

# Contents

<i>Preface</i>	vii
1. Basics on error control	1
1.1 ABC on codes . . . . .	1
1.1.1 Basic notations and terminology . . . . .	1
1.1.2 Hamming weight and distance . . . . .	2
1.1.3 Support of a set of vectors . . . . .	2
1.1.4 Extending vectors . . . . .	3
1.1.5 Ordering . . . . .	3
1.1.6 Entropy . . . . .	3
1.1.7 Systematic codes . . . . .	3
1.1.8 Equivalent codes . . . . .	4
1.1.9 New codes from old . . . . .	4
1.1.10 Cyclic codes . . . . .	5
1.2 Linear codes . . . . .	6
1.2.1 Generator and check matrices for linear codes . . . . .	6
1.2.2 The simplex codes and the Hamming codes . . . . .	6
1.2.3 Equivalent and systematic linear codes . . . . .	7
1.2.4 New linear codes from old . . . . .	7
1.2.5 Cyclic linear and shortened cyclic linear codes . . . . .	10
1.3 Distance distribution of codes . . . . .	13
1.3.1 Definition of distance distribution . . . . .	13
1.3.2 The MacWilliams transform . . . . .	13
1.3.3 Binomial moment . . . . .	16
1.3.4 Distance distribution of complementary codes . . . . .	20
1.4 Weight distribution of linear codes . . . . .	22
1.4.1 Weight distribution . . . . .	22

1.4.2	Weight distribution of $*$ -extended codes . . . . .	23
1.4.3	MacWilliams's theorem . . . . .	23
1.4.4	A generalized weight distribution . . . . .	24
1.4.5	Linear codes over larger fields . . . . .	24
1.4.6	Weight distribution of cosets . . . . .	25
1.4.7	Counting vectors in a sphere . . . . .	27
1.4.8	Bounds on the number of code words of a given weight . . . . .	29
1.5	The weight hierarchy . . . . .	30
1.6	Principles of error detection . . . . .	30
1.6.1	Pure detection . . . . .	30
1.6.2	Combined correction and detection . . . . .	31
1.7	Comments and references . . . . .	32
2.	Error detecting codes for the $q$ -ary symmetric channel . . . . .	35
2.1	Basic formulas and bounds . . . . .	35
2.1.1	The $q$ -ary symmetric channel . . . . .	35
2.1.2	Probability of undetected error . . . . .	35
2.1.3	The threshold . . . . .	42
2.1.4	Alternative expressions for the probability of undetected error . . . . .	44
2.1.5	Relations to coset weight distributions . . . . .	45
2.2	$P_{ue}$ for a code and its MacWilliams transform . . . . .	45
2.3	Conditions for a code to be satisfactory, good, or proper . . . . .	47
2.3.1	How to determine if a polynomial has a zero . . . . .	47
2.3.2	Sufficient conditions for a code to be good . . . . .	49
2.3.3	Necessary conditions for a code to be good or satisfactory . . . . .	49
2.3.4	Sufficient conditions for a code to be proper . . . . .	57
2.3.5	Large codes are proper . . . . .	60
2.4	Results on the average probability . . . . .	66
2.4.1	General results on the average . . . . .	66
2.4.2	The variance . . . . .	67
2.4.3	Average for special classes of codes . . . . .	68
2.4.4	Average for systematic codes . . . . .	72
2.5	The worst-case error probability . . . . .	79
2.6	General bounds . . . . .	84
2.6.1	Lower bounds . . . . .	84
2.6.2	Upper bounds . . . . .	89

2.6.3	Asymptotic bounds . . . . .	95
2.7	Optimal codes . . . . .	97
2.7.1	The dual of an optimal code . . . . .	97
2.7.2	Copies of the simplex code . . . . .	97
2.8	New codes from old . . . . .	97
2.8.1	The *-operation . . . . .	98
2.8.2	Shortened codes . . . . .	101
2.8.3	Product codes . . . . .	102
2.8.4	Repeated codes . . . . .	102
2.9	Probability of having received the correct code word . . .	103
2.10	Combined correction and detection . . . . .	105
2.10.1	Using a single code for correction and detection .	105
2.10.2	Concatenated codes for error correction and detec- tion . . . . .	108
2.10.3	Probability of having received the correct code word after decoding . . . . .	109
2.11	Complexity of computing $P_{ue}(C, p)$ . . . . .	109
2.12	Particular codes . . . . .	110
2.12.1	Perfect codes . . . . .	110
2.12.2	MDS and related codes . . . . .	112
2.12.3	Cyclic codes . . . . .	114
2.12.4	Two weight irreducible cyclic codes . . . . .	115
2.12.5	The product of two single parity check codes . . .	116
2.13	How to find the code you need . . . . .	116
2.14	The local symmetric channel . . . . .	118
2.15	Comments and references . . . . .	124
3.	Error detecting codes for the binary symmetric channel	129
3.1	A condition that implies "good" . . . . .	129
3.2	Binary optimal codes for small dimensions . . . . .	132
3.3	Modified codes . . . . .	136
3.3.1	Adding/removing a parity bit . . . . .	136
3.3.2	Even-weight subcodes . . . . .	137
3.4	Binary cyclic redundancy check (CRC) codes . . . . .	137
3.5	Particular codes . . . . .	140
3.5.1	Reed-Muller codes . . . . .	140
3.5.2	Binary BCH codes . . . . .	143
3.5.3	$Z_4$ -linear codes . . . . .	144
3.5.4	Self-complementary codes . . . . .	147

3.5.5	Self-dual codes . . . . .	148
3.6	Binary constant weight codes . . . . .	149
3.6.1	The codes $\Omega_n^m$ . . . . .	149
3.6.2	An upper bound . . . . .	151
3.6.3	Lower bounds . . . . .	151
3.7	Comments and references . . . . .	152
4.	Error detecting codes for asymmetric and other channels	153
4.1	Asymmetric channels . . . . .	153
4.1.1	The Z-channel . . . . .	153
4.1.2	Codes for the $q$ -ary asymmetric channel . . . . .	156
4.1.3	Diversity combining on the Z-channel . . . . .	159
4.2	Coding for a symmetric channel with unknown characteristic . . . . .	162
4.2.1	Bounds . . . . .	163
4.2.2	Constructions . . . . .	164
4.3	Codes for detection of substitution errors and transpositions . . . . .	165
4.3.1	ST codes . . . . .	165
4.3.2	ISBN . . . . .	170
4.3.3	IBM code . . . . .	171
4.3.4	Digital codes with two check digits . . . . .	172
4.3.5	Barcodes . . . . .	173
4.4	Error detection for runlength-limited codes . . . . .	175
4.5	Comments and references . . . . .	178
	<i>Bibliography</i>	181
	<i>Index</i>	199