Coding Theory and Number Theory

by

Toyokazu Hiramatsu

Hosei University,
Tokyo, Japan

and

Günter Köhler

Würzburg University,
Würzburg, Germany

KLUWER ACADEMIC PUBLISHERS
DORDRECHT / BOSTON / LONDON

Contents

Preface ix

1. LINEAR CODES 1

   1 Coding Theory 1

   2 Linear codes 4

   3 Cyclic codes 7

   4 Finite fields 13

   5 BCH codes 14

2. DIOPHANTINE EQUATIONS AND CYCLIC CODES 17

   1 Diagonal equations over finite fields 17

   2 The number of solutions and weight distributions of cyclic codes 18

3. ELLIPTIC CURVES, HECKE OPERATORS AND WEIGHT DISTRIBUTION OF CODES 23

   1 Elliptic curves over finite fields 23

   1.1 The group law 24

   1.2 Hasse's theorem 27

   2 Modular forms and Hecke operators 29

   2.1 $SL_2(\mathbf{Z})$ and its congruence subgroups 29

   2.2 The upper half-plane 30

   2.3 Modular forms and cusp forms 30

   2.4 Hecke operators 32

   3 Weight distribution of linear codes 35

   3.1 The MacWilliams identities and Delsarte's theorem 35

   3.2 The weight distribution of the Melas codes 39

4. ALGEBRAIC-GEOMETRIC CODES AND MODULAR CURVE CODES 49

1 Classical Goppa codes 49

1.1 The basic idea 49

1.2 Basic properties of $\Gamma(L, g)$ 51

2 Algebraic curves 52

2.1 Affine varieties and projective varieties 52

2.2 Divisors of algebraic curves 55

3 The zeta functions of curves and rational points 58

3.1 Basic properties of the zeta functions 58

3.2 Maximum number of rational points 61

4 Algebraic-geometric codes 62

4.1 Algebraic-geometric codes of the first kind 62

4.2 Algebraic-geometric codes of the second kind 65

5 Modular curves and codes 66

5.1 Modular curves and their reduction modulo p 67

5.2 Proof of Theorem 4.8 69

5.3 Asymptotic bounds 72

5. THETA FUNCTIONS AND SELF-DUAL CODES 77

1 Lattices and codes 77

1.1 Lattices 77

1.2 Constructing lattices from binary codes 81

1.3 Examples 83

1.4 The lattices associated to a code and the dual code 91

2 Theta functions and weight distributions 92

2.1 The theta function of a lattice 92

2.2 The MacWilliams identity 101

3 Doubly-even self-dual codes 105

3.1 The weight enumerator of doubly-even self-dual codes 105

3.2 The extended Golay code 108

3.3 The Leech lattice 112

Appendix 116

The Kloosterman Codes and Distribution of the Weights 117

1 Introduction 117

2 Melas code and Kloosterman sums 119
3 Hyper-Kloosterman code 122
4 Quasi-cyclic property 126
5 Weight distribution 128
6 Minimum distance of $C_m(q)$ 133
7 A divisibility theorem for Hamming weights 136

References 141

Index 145