

Contents

Preface	i
Contents	iii
List of Symbols	v
I Parallel linear algebra	1
1 Parallel Gaussian Elimination over Small Finite Fields	3
1.1 Introduction	3
1.2 Implementation of field elements	4
1.2.1 Implementation of prime fields	4
1.2.2 Implementation of arbitrary fields	8
1.2.3 The concept of precomputation	9
1.3 Gaussian elimination	10
1.3.1 Computing the null space	10
1.3.2 Searching for pivot elements	11
1.3.3 Performing row operations by column operations	13
1.3.4 Matrix partition	15
1.3.5 Eliminating multiple rows in a single turn	16
1.4 Implementation	21
1.4.1 Scaling behaviour	21
1.4.2 Implementation of broadcasts	25
1.4.3 Conclusions	27
2 Constructing invariant subspaces	29
2.1 Introduction	29
2.2 The standard approach	29
2.3 Storing subspaces – full versus semi echelon	30
2.4 The parallel algorithm	32
3 Norton's Irreducibility Criterion	35
3.1 Application	36

II	Diagonalisation algorithms	37
4	Diagonalising and Triangulising Matrices over Rings	39
4.1	Introduction	39
4.2	Greatest common divisor computation	39
4.2.1	Smith's GCD computation	40
4.2.2	Blankenship's GCD computation	41
4.2.3	Approximate running times for polynomial domains	45
4.3	Matrix triangulisation	49
4.3.1	Running times and coefficient growth	53
4.4	Matrix diagonalisation	53
4.4.1	Running times and coefficient growth	55
4.5	Parallel implementations	55
4.5.1	Data structures	56
4.5.2	Parallel versions of Blankenship's HNF and LHNH algorithm	57
4.5.3	Running times	58
5	Diagonalizing Characteristic Matrices	61
5.1	Introduction	61
5.2	The Reduction Theorem	62
5.3	The Diagonalizing Algorithm	66
5.4	The Invariant Factors	75
5.5	The Rational Canonical Form	85
5.6	Implementation Notes	87
5.7	Running Times	92
III	Factorization algorithms	97
6	Implementation of Polynomial Factorization Algorithms	99
6.1	Introduction	99
6.2	Basic concepts	100
6.2.1	Equivalent subspaces	100
6.2.2	Extracting factors and randomization	101
6.2.3	Berlekamp's and Niederreiter's Subspaces	102
6.3	The implementations	104
6.4	Concluding remarks	106
	Contact Information	109
	Bibliography	111