

Contents

Abstract	vii
Kurzfassung	ix
1 Introduction	1
1.1 Background and Motivation	1
1.2 Overview of The Thesis	2
1.3 How to Read The Thesis	4
1.4 Contributions	5
2 Partial-Inverse mod $m(x)$ and Reed-Solomon Decoding	7
2.1 The Partial-Inverse Problem	7
2.2 Remarks On The Problem	9
2.3 The Algorithm to Solve The Problem	13
2.4 Two Variations of The Algorithm	14
2.4.1 The Quotient-Saving Algorithm	15
2.4.2 The Remainder-Saving Algorithm	17
2.5 Application to Decoding Reed-Solomon Codes	19
2.5.1 Reed-Solomon Codes	19
2.5.2 Error-locator and Error Locator-based Interpolation	20
2.5.3 Decoding With The Alternative Key Equation . .	21
2.5.4 Decoding With The Transformed Key Equation . .	23
2.5.5 Concluding Remarks: Berlekamp-Massey-Like Computation for any $m(x)$	25
2.6 Key Elements of The Proof	25
2.7 Proof of The Algorithm	27
2.7.1 Correctness of the Proposed Algorithm	27
2.7.2 Proving Propositions 2.5 and 2.6	29
2.7.3 Proof of Proposition 2.7	29

2.8	Application to Padé Approximation	31
2.9	Application to Solving Standard Key Equation	31
2.10	Proving The Transformed Key Equation and Deriving Standard Key Equation	33
2.10.1	Deriving and Proving Theorem 2.4	34
2.10.2	A Way to Derive the Standard Key Equation	36
2.11	Constrained Partial-Inverse Problem	37
2.12	Joint Errors-and-Erasures Decoding of Reed-Solomon Codes	39
2.13	Conclusion	42
3	Chinese Remainder and Polynomial Remainder Codes	45
3.1	Introduction	45
3.2	Chinese Remainder Codes	47
3.2.1	Chinese Remainder Theorem and Codes	47
3.2.2	Interpolation	49
3.2.3	Hamming Distance and Singleton Bound	51
3.3	Polynomial Remainder Codes (PRC)	52
3.3.1	Definition and Some Examples	52
3.3.2	Degree-weighted Distance	53
3.3.3	Interpolation and Erasures Decoding	56
3.3.4	Minimum-Distance Decoding	57
3.3.5	Summary of Code Parameters	58
3.4	Error Factor Polynomial and The Key Equations	59
3.5	Error Factor-Based Interpolation	61
3.6	Decoding PRC via The Alternative Key Equation	62
3.6.1	Errors-only Decoding	63
3.6.2	Joint Errors-and-Erasures Decoding	63
3.7	Conclusion	65
4	GCD-Based Decoding of Polynomial Remainder Codes	67
4.1	An Extended GCD Algorithm	67
4.2	Modifications for Partially Known $E(x)$	70
4.3	Alternative Modifications for Partially Known $E(x)$	71
4.4	Summary of Decoding	72
4.5	Relation to Prior Work	73
4.6	Conclusion	75
4.7	An Extension	75
4.8	Proof of Theorem 4.3	76
4.9	Proof of Theorem 4.4	81

5	An Algorithm for Simultaneous Partial Inverses	85
5.1	The Simultaneous Partial-Inverse Problem	85
5.2	Existence, Uniqueness, and Degree of The Solution	86
5.3	The Proposed Algorithm	88
5.4	Remarks	91
5.4.1	Complexity of The Algorithm	91
5.4.2	By-products	92
5.5	Proof of The Algorithm	92
5.5.1	Proof of Lemma 5.1	92
5.5.2	Annotated Algorithm	94
5.5.3	Proof of Lemma 5.2	98
5.5.4	Proving the Minimality of The Returned $\Lambda(x)$. .	99
5.6	Conclusion	104
6	Simultaneous Partial-Inverse and Decoding Interleaved Reed-Solomon Codes	105
6.1	Interleaved Reed-Solomon Codes	105
6.2	Channel Model and Error Locator Polynomial	106
6.3	Guaranteed Decoding Using Rank Information	107
6.4	The New Decoding Algorithm	108
6.4.1	Locating Algorithm	108
6.4.2	Decoding	109
6.5	A Remark on The Decoding Algorithm	110
6.6	Proof of Theorem 6.1	110
6.7	Conclusion	112
7	Simultaneous Partial-Inverse and Reed-Solomon Decoding	113
7.1	Decoding Beyond Half the Minimal Distance	113
7.2	Potential Error-Correcting Radius	116
7.3	Conclusion	118
A	The Number of Monic Irreducible Polynomials	119
	Bibliography	121
	About the Author	127