	53
4.2 Capacity Achieving Code over Small Alphabet . . . . .	56
4.3 Unique Decoding of Random Ensembles of Binary Codes . . . . .	60
4.4 Different variables in the proof of Theorem 4.5. . . . .	69
5.1 Geometric interpretations of functions $\alpha_2(\cdot)$ and $f_{x,2}(\cdot)$ . . . . .	74
7.1 Definition of a Pseudoflat . . . . .	116
8.1 The Reduction from Valiant's Result . . . . .	155

**LIST OF TABLES**

Table Number	Page
4.1 Comparison of the Blokh Zyablov and Zyablov Bounds . . . . .	54