Norbert Göb

Automorphism Groups of Hyperelliptic Function Fields

Vom Fachbereich Mathematik
der Technischen Universität Kaiserslautern
zur Verleihung des akademischen Grades
Doktor der Naturwissenschaften
(Doctor rerum naturalium, Dr. rer. nat.)
genehmigte Dissertation

Gutachter:
Privatdozent Dr. Andreas Guthmann
Prof. Dr. Wolfram Decker

Datum der Disputation:
28. Januar 2004

D 386

For my son Hendrik

Contents

Notation 3

Introduction 5

Chapter I. Hyperelliptic Function Fields 9
1. Elementary Notations 9
2. Algebraic Function Fields 9
3. The Riemann-Roch Theorem 12
4. Subfields of Algebraic Function Fields 15
5. Automorphisms of Algebraic Function Fields 19
6. Hyperelliptic Function Fields 21
7. Weierstraß Points 25
8. Cantor's Representation of Divisor Classes 29

Chapter II. Cryptographic Aspects 33
1. Hyperelliptic Crypto Systems 33
2. Attacks on HECC 36
3. Known Algorithms for Computing the Order of Jacobians 37
3.1. Zeta Functions 37
3.2. CM-Method 38
3.3. Weil Descent 39
3.4. AGM Method (Gaudry-Harley) 40
4. A Theorem by Madan and its Practical Consequences 41

Chapter III. Defining Equations 49
1. A Simple Criterion 49
2. A Theorem by Lockhart 51
3. Basis Transformations 52
3.1. Relations Between the Variable Symbols 53
3.2. Relation Between the Square Roots 54
3.3. Putting Both Relations Together 57
4. Isomorphisms 60

Chapter IV. Isomorphisms and Normal Forms 63
1. Checking for Defining Equations 63
1.1. Solving Over the Given Constant Field 64
1.2. Constructing Necessary Constant Field Extensions 75
1.3. Checking for Solutions Over the Algebraic Closure 76
2. Explicit Determination of Isomorphisms 77
3. Normal Forms 79

Chapter V. Computing the Automorphism Group 85
1. Elementary Facts on Automorphism Groups 86
2. Automorphism Groups and Associated Normal Forms 88
3. Subgroup Checking 94

3.1. Checking for Cyclic Subgroups Whose Order is Prime to char(k) 94
3.2. Checking for Elementary Abelian char(k)-Groups 95
3.3. Checking for Semidirect Product Groups 96
4. Computing the Automorphism Group 97
5. Stoll's Algorithm 98

Chapter VI. Computational Aspects 101
1. A Secure Jacobian 101
2. The Number of Non-Trivial Automorphism Groups 102
3. Fixed Fields and Their Class Numbers 103
3.1. Fixed Fields of $\mathcal{C}_n$, where $(n, \mathrm{char}(k)) = 1$ and $\nu = 0$ 104
3.2. Fixed Fields of $\mathcal{C}_n$, where $(n, \mathrm{char}(k)) = 1$ and $\nu = 1$ 106
3.3. Fixed Fields of $\mathcal{C}_p^m$ 109
4. Efficiency Considerations and Comparison to Stoll's Algorithm 111

Conclusion 115

Appendix A. Function Fields with Nontrivial Automorphism Groups 117
1. All Imaginary Quadratic Hyperelliptic Fields of Genus 2 over $\mathbb{F}_3$ 117
2. All Imaginary Quadratic Hyperelliptic Fields of Genus 3 over $\mathbb{F}_3$ 118
3. All Imaginary Quadratic Hyperelliptic Fields of Genus 2 over $\mathbb{F}_5$ 121
4. Random Hyperelliptic Fields of Genus 3 130
5. Random Hyperelliptic Fields of Genus 4 131

Appendix B. Jacobian Orders of Subfields 133
1. Fixed Fields of $\mathcal{C}_n$, where $(n, \mathrm{char}(k)) = 1$ and $\nu = 0$ 133
2. Fixed Fields of $\mathcal{C}_n$, where $(n, \mathrm{char}(k)) = 1$ and $\nu = 1$ 137

Bibliography 141

Index 145

Lebenslauf des Autors 147

Author's Curriculum Vitae 149

Notation

In this work, the following notations are used—some of them without further definition.

$(k,+)$	additive group of the field k
$\mathcal{A}_F$, $\mathcal{A}_F(A)$	adele spaces of F
$\overline{k}$	algebraic closure of k
$\mathcal{A}_n$	alternating group of order $\frac{1}{2}n!$
$\mathrm{Aut}(F/k)$	field automorphisms of F fixing k
$\mathrm{Aut}(G)$	automorphisms of G
$\lvert M\rvert$	cardinality of the set M
$\mathrm{char}(k)$	characteristic of the field k
$\mathbb{C}$	complex numbers
Fk	composite field of the fields F and k
$\mathrm{Con}_{F'/F}$	conorm of the function field extension F'/F
$\mathcal{C}_n$	cyclic group of order n
$\mathrm{d}(P'/P)$	different exponent of the place P' lying over P
$\mathrm{Diff}(F'/F)$	different of the function field extension F'/F
$\mathcal{D}_n$	dihedral group of order $2n$
$\dim_k(V)$	dimension of a vector space over k
$\mathrm{div}(a,b)$	divisor defined by the polynomials a and b (Cantor representation)
$a \mid b$	a is a divisor of b
$a \nmid b$	a is no divisor of b
$\mathcal{C}_F$	divisor class group of F
$\mathcal{D}_F$	divisor group of F
$\mathcal{C}_p^m$	elementary abelian p-group of order mp
$a \equiv b \mod n$	n is a divisor of $a-b$
$A \sim B$	the divisors A and B are equivalent
F^G	fixed field of $G \leq \mathrm{Aut}(F/k)$
$\tilde{k}$	full constant field of a function field F/k
$G \leq G'$	G is a subgroup of G'
$G \trianglelefteq G'$	G is a normal subgroup of G'
$\mathrm{Gal}(F'/F)$	Galois group of the field extension F'/F
(a,b)	greatest common divisor of a and b
g, g_F	genus of the function field F
$\mathbb{F}_q$	Galois field, i.e. the finite field of cardinality q
$\mathrm{GL}_n(k)$	general linear group over k
$\mathrm{GL}_n(q)$	general linear group over $\mathbb{F}_q$
Φ	hyperelliptic involution
id_F	identity map on F
$F \cong F'$	F and F' are isomorphic
$\mathbb{J}_F$	Jacobian of the function field F
$\left(\frac{D}{a}\right)$	Jacobi symbol; determines, whether D is a square modulo a
$\mathrm{Ker}(\varphi)$	kernel of φ

