

Contents

1	Background on Information Theory and Coding Theory	1
1.1	Binary Symmetric Channel	1
1.1.1	Uncertainty	2
1.1.2	Shannon's Theorem	3
1.2	A Simple Example	4
1.3	Basic Definitions	7
1.3.1	The Hamming Metric	9
1.4	Linear Block Codes	10
1.4.1	Decoding Basics	12
1.4.2	Hamming Codes over $GF(q)$	14
1.5	Bounds on the Parameters of a Code	16
1.5.1	Question: What Is "The Best" Code?	18
1.5.2	The Fake Singleton Bound	21
1.6	Quadratic Residue Codes and Other Group Codes	22
1.6.1	Automorphism Groups	22
1.6.2	Cyclic Codes	22
1.6.3	Quadratic Residue Codes	24
2	Self-dual Codes, Lattices, and Invariant Theory	29
2.1	Weight Enumerators	29
2.2	Divisible Codes	31
2.3	Some Invariants	35
2.4	Codes over Other Finite Rings	38
2.5	Lattices from Codes	39
2.5.1	Constructions from Codes	42
2.5.2	Theta Function of a Lattice	43
2.6	More Problems Related to a Prize Problem	44
3	Kittens, Mathematical Blackjack, and Combinatorial Codes	47
3.1	Hadamard Matrices and Codes	47
3.2	Designs, Orthogonal Arrays, Latin Squares, and Codes	51
3.2.1	Examples from Golay Codes	53

3.2.2	Assmus–Mattson Theorem	53
3.2.3	Orthogonal Arrays, Latin Squares and Codes	56
3.3	Curtis’ Kitten, Conway’s Minimog	58
3.3.1	The MINIMOG Description	61
3.3.2	Construction of the Extended Ternary Golay Code	64
3.3.3	The “col/tet” Construction	65
3.3.4	The Kitten Labeling	66
3.4	Playing “Mathematical Blackjack”	67
3.5	Playing the Horses	70
4	The Riemann Hypothesis and Coding Theory	71
4.1	Introduction to the Riemann Zeta Function	72
4.2	Introduction to the Duursma Zeta Function	73
4.3	Introduction	74
4.3.1	Virtual Weight Enumerators	74
4.4	The Zeta Polynomial	77
4.4.1	First Definition	77
4.4.2	Second Definition	83
4.4.3	Third Definition	84
4.4.4	Analogies with Curves	86
4.5	Properties	88
4.5.1	The Functional Equation	89
4.5.2	Puncturing Preserves P	91
4.5.3	The Riemann Hypothesis	91
4.6	Self-reciprocal Polynomials	93
4.6.1	“Smoothness” of Roots	94
4.6.2	Variations on a Theorem of Eneström–Kakeya	94
4.6.3	A Literature Survey	95
4.6.4	Duursma’s Conjecture	103
4.6.5	A Conjecture on Zeros of Cosine Transforms	104
4.7	Examples	106
4.7.1	Komichi’s Example	106
4.7.2	The Extremal Case	107
4.7.3	“Random Divisible Codes”	110
4.7.4	A Formally Self-dual $[26, 13, 6]_2$ -code	110
4.7.5	Extremal Codes of Short Length	111
4.7.6	Non-self-dual Examples	112
4.8	Chinen Zeta Functions	113
4.8.1	Hamming Codes	117
4.8.2	Golay Codes	118
4.8.3	Examples	118
5	Hyperelliptic Curves and Quadratic Residue Codes	123
5.1	Introduction	124
5.2	Points on Hyperelliptic Curves over Finite Fields	124
5.3	Non-Abelian Group Codes	126

5.4	Cyclotomic Arithmetic mod 2	126
5.5	Quasi-quadratic Residue Codes	128
5.6	Weight Distributions	136
5.7	Long Quadratic Residue Codes	138
5.7.1	Examples	141
5.7.2	Goppa's Conjecture Revisited	141
5.8	Some Results of Voloch	141
6	Codes from Modular Curves	145
6.1	An Overview	145
6.2	Introduction to Algebraic Geometric Codes	146
6.2.1	The Codes	147
6.2.2	The Projective Line	148
6.3	Introduction to Modular Curves	150
6.3.1	Shimura Curves	151
6.3.2	Hecke Operators and Arithmetic on $X_0(N)$	157
6.3.3	Eichler–Selberg Trace Formula	159
6.3.4	Modular Curves $X(N)$	161
6.4	Application to Codes	163
6.4.1	The Curves $X_0(N)$ of Genus 1	167
6.5	Some Estimates on AG Codes	168
6.6	Examples	169
6.6.1	The Generator Matrix (According to Goppa)	170
6.7	Ramification Module of $X(N)$	172
6.7.1	Example: $N = 7$	173
7	Appendices	177
7.1	Coding Theory Commands in SAGE	177
7.2	Finite Fields	179
7.3	Tables of Self-dual Codes in SAGE	182
7.4	Proofs	183
7.4.1	MacWilliam's Identity	183
7.4.2	Mallows–Sloane–Duursma Bounds	185
7.5	Ramification Module and Equivariant Degree	187
	References	189
	Index	197