

Cambridge University Press

978-0-521-66543-8 - Rational Points on Curves over Finite Fields: Theory and Applications

Harald Niederreiter and Chaoping Xing

Table of Contents

[More information](#)

Contents

Preface	ix
1 Background on Function Fields	1
1.1 Riemann-Roch Theorem	1
1.2 Divisor Class Groups and Ideal Class Groups	6
1.3 Algebraic Extensions and the Hurwitz Formula	10
1.4 Ramification Theory of Galois Extensions	14
1.5 Constant Field Extensions	20
1.6 Zeta Functions and Rational Places	26
2 Class Field Theory	36
2.1 Local Fields	36
2.2 Newton Polygons	38
2.3 Ramification Groups and Conductors	39
2.4 Global Fields	44
2.5 Ray Class Fields and Hilbert Class Fields	47
2.6 Narrow Ray Class Fields	50
2.7 Class Field Towers	55
3 Explicit Function Fields	62
3.1 Kummer and Artin-Schreier Extensions	62
3.2 Cyclotomic Function Fields	65
3.3 Drinfeld Modules of Rank 1	72
4 Function Fields with Many Rational Places	76
4.1 Function Fields from Hilbert Class Fields	76
4.2 Function Fields from Narrow Ray Class Fields	82
4.2.1 The First Construction	82
4.2.2 The Second Construction	92
4.2.3 The Third Construction	94
4.3 Function Fields from Cyclotomic Fields	108
4.4 Explicit Function Fields	113
4.5 Tables	118

Cambridge University Press

978-0-521-66543-8 - Rational Points on Curves over Finite Fields: Theory and Applications

Harald Niederreiter and Chaoping Xing

Table of Contents

[More information](#)

viii

CONTENTS

5 Asymptotic Results	122
5.1 Asymptotic Behavior of Towers	122
5.2 The Lower Bound of Serre	126
5.3 Further Lower Bounds for $A(q^m)$	133
5.4 Explicit Towers	136
5.5 Lower Bounds on $A(2)$, $A(3)$, and $A(5)$	138
6 Applications to Algebraic Coding Theory	141
6.1 Goppa's Algebraic-Geometry Codes	141
6.2 Beating the Asymptotic Gilbert-Varshamov Bound	150
6.3 NXL Codes	156
6.4 XNL Codes	160
6.5 A Propagation Rule for Linear Codes	164
7 Applications to Cryptography	170
7.1 Background on Stream Ciphers and Linear Complexity	170
7.2 Constructions of Almost Perfect Sequences	177
7.3 A Construction of Perfect Hash Families	184
7.4 Hash Families and Authentication Schemes	186
8 Applications to Low-Discrepancy Sequences	191
8.1 Background on (t, m, s) -Nets and (t, s) -Sequences	191
8.2 The Digital Method	197
8.3 A Construction Using Rational Places	203
8.4 A Construction Using Arbitrary Places	212
A Curves and Their Function Fields	219
A.1 Transcendence Degree	219
A.2 Affine Spaces	219
A.3 Projective Spaces	220
A.4 Affine Varieties	222
A.5 Projective Varieties	224
A.6 Projective Curves	225
Bibliography	227
Index	240