$[k' : k]$	degree of the field extension $k' \supseteq k$
$\mathrm{lc}_t(f)$	the leading coefficient of the polynomial f with respect to the variable t
$\lfloor x \rfloor$	floor(x), largest integer $< x$
$P' \mid P$	the place P' lies over the place P
$(l \cdot c)$	linear combination, cf. definition V.2
$\mathbb{N}$	nonnegative integers
$\mathbb{N}_+$	positive integers
$\mathcal{O}(f)$	$\mathcal{O}$-estimation of f as is known from complexity theory
$\mathrm{ord}(g)$	order of a group or group element g
$\mathrm{PGL}_n(k)$	projective general linear group over k
$\mathrm{PGL}_n(q)$	projective general linear group over $\mathbb{F}_q$
$\mathbb{P}_F$	places of the function field F
$p^m \parallel n$	p^m divides n, while p^{m+1} does not
$(x)^F_\infty$	pole divisor of $x \in F$
$(x)^F$	principal divisor of $x \in F$
$\mathcal{P}_F$	principal divisors of F
$\mathbb{P}_n(k)$	n-dimensional projective space over k
$\mathrm{PSL}_n(k)$	projective special linear group over k
$\mathrm{PSL}_n(q)$	projective special linear group over $\mathbb{F}_q$
$\mathrm{e}(P'/P)$	ramification index of the place P' lying over P
$\mathrm{f}(P'/P)$	relative degree of the place P' lying over P
$\mathcal{L}(D)$	Riemann-Roch space of the divisor D
$G \rtimes H$	semidirect product group
$\sigma\vert_F$	restriction of the function σ to F
$\mathrm{SL}_n(k)$	special linear group over k
$\mathrm{SL}_n(q)$	special linear group over $\mathbb{F}_q$
$\langle g_0, \ldots, g_{n-1} \rangle$	span of $g_0, \ldots, g_{n-1}$
$\mathrm{supp}(D)$	support of the divisor D
$\mathcal{S}_n$	symmetric group of order $n!$
$\mathrm{U}_F(G)$	subgroup of $\mathrm{Aut}(F/k)$ if F is of type $\mathrm{F}[G, k]$, cf. definition V.1
$\mathrm{F}[G, k]$	type of a function field, cf. definition V.1
R^*	unit group of the ring R
v_P	valuation corresponding to the place P
$\mathcal{O}_P$	valuation ring corresponding to the place P
Ω_F, $\Omega_F(A)$	Weil differentials of F
$\mathbb{Z}$	integers
$(x)^F_0$	zero divisor of $x \in F$

Introduction

Today, electronic data exchange is part of our everyday lives. Hence, it is essential to protect valuable information against unauthorized access. To be able to do so, cryptographic algorithms need to be researched continuously.

The most widely used public-key crypto system[1] today is RSA ([**RSA78**]). Due to the development of the number field sieve[2], RSA can only assure a sufficient level of security if very large keys are used. Elliptic curves[3] are an alternative to RSA, because they guarantee a high level of security even for small keys[4]. Therefore, they are widely used on smart cards and in similar environments where storage space is limited or expensive.

In 1989, Neal Koblitz suggested to use Jacobians of hyperelliptic curves for cryptographic purposes ([**Kob89**]). These are a natural generalization of (groups of points of) elliptic curves. Hence, they provide more flexibility at a level of security which is at least as high as for elliptic curves, if the same key lengths are used. While both elliptic and (Jacobians of) hyperelliptic curves are considered to be secure in general, there are specific, insecure curves in both cases. To apply (hyper-)elliptic curves in practice, methods are needed which identify insecure curves, allowing users to generate secure ones using a trial-and-error strategy. While this problem is solved for elliptic curves[5], there is no efficient possibility known to find out whether a general[6] hyperelliptic curve has a secure Jacobian.

In order to obtain secure Jacobians $\mathbb{J}$ it is necessary to prevent attacks[7] like Pohlig-Hellman's ([**PH78**]), Frey-Rück's ([**FR94**]) or Duursma-Gaudry-Morain's attacks ([**DGM99**]). The latter is only feasible, if the Jacobian has an automorphism of large order. Because each automorphism of the corresponding hyperelliptic function field[8] defines an automorphism of the Jacobian, at least the field's automorphism group ought to be small for secure Jacobians. To forestall the Pohlig-Hellman attack, one needs to assert that the group order is almost prime, i.e. it ought to contain a large prime factor p_0. To prevent the Frey-Rück attack, p_0 needs to possess additional properties.

