

On the automorphism group of various Goppa codes

Submitted by Stephan Wesemeyer to the University of
Exeter as a thesis for the degree of Doctor of
Philosophy in Mathematics in the Faculty of Science,
August 1997.

This thesis is available for Library use on the
understanding that it is copyright material and that no
quotation from the thesis may be published without
proper acknowledgement.

I certify that all material in this thesis which is not my
own work has been identified and that no material is
included for which a degree has previously been
conferred upon me.

.....
(Stephan Wesemeyer)

Contents

Introduction	vi
Acknowledgements	vii
1 Coding Theory Background	1
1.1 Introduction	1
1.2 Fundamentals	2
1.3 t -Error-Correcting and t -Error-Detecting Codes	5
1.4 The Packing and Covering Radii of a Code	7
1.5 Linear Codes	8
1.6 Hamming Codes - an Example	12
1.7 Some General Properties of Linear Codes	13
1.8 Cyclic Codes and BCH Codes	16
1.8.1 Definition of a cyclic code	16
1.8.2 Generator matrix and check polynomial	17
1.8.3 Zeros of a cyclic code	18
1.8.4 BCH codes	19
1.9 Classical Goppa Codes	22
1.9.1 Motivation	22
1.9.2 Goppa codes	22
2 Function Fields And Places	25
2.1 Introduction	25
2.2 Places	25
2.3 Divisors	29
2.4 The Riemann-Roch Theorem	32
2.5 Algebraic Extensions of Function Fields	35

2.6	Examples of Function Fields	38
2.6.1	Rational function field	38
2.6.2	Elliptic and hyperelliptic function fields	39
2.6.3	Tame cyclic extensions of the rational function field	42
2.6.4	Some elementary abelian p -extensions of $K(x)$, $\text{char } K = p > 0$	43
3	Function Fields And Codes	46
3.1	Introduction	46
3.2	Geometric Goppa Codes	46
3.3	Automorphisms of Geometric Goppa Codes	49
3.4	Rational Geometric Goppa Codes	50
3.5	Hermitian Codes	54
4	Automorphisms Of AG Codes And A Map On $\mathcal{L}(G)$	57
4.1	Introduction	57
4.2	Stichtenoth's Result	58
4.3	The Ingredients Needed....	60
5	Automorphisms Of Elliptic And Hyperelliptic Codes	67
5.1	Introduction	67
5.2	Elliptic and Hyperelliptic Codes	67
5.2.1	Fixing the notation for the rest of this section	68
5.2.2	The automorphism group of elliptic and hyperelliptic codes	69
5.3	The Elliptic Case $g = 1$ - An Example	77
5.4	A Hyperelliptic Code in char 2	79
6	A Special Class Of Function Fields	81
6.1	Introduction	81
6.2	Preliminaries	81
6.3	Codes Associated with Admissible Function Fields	83
6.4	The Automorphism Group of Hermitian Codes - An Example	88
7	A Paper Of Xing's Revisited	90
7.1	Introduction	90
7.2	Preliminary Results - Group Theoretical Lemmas	91
7.3	Main Results	94

7.3.1	Case 1: $H(\mathbb{F}_q)[2] = \{Q_\infty, P_{2r+1}, P_{2r+2}, P_{2r+3}\}$	95
7.3.2	Case 2: $H(\mathbb{F}_q)[2] = \{Q_\infty, P_{2r+1}\}$	97
7.3.3	Case 3: $H(\mathbb{F}_q)[2] = \{Q_\infty\}$	99
7.4	Xing's Result Improved	100
8	Codes Associated With The Klein Quartic	103
8.1	Introduction	103
8.2	The Function Field Associated with the Klein Quartic	103
8.3	The Easy Case	104
8.4	The General Case	108
8.5	The Remaining Cases and Examples	128
9	Computational Aspects And Conclusion	131
9.1	Introduction	131
9.2	The General Idea	132
9.3	The Program - Function Fields	133
9.3.1	The elliptic and hyperelliptic case	133
9.3.2	Codes associated with the Klein Quartic	136
9.3.3	Dual codes	137
9.4	The Program - Code Automorphisms	138
9.5	Examples	142
9.5.1	The elliptic function field $F = \mathbb{F}_{17}(x, y)$ defined by $y^2 = x^3 - x$	142
9.5.2	Some hyperelliptic function fields associated with $y^2 = x^5 - x$	147
9.5.3	The Klein Quartic over \mathbb{F}_q where $q \equiv 1 \pmod{7}$	152
9.6	Conclusion	153
A	MAPLE Program	155
A.1	CodeGen2.txt	155
A.2	Klein.txt	163
A.3	FindH.txt	163
B	C++ Program	165
C	MAPLE Sessions	168
C.1	Example 9.5.2 and Example 9.5.3	168
C.2	Example 9.5.4 and Example 9.5.5	179

CONTENTS

C.3 Lemma 9.5.7 (d)	181
C.4 Lemma 9.5.16	182