Preface iii

1 Linear Codes 1
1.1 Introduction 1
1.2 Linear Codes 2
1.3 Error Correction , 3
1.4 Cyclic Codes 4
1.5 The Parameters of a Linear Code. 6
1.6 Asymptotic Bounds 7
1.7 Exercises 9

2 AIgebraic Function Fields 11
2.1 Introduction 11
2.2 Valuations 12
2.3 Relation of Valuations and Points in the Rational Case 14
2.4 Extension of Valuations 15
2.5 The Set of Prime Divisors. 15
2.6 The Group of Divisors 16
2.7 The Linear Space of a Divisor. 18
2.8 The Theorem of Riemann-Roch 19
2.9 Exercises 20

3 Geometric Goppa Codes 21
3.1 Construction of Geometric Goppa Codes 21
3.2 Codes in the rational function field 22
3.3 A Nontrivial Example 23
3.4 Exercises 26

4 Codes above the Gilbert- Varshamov-Bound 27
4.1 Asymptotics 27
4.2 Codes Beyond the Gilbert-Varshamov-Bound 28

5 Modular Function Fields 29
5.1Introduction 29
5.2 Congruence Subgroups 29
5.3 Exercises 34

6 The Space of Cusp Forms 35
6.1 Introduction 35
6.2 The Space of Cusp Forms 35
6.3 Hecke Operators 36

7 Number of Prime Divisors of p-modular Fields 39
7.1 Relation to the Traces of Hecke Operators. 39
7.2 Codes Beyond the Gilbert-Varshamov-Bound 42

8 An Introduction to the Theory of Bilinear Complexity 43
8.1 Introduction 43
8.2 Computation Sequences and Multiplicative Complexity 45
8.3 Rank o f Bilinear Mappings 50
8.4 Concise bilinear mappings 53
8.5 Lower Bounds for some Computational Problems. 54
8.6 Exercises 59

9 Bilinear Complexity and Codes 61
9.1 Bilinear Complexity and Codes. 61
9.2 A Lower Bound for Matrix Multiplication 62
9.3 A Lower Bound for Polynomial Multiplication 63
9.4 Exercises 65

10 Multiplication in finite fields 67
10.1 The Theorem of Chudnovsky & Chudnovsky 67
10.2 An Asymptotic Linear Upper Bound 68
10.3FurtherResults 70

11 Answers to all Exercises 71

Bibliography 77