Therefore, one needs to know both the automorphism group of the function field and the order of the Jacobian. Unfortunately, there is no efficient algorithm known

[1] Public-key cryptography has been invented by Diffie and Hellman, cf. [**DH76**].

[2] cf. [**LL93**]

[3] cf. e.g. [**Sil86**]

[4] Today, a key length of 256 bit provides security for elliptic curve crypto systems, while equally secure RSA keys need to be 2048 bits long.

[5] The major problem is to avoid Pohlig-Hellman attacks (see chapter II), which can be done using Satoh's point counting algorithm ([**Sat00**], [**FGH00**]).

[6] Nevertheless, it is possible to construct secure curves of specific forms, cf. section II.3.

[7] cf. section II.2

[8] Each (hyper-)elliptic curve corresponds to a (hyper-)elliptic function field and vice versa. Hence, we can also speak of the Jacobian $\mathbb{J}_F$ of a hyperelliptic function field F instead of that of the corresponding hyperelliptic curve. See chapter I for details.

to compute this order for arbitrary hyperelliptic curves. Only for specific types of curves, divisor class counting[9] is feasible for cryptographically relevant group sizes (e.g. [**SSI98**], [**GH00**], cf. section II.3).

A theorem by Madan ([**Mad70**], cf. theorem II.1) implies that $|\mathbb{J}_F|$ divides $|\mathbb{J}_{F'}|$ whenever $F \subseteq F'$ is a finite Galois extension of hyperelliptic function fields. Thus, a hyperelliptic function field with secure Jacobian will most likely have trivial automorphism group $\mathrm{Aut}(F/k) \cong \mathcal{C}_2$, generated by the hyperelliptic involution Φ, only.

This leads us to the following idea of how test Jacobians for insecurity: We compute the automorphism group of the corresponding hyperelliptic function field. If it is non-trivial, we assume the Jacobian to be insecure. Otherwise, we hope it to be secure and apply more expensive algorithms to check this supposition. Some of the known algorithms to generate secure Jacobians as well as some attacks work over constant field extensions[10] of the corresponding hyperelliptic function field. Thus, instead of considering the automorphism group of a function field F/k itself, we compute that over the algebraic closure $\overline{k}$ and abandon all fields as being probably insecure, where $\mathrm{Aut}(F\overline{k}/\overline{k}) \ncong \mathcal{C}_2$.

In this thesis, an algorithm to compute the automorphism group $\mathrm{Aut}(F\overline{k}/\overline{k})$ is developed. Let us outline this algorithm, briefly. It is well known that the automorphism group of a hyperelliptic function field is finite (cf. [**Sch38**], remark I.52). For each finite group, which can occur as subgroup of such an automorphism group, Brandt has given a normal form for the corresponding hyperelliptic function fields as well as explicit formulas for these automorphisms (cf. [**Bra88**], theorem V.6). Brandt's results only apply to function fields over algebraically closed constant fields, which is no problem because we only wanted to compute over the algebraic closure in the first place. Furthermore, it is also possible (but inefficient) to determine the automorphism group over k from that over $\overline{k}$ by explicitly computing the generators of the latter[11]. Because of Brandt's theorem, computing the automorphism group reduces to the problem of deciding, whether the function field has a defining equation of a given form.

Consequently, given two defining equations $u^2 = D_t$ and $y^2 = D_x$ of hyperelliptic function fields, we need to decide, whether $\overline{k}(t,u) = \overline{k}(x,y)$. It can be shown[12] that this question is equivalent to asking whether two function fields $\overline{k}(t,u)$, $u^2 = D_t$ and $\overline{k}(x,y)$, $y^2 = D_x$ are $\overline{k}$-isomorphic. Because Brandt's normal forms contain parameters, this decision must even be possible, if some coefficients of D_t are unknown.

To solve the above problem, we could possibly use results by Wulf-Dieter Geyer[13], which characterize the set of isomorphism classes of hyperelliptic function fields of a given genus over an algebraically closed constant field: According to [**Gey74**], this set is nothing but the spectre[14] of a specific ring. But, it is not obvious from Geyer's paper how to check two fields to be elements of the same prime ideal—especially since D_t may not be known, completely. Therefore, the author developed

[9] i.e. computation of the order of the Jacobian

[10] The constant field of a hyperelliptic function field is the same as the ground field of the corresponding hyperelliptic curve. Because of our cryptographic motivation, we will only consider constant fields whose characteristic is an odd prime.

[11] cf. remark V.10, as well as sections IV.1.1 and IV.1.2.

[12] cf. section III.4

[13] The author thanks Arieh Cohen for referring him to this fact at the MEGA 2003 conference shortly before the finishing of this thesis.

[14] i.e. the set of prime ideals

an algorithm which can be used over both finite and algebraically closed constant fields.

The main ingredient of this algorithm is theorem III.18. It states that two hyperelliptic function fields $F_1 = k(t, u)$ and $F_2 = k(x, y)$ are equal, iff x is a fraction of linear polynomials in $k[t]$ and y is a $k(t)$-multiple of u, where the factor $\frac{y}{u}$ is given up to its sign by the relation of x and t. This condition can be checked using Gröbner basis techniques, as is described in chapter IV as well as in [**Göb03a**]. Theorem III.18 is also of theoretical interest, as we will see for example in chapter VI.

