

Contents

1	Finite fields, polynomials, vector spaces	1
1.1	Metrics	1
1.2	Rank metric	2
1.3	Finite field constructions	2
1.4	Multiplicative structure of a finite field	5
1.5	Polynomial ring over a finite field	6
1.6	Inverse elements	9
1.7	Division with remainder for integers and polynomials	9
1.8	Euclidean algorithm for polynomials	10
1.9	Computation of powers and logarithms	12
1.10	Trace and normal basis	12
1.11	Ring of linearized polynomials	13
1.11.1	Left and right Euclidean algorithms	14
1.11.2	Factor ring of linearized polynomials	16
2	Rank metric codes	19
2.1	Delsarte matrix codes in rank metric	21
2.2	Dual bases	22
2.3	MRD Gabidulin vector codes	23
2.3.1	Vector codes based on dual bases	24
2.3.2	Generalized vector codes	25
2.3.3	Vector codes based on linearized polynomials	25
3	q-cyclic rank metric codes	29
3.1	q-cyclic codes as ideals	29
3.2	Check polynomials	30
3.3	Defining q-cyclic codes by roots	31
3.4	Generator matrices	32

3.5	Check matrices	33
4	Fast algorithms for decoding rank codes	35
4.1	Error correction in rank metric	35
4.2	Error and erasure correction by MRD codes	39
4.3	Rank errors and rank erasures	41
4.4	Simultaneous error and erasure correction	44
4.4.1	Exclusion of row erasures	45
4.4.2	Exclusion of column erasures	48
4.4.3	Short description of the algorithm correcting errors and erasures simultaneously	49
4.4.4	Correction of erasures only	50
4.5	Examples	51
4.6	Error correction in the Hamming metric	58
5	Symmetric rank codes	61
5.1	Introduction	61
5.2	Matrix and vector representations of extension finite fields . . .	65
5.3	Symmetric matrices representing a field	67
5.3.1	Auxiliary matrices and determinants	67
5.3.2	The main construction	68
5.3.3	Other constructions	72
5.4	Codes based on symmetric matrices	73
5.5	Erasure correction	74
5.6	Codes with subcodes of symmetric matrices	78
5.7	Conclusions	82
6	Rank metric codes in network coding	83
6.1	Principles of network coding	83
6.2	Spaces and subspaces	85
6.2.1	Linear vector spaces	85
6.2.2	Subspace metric	86
6.2.3	Grassmannian	87
6.3	Subspace codes	88
6.3.1	Kötter-Kschischang model	88
6.3.2	Lifting construction of network codes	89
6.3.3	Matrix rank codes in network coding	90
6.3.4	Preliminary linear transformations	91

6.4	Decoding of rank codes	94
6.4.1	When errors and generalized erasures will be corrected	94
6.4.2	Possible variants of errors and erasures	95
6.5	An example	98
6.5.1	Code, channel, received matrix	98
6.5.2	Preliminary transformations	100
6.5.3	Syndrome computation	102
6.5.4	Exclusion of column erasures	103
6.5.5	Exclusion of row erasures	104
6.5.6	Correction of random error	105
6.5.7	Erasures correction	105
6.6	Conclusions	107
7	Multicomponent prefix codes	109
7.1	Gabidulin–Bossert subspace codes	109
7.2	Multicomponent Gabidulin–Bossert subspace codes	111
7.3	Decoding codes with maximum distance	113
7.4	Decoding multicomponent prefix codes	114
7.5	Cardinality of MZP codes	115
7.6	Additional cardinality	116
7.7	Efficiency of MZP codes with maximal code distance	118
7.8	Dual multicomponent codes	121
7.9	Maximal cardinality MZP and DMC codes	121
7.10	ZJSSS codes with maximal cardinality	122
7.11	Dual ZJSSS code	123
7.12	The family of MZP and combined codes	124
7.13	MZP codes with dimension $m \geq 4$ and dual codes	126
7.14	Conclusions	127
8	Multicomponent codes based on combinatorial block designs	129
8.1	Introduction	129
8.2	Reduced row echelon form of matrices	130
8.3	Rank codes with restrictions	131
8.4	Singleton bound	132
8.5	Combinatorial block designs	134
8.5.1	Matrices of the first and the second components	136
8.6	Decoding a restricted rank code	139
8.7	Decoding subspace code	140

8.8	Conclusions	144
9	Problems	145
9.1	Subgroups	145
9.2	Rank codes	147
9.3	q -cyclic codes	152
9.4	Fast decoding algorithms	154
9.5	Symmetric rank codes	155
9.6	Rank codes in network coding	155
9.7	Codes based on combinatorial block designs	155
	Epilogue	157