This thesis is structured as follows: In chapter I, we present fundamental facts and definitions related to hyperelliptic function fields. Chapter II is concerned with our cryptographic motivation. We discuss hyperelliptic crypto systems, methods to construct secure Jacobians, attacks and the aforementioned theorem by Madan. The question whether two hyperelliptic function fields are equal or isomorphic is dealt with in chapter III. How to turn the resulting theory into efficient algorithms is the major topic of chapter IV, where we also develop a normal form for hyperelliptic function fields and methods to compute it. We state Brandt's theorem and describe our algorithm to compute automorphism groups in chapter V. We conclude the chapter presenting Stoll's algorithm. Chapter VI concentrates on aspects of the authors implementation of the above algorithms. We compute automorphism groups in order to see whether our initial goal of identifying insecure Jacobians can be fulfilled. This involves the computation of fixed fields, which is done both theoretically and computationally in section VI.3. Finally, we investigate the efficiency of our algorithms and compare it to that of Stoll's algorithm. Because of the large number of examples[15], most of them are listed in the appendix or can be found in [**Göb03b**]. Our main results are summarized in the conclusion.

Acknowledgments

I thank PD Dr. Andreas Guthmann for introducing me into the topic of this work and giving me good advice and encouragement, Professor Wolfram Decker for helpful mathematical discussions, Dr. Franz-Josef Pfreundt and Professor Damian Weber, who has always been a good adviser, for initiating this project, the BGS Systemplanung AG, Mainz, especially Dr. Bernd Kuhlmann, for the interest in my work as well as the financial support, Dr. Anne Frühbis-Krüger for encouraging me to present parts of this thesis at the Mega 2003 conference and for her help in doing so. I would also like to thank the Fraunhofer Institut für Techno- und Wirtschaftsmathematik—especially the department Modelle und Algorithmen in der Bildverarbeitung—for their support and the pleasant working atmosphere. Special thanks go to my wife Silke and my family for their encouragement and patience.

Norbert Göb, August 2003

[15] In total, the author computed 37705 examples.

CHAPTER I

Hyperelliptic Function Fields

Most of the notations as well as many facts stated in this chapter are taken from [**Sti93**]. Readers familiar with Stichtenoth's book and hyperelliptic function fields should understand the remainder of my thesis without perusing this chapter. Nevertheless, starting with section 4 some facts are stated, which are not taken from the common literature.

1. Elementary Notations

Conforming to DIN 1302 ("Deutsches Institut für Normung", German standardization institute) the *natural numbers* $\mathbb{N}$ start at zero, i.e. $\mathbb{N} := \{0, 1, 2, \dots\}$. We adopt this standard. Furthermore, the set of *positive integers* is denoted by $\mathbb{N}_+ := \{1, 2, \dots\}$.

2. Algebraic Function Fields

Definition I.1. Let k be a field. A field $F \supseteq k$ is called an *algebraic function field* or a *function field* over k, if there is some $t \in F$ such that t is transcendental over k and F is a finite algebraic extension of $k(t)$. To mark that F is a function field *over* k, we also denote it by F/k.

We call k the *constant field* of F. The field $\tilde{k}$ of all $x \in F$ which are algebraic over k is called the *full constant field* of F. We will always assume $k = \tilde{k}$.

A function field $k(x)$, where x is transcendental is called a *rational function field.*

Definition I.2. Let F/k be a function field. A surjective mapping $v : F \to \mathbb{Z} \cup \{\infty\}$ is called *valuation* if the following holds.

(1) $v(x) = \infty$ iff $x = 0$.
(2) $v(xy) = v(x) + v(y)$ for all $x, y \in F$.
(3) $v(x + y) \geq \min(v(x), v(y))$ for all $x, y \in F$.
(4) $v(x) = 0$ for all $x \in k^*$.

Definition I.3. Let F/k be a function field and v a valuation of F. Then the set

$$P := \{x \in F \mid v(x) > 0\}$$

is called the *place* associated with v. We also denote v as v_P. The set

$$\mathcal{O}_P := \{x \in F \mid v(x) \geq 0\}$$

is called the *valuation ring of* P. The set of all places of F is denoted by $\mathbb{P}_F$.

The following remark shows the connection between places, valuations and valuation rings. The corresponding proofs can be found in [**Sti93**, section I.1].

Remark I.1. Let v be a valuation of F, and P the place associated with v. Then $\mathcal{O}_P$ really is a *valuation ring*, i.e. $\mathcal{O}_P \subsetneq F$ is a subring such that $k \subsetneq \mathcal{O}_P$ and for each $x \in F$ we have $x \in \mathcal{O}_P$ or $x^{-1} \in \mathcal{O}_P$.

The place P is the maximal ideal of $\mathcal{O}_P$. Thus it is also possible to define a place to be the maximal ideal of a valuation ring. It can also be proved that P is a principal ideal in $\mathcal{O}_P$, i.e. $P = t\mathcal{O}_P$ for some $t \in \mathcal{O}_P$. Such a t is called a *prime element* or a *prime* for P. Using t we can define a valuation w of F: We set $w(0) := \infty$. For $x \in F^*$ we write $x = t^n y$ with $n \in \mathbb{Z}$ and $y \in \mathcal{O}_P{}^*$. Then we set $w(x) := n$. The valuation w defined in this way equals v_P.

More on valuation theory can be found in [**vdW93b**, Kapitel 18]. Let us define divisors, next. These are formal sums of places:

Definition I.4. The free abelian group over $\mathbb{P}_F$ is called the *divisor group* of F, denoted by $\mathcal{D}_F$. We write $\mathcal{D}_F$ additively. The elements of $\mathcal{D}_F$ are *divisors.*

We extend the notation of valuations to divisors: Let $Q \in \mathbb{P}_F$ and $A = \sum_{P\in\mathbb{P}_F} n_P P$ be a divisor of F. Then we write $\mathrm{v}_Q(A) := n_Q$. Using this notation, we can define a partial order on $\mathcal{D}_F$. If $A, B \in \mathcal{D}_F$, we write $A \leq B$, iff $\mathrm{v}_P(A) \leq \mathrm{v}_P(B)$ for all places $P \in \mathbb{P}_F$.

Let $D \in \mathcal{D}_F$, $D = \sum_{P\in\mathbb{P}_F} n_P P$ with $n_P \in \mathbb{Z}$ be a divisor of F. Then we define the *support* of D by

$$\operatorname{supp}(D) := \{P \in \mathbb{P}_F \mid n_P \neq 0\}.$$

The divisor group obviously is not finite. We will see below, that there exists a quotient of a subgroup $\mathcal{D}_F^0 \leq \mathcal{D}_F$, called the Jacobian $\mathbb{J}_F$, which is a finite group if k is finite. The Jacobian can be used for cryptographic algorithms (cf. chapter II). In order to define $\mathcal{D}_F^0$, we need the concept of the degree of a divisor. By the following proposition, each place defines an algebraic field extension of k of finite degree.

Proposition I.2. *Let F/k be an algebraic function field and $P \in \mathbb{P}_F$. Then P is the maximal ideal of $\mathcal{O}_P$ and $\mathcal{O}_P/P$ is a finite field extension of k. If $0 \neq x \in P$ then*

$$[\mathcal{O}_P/P : k] \leq [F : k(x)] < \infty.$$

Proof. By [**Sti93**, theorem I.1.12], P is the maximal ideal of the valuation ring $\mathcal{O}_P$. The degree formula is proved in [**Sti93**, proposition I.1.14]. □

Definition I.5. Let F/k be an algebraic function field and $P \in \mathbb{P}_F$ a place of F. Then the *degree* of P is defined by

$$\deg(P) := [\mathcal{O}_P/P : k].$$

If $D = \sum_{P\in\mathbb{P}_F} n_P P \in \mathcal{D}_F$ is a divisor, its *degree* is defined by

$$\deg(D) := \sum_{P\in\mathbb{P}_F} n_P \deg(P).$$

The divisors of degree 0 form a subgroup $\mathcal{D}_F^0 \leq \mathcal{D}_F$.

As we wish to define the Jacobian, a quotient of $\mathcal{D}_F^0$, we need to construct a subgroup $\mathcal{P}_F$ of $\mathcal{D}_F^0$. This group will consist of so called principal divisors which are generated by evaluating elements of F with respect to all places. We proceed with constructing principal divisors.

Definition I.6. Let F/k be an algebraic function field and $x \in F$. A place $P \in \mathbb{P}_F$ is called *zero* of x if $\mathrm{v}_P(x) > 0$. If we have $\mathrm{v}_P(x) < 0$, we call P a *pole* of x.

We would like to construct the principal divisor of an $x \in F$ by evaluating it with respect to all places setting $(x) := \sum_{P \in \mathbb{P}_F} \mathrm{v}_P(x)P$. Thus, we have to assure that the latter sum consists of only finitely many terms.

Lemma I.3. *Let F/k be an algebraic function field and $0 \neq x \in F$. Then x has only finitely many zeroes and poles.*

Proof. [**Sti93**, corollary I.3.4]. □

Definition I.7. Let F/k be an algebraic function field and $0 \neq x \in F$. The *principal divisor* of x is given by

$$(x) := (x)^F := \sum_{P \in \mathbb{P}_F} \mathrm{v}_P(x)P.$$

The *zero divisor* of x is

$$(x)_0 := (x)_0^F := \sum_{P \in Z} \mathrm{v}_P(x)P,$$

w here $Z \subseteq \mathbb{P}_F$ is the set of zeroes of x. The *pole divisor* of x is

$$(x)_\infty := (x)_\infty^F := \sum_{P \in N} -\mathrm{v}_P(x)P,$$

where $N \subseteq \mathbb{P}_F$ is the set of poles of x.

By lemma I.3, (x), $(x)_0$ and $(x)_\infty$ all are divisors, i.e. the sums are finite. Furthermore, it is obvious that $(x)_0, (x)_\infty \geq 0$ and

$$(x) = (x)_0 - (x)_\infty.$$

If $0 \neq x, y \in F$, the property $\mathrm{v}_P(xy) = \mathrm{v}_P(x) + \mathrm{v}_P(y)$ of the valuation v_P implies the equation $(xy) = (x) + (y)$. Thus, the set $\mathcal{P}_F$ is a subgroup of $\mathcal{D}_F$. Furthermore, principal divisors have degree 0:

Proposition I.4. *Let F/k be a function field with $k = \tilde{k}$ and $0 \neq x \in F$.*

1. *If $x \in k$, then $(x) = (x)_0 = (x)_\infty = 0$.*
2. *If $x \notin k$, then we have*

$$\deg((x)_0) = \deg((x)_\infty) = [F : k(x)].$$

Thus $\mathcal{P}_F \leq \mathcal{D}_F^0$.

Proof. If $x \in k$ and $P \in \mathbb{P}_F$, we have $\mathrm{v}_P(x) = 0$ by definition, thus $(x) = (x)_0 = (x)_\infty = 0$. If $x \notin k$, our claim is proved in [**Sti93**, theorem I.4.11].

As $\deg(0) = 0$, we get $\mathcal{P}_F \subseteq \mathcal{D}_F^0$. The subgroup property is seen easily: The elements of k all have 0 as their principal divisor. If $x, y \in F$, we have seen above that $(x) + (y) = (xy)$. Finally for each $x \in F$, we have $(\frac{1}{x}) = -(x)$, because $\mathrm{v}_P(x) + \mathrm{v}_P(\frac{1}{x}) = \mathrm{v}_P(\frac{x}{x}) = \mathrm{v}_P(1) = 0$ for each $P \in \mathbb{P}_F$. □

As $\mathcal{P}_F$ is a subgroup of $\mathcal{D}_F^0 \leq \mathcal{D}_F$ and all of these are abelian groups, their quotients are also abelian groups.

Definition I.8. Let F/k be a function field such that $k = \tilde{k}$. Then the *divisor class group* of F is the quotient group

$$\mathcal{C}_F := \mathcal{D}_F / \mathcal{P}_F.$$

If $A, B \in \mathcal{D}_F$ are in the same divisor class, i.e. if $A = B + (x)$ for some $x \in F$, we call them *equivalent*, denoted by $A \sim B$. Analogously, we define the *group of divisor classes of degree* 0 by

$$\mathbb{J}_F := \mathcal{C}_F^0 := \mathcal{D}_F^0 / \mathcal{P}_F.$$

This group is also called the *Jacobian* of F.

The Jacobian of a hyperelliptic function field (cf. section 6) is the most common group to be used for hyperelliptic crypto systems. Of course, any cryptographically relevant group needs to be finite in order to be able to represent it on a computing device. According to the following proposition, Jacobians over finite constant fields are always finite.

Proposition I.5. *Let F/k be a function field such that $k = \tilde{k}$ and k is finite. Then $\mathbb{J}_F$ is a finite abelian group.*

Proof. We already know, that $\mathbb{J}_F$ is an abelian group. Its finiteness is proved in [**Sti93**, proposition V.1.3]. □

3. The Riemann-Roch Theorem

In this section we introduce the Riemann-Roch spaces, the genus of a function field, Weil differentials and the famous Riemann-Roch theorem. An introduction to Riemann-Roch theory, where slightly different notations are used, can be found in [**vdW93b**, Kapitel 19].

Definition I.9. Let F/k be a function field such that $k = \tilde{k}$ and $A \in \mathcal{D}_F$. Then the set

$$\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\}$$

is called the *Riemann-Roch space* of A.

As the name “space” suggests, Riemann-Roch spaces actually are vector spaces:

Proposition I.6. *Let F/k be a function field such that $k = \tilde{k}$ and $A \in \mathcal{D}_F$. Then $\mathcal{L}(A)$ is a finite dimensional k-vector space.*

Proof. [**Sti93**, proposition I.4.9] □

Let us state some elementary, but useful properties of Riemann-Roch spaces.

Proposition I.7. *Let F/k be a function field such that $k = \tilde{k}$ and $A \in \mathcal{D}_F$. Then the following holds:*

(1) *Let $x \in F$. We have $x \in \mathcal{L}(A)$ iff $\mathrm{v}_P(x) \geq -\mathrm{v}_P(A)$ for all places $P \in \mathbb{P}_F$.*
(2) *If $B \in \mathcal{D}_F$ is equivalent to A, then $\mathcal{L}(A)$ and $\mathcal{L}(B)$ are isomorphic k-vector spaces.*
(3) *$\mathcal{L}(A) \neq \{0\}$ iff there exists a divisor $B \in \mathcal{D}_F$ with $B \sim A$ and $B \geq 0$.*
(4) *If $A < 0$, then $\mathcal{L}(A) = \{0\}$.*
(5) *$\mathcal{L}(0) = k$.*

Proof. [**Sti93**, remark I.4.5, lemma I.4.6 and lemma I.4.7] □

Definition I.10. Let F/k be a function field such that $k = \tilde{k}$ and $A \in \mathcal{D}_F$. We call the vector space dimension of $\mathcal{L}(A)$ over k the *dimension of A* and denote it by

$$\dim(A) := \dim_k(\mathcal{L}(A)).$$

Using the dimension, we can give a characterization of principal divisors.

Proposition I.8. *Let F/k be a function field and $A \in \mathcal{D}_F$. A is principal, iff* $\deg(A) = 0$ *and* $\dim(A) = 1$ *which is equivalent to* $\deg(A) = 0$ *and* $\dim(A) \geq 1$.

Proof. [**Sti93**, corollary I.4.12]. □

The following proposition tells us that the difference between the degree and the dimension of a divisor is bounded by some global bound. The smallest such bound will be of great interest as it defines the genus of the function field.

Proposition I.9. *Let F/k be a function field such that $k = \tilde{k}$. Then there exists an integer $\gamma \in \mathbb{Z}$ such that we have for each divisor $A \in \mathcal{D}_F$ the inequality*

$$\deg(A) - \dim(A) \leq \gamma.$$

Proof. [**Sti93**, proposition I.4.14]. □

Definition I.11. Let F/k be a function field such that $k = \tilde{k}$. Then we define the *genus* g_F of F by

$$\mathrm{g} := \mathrm{g}_F := \max\{\deg(A) - \dim(A) + 1 \mid A \in \mathcal{D}_F\}.$$

The theorem of Riemann-Roch states the connection between genus of a function field and degree and dimension of its divisors. It uses so called Weil differentials of a function field. In order to define them, we need the concept of adeles:

Definition I.12. Let F/k be a function field with $k = \tilde{k}$. An *adele* of F/k is a map $\alpha : \mathbb{P}_F \to F$, such that $\alpha(P) \in \mathcal{O}_P$ for almost all[1] places $P \in \mathbb{P}_F$. We regard an adele as an element of $\prod_{P \in \mathbb{P}_F} F$. Thus, the set $\mathcal{A}_F$ of all adeles of F becomes a k-vector space. We call $\mathcal{A}_F$ the *adele space of F*.

The *principal adele* of a field element $x \in F$ is defined to be the adele $x : \mathbb{P}_F \to F$, $P \mapsto x$. Thus, we can consider F to be a subspace of $\mathcal{A}_F$. Let us extend the notion of valuations to arbitrary adeles. If $P \in \mathbb{P}_F$ and $\alpha \in \mathcal{A}_F$, we set

$$\mathrm{v}_P(\alpha) := \mathrm{v}_P(\alpha(P)).$$

If $A \in \mathcal{D}_F$, we define a k-subspace of $\mathcal{A}_F$ by

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \mid \mathrm{v}_P(\alpha) \geq -\mathrm{v}_P(A) \text{ for all } P \in \mathbb{P}_F\}.$$

Let us proceed defining Weil differentials:

Definition I.13. Let F/k be a function field with $k = \tilde{k}$. For each divisor $A \in \mathcal{D}_F$, we consider the k-vector space

$$\Omega_F(A) := \{\omega : \mathcal{A}_F \to k \mid \omega \text{ is } k\text{-linear and } \omega(\alpha) = 0 \text{ for all } \alpha \in \mathcal{A}_F(A) + F\}.$$

The sum

$$\Omega_F := \sum_{A \in \mathcal{D}_F} \Omega_F(A)$$

is called the *vector space of Weil differentials*, its elements are *Weil differentials.*

Remark I.10. Weil differentials are the same as ordinary differentials: Let F/k be a function field where k is a perfect field. For simplicity, we assume k to be algebraically closed. We consider differentials $w\,\mathrm{d}z$ as defined by Helmut Hasse, [**Has34a**]: First of all, the fraction $\frac{\mathrm{d}z}{\mathrm{d}t}$, where t is a prime of some place $P \in \mathbb{P}_F$ and $z \in F$, is defined as the formal derivative of z with respect to t: We interpret z as a power series with respect to t, i.e. $z = \sum a_i t^i$, $a_i \in k$. Then we set $\frac{\mathrm{d}z}{\mathrm{d}t} := \sum i a_i t^{i-1}$.

Let $w \in F$. We define $w\frac{\mathrm{d}z}{\mathrm{d}t}$ in the following way: Consider both w and z as power series $w = \sum b_i t^i$, $z = \sum a_i t^i$. Then we set

$$w\frac{\mathrm{d}z}{\mathrm{d}t} := w \cdot \frac{\mathrm{d}z}{\mathrm{d}t} = \left(\sum b_i t^i\right) \cdot \left(\sum i a_i t^{i-1}\right)$$

[1] i.e. all but finitely many

and expand the product, i.e. we compute $c_i \in k$ such that $w\frac{\mathrm{d}z}{\mathrm{d}t} = \sum c_i t^i$. Hasse defines the totality of all $w\frac{\mathrm{d}z}{\mathrm{d}t}$, where $P \in \mathbb{P}_F$ and t is a prime of P to be the *differential* $w\,\mathrm{d}z$. For each place P, Hasse mentions two invariants of each differential $w\,\mathrm{d}z$: Its *valuation* and its *residue* with respect to $P \in \mathbb{P}_F$. The term "invariant" stresses the fact these notions are not affected by the choice of the prime $t \in P$. The valuation of a differential $w\,\mathrm{d}z$ is defined by

$$\mathrm{v}_P(w\,\mathrm{d}z) := \min\left(\{i \in \mathbb{Z} \mid c_i \neq 0\} \cup \{\infty\}\right), \text{ where } w\frac{\mathrm{d}z}{\mathrm{d}t} = \sum c_i t^i.$$

Its residue simply is the coefficient c_{-1} of t^{-1} in the power series $w\frac{\mathrm{d}z}{\mathrm{d}t}$.

In order to obtain a Weil differential, we need to define the mapping $w\,\mathrm{d}z : \mathcal{A}_F \to k$. We start defining its local components $(w\,\mathrm{d}z)_P : F \to k$, first. Let $P \in \mathbb{P}_F$ and $t \in P$ be a prime of P. We compute the power series $w\frac{\mathrm{d}z}{\mathrm{d}t} = \sum c_i t^i$. Let $x \in F$ have the power series $\sum x_i t^i$. We compute the product $(w\frac{\mathrm{d}z}{\mathrm{d}t})x =: \sum d_i t^i$ and define

$$(w\,\mathrm{d}z)_P(x) := d_{-1} \in k,$$

to be the residue of $(w\frac{\mathrm{d}z}{\mathrm{d}t})x$ with respect to P. Thus, $(w\,\mathrm{d}z)_P : F \to k$ maps each x to the residue of the product $w\frac{\mathrm{d}z}{\mathrm{d}t}x$, which does—as mentioned above—not depend on the choice of t.

Now, we are able to define $w\,\mathrm{d}z : \mathcal{A}_F \to k$. Let $\alpha \in \mathcal{A}_F$. Then we set

$$(w\,\mathrm{d}z)(\alpha) := \sum_{P \in \mathbb{P}_F} (w\,\mathrm{d}z)_P(\alpha(P)).$$

It can be shown that $w\,\mathrm{d}z$, defined in this way is a Weil differential and that all Weil differentials are of this kind. More detailed discussions of the relation between Weil differentials and ordinary ones can be found in [**Sti93**, chapter IV] and [**vdW93b**, §156].

With each differential, we associate a divisor. All such divisors are called canonical:

Definition I.14. Let F/k be a function field with $k = \tilde{k}$ and $0 \neq \omega \in \Omega_F$ be a Weil differential.

(1) The *divisor of* ω is the divisor $W \in \mathcal{D}_F$ which is uniquely determined[2] by the following conditions.
   (a) $\omega \in \Omega_F(W)$, i.e. ω vanishes on $\mathcal{A}_F(W) + F$.
   (b) If $\omega \in \Omega_F(A)$ for a divisor $A \in \mathcal{D}_F$, then $A \leq W$.
   Hence W is the maximal divisor such that $\omega \in \Omega_F(W)$.
(2) Let $P \in \mathbb{P}_F$. Then we set $\mathrm{v}_P(\omega) := \mathrm{v}_P(W)$, where W is the divisor of ω.
(3) A divisor W is called *canonical divisor* if there is a Weil differential $\omega \in \Omega_F$ such that W is the divisor of ω.

The following proposition yields an easy criterion for a divisor to be canonical.

Proposition I.11. *Let F/k be a function field of genus g with $k = \tilde{k}$. A divisor $A \in \mathcal{D}_F$ is canonical iff $\deg(A) = 2\mathrm{g} - 2$ and $\dim(A) \geq \mathrm{g}$.*

Proof. [**Sti93**, proposition I.6.2]. □

Now, we are able to state the Riemann-Roch theorem:

Theorem I.12 (Riemann-Roch). *Let F/k be a function field of genus g with $k = \tilde{k}$, $W \in \mathcal{D}_F$ a canonical divisor and $A \in \mathcal{D}_F$ any divisor. Then we have the formula*

$$\dim(A) = \deg(A) + 1 - \mathrm{g} + \dim(W - A).$$

[2] Existence and uniqueness of W are proved in [**Sti93**, lemma I.5.10].

Proof. [**Sti93**, theorem I.5.15]. □

A consequence of theorem I.12 is the following.

Proposition I.13. *Let F/k be a function field of genus* g *with $k = \tilde{k}$ and $A \in \mathcal{D}_F$ with* $\deg(A) \geq 2g - 1$. *Then*

$$\dim(A) = \deg(A) + 1 - g.$$

Proof. [**Sti93**, theorem I.5.17]. □

Remark I.14. Most aspects of the Riemann-Roch theory can be implemented efficiently on a computer, provided one considers only function fields over finite constant fields. In particular, it is possible to represent Riemann-Roch spaces, compute the genus of a function field and determine divisor class numbers if these are not too large. Cf. [**Hes99**] for more details.

4. Subfields of Algebraic Function Fields

We will investigate algorithms to compute the automorphism group of a hyperelliptic function field in chapter V. Naturally, automorphism groups are closely related to subfields. In this section, we discuss the fundamentals of algebraic field extensions of function fields.

> *Throughout this section, we will assume all constant fields k to be the full constant field $k = \tilde{k}$ of their corresponding function field F/k. Furthermore, all constant fields are assumed to be perfect.*[3]

As this thesis is concerned with hyperelliptic function fields over finite or algebraically closed constant fields, these conditions will always hold in the following chapters.

Definition I.15. Let F/k and F'/k' be algebraic function fields.

(1) F'/k' is called an *algebraic extension* or simply *extension* of F/k, if $F' \supseteq F$ and $k' \supseteq k$ both are algebraic field extensions. The function field F/k is called *subfield* of F'/k'.
The extension is called *separable*, if $F' \supseteq F$ is separable. It is called *finite*, if $F' \supseteq F$ is of finite degree.
(2) F'/k' is called *constant field extension* of F/k if it is an algebraic extension of F/k and $F' = Fk'$ is the composite field of F and k'.
(3) Let F'/k' be an extension of F/k, $P' \in \mathbb{P}_{F'}$ and $P \in \mathbb{P}_F$. The place P' *lies over* P (or P *lies under* P') if $P \subseteq P'$. If P' lies over P, we write $P' \mid P$.

Let us state some elementary facts on extension fields of algebraic function fields.

Proposition I.15. *Let F'/k' be an extension of F/k, $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ and $P'|P$. Then we have*

(1) $F \cap k' = k$.
(2) *F'/k' is a finite extension of F/k iff $[k' : k] < \infty$.*
(3) *$P = P' \cap F$ and $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$.*
(4) *There exists an integer $e \geq 1$ such that $\mathrm{v}_{P'}(x) = e \cdot \mathrm{v}_P(x)$ for all $x \in F$.*
(5) *For each place $Q \in \mathbb{P}_F$, there is at least one, but only finitely many places $Q' \in \mathbb{P}_{F'}$ such that $Q' \mid Q$.*

[3] Note that finite fields, algebraically closed fields and fields of characteristic 0 all are perfect (cf. [**Kun94**, §8]), i.e. all constant fields of practical relevance are perfect.

Proof. [**Sti93**, lemma III.1.2, proposition III.1.4 and proposition III.1.7]. □

In many situations we will assume function field extensions to be finite and separable and to share the same constant field. The following proposition justifies this assumption.

Proposition I.16. *Let F'/k' be an algebraic function field extension of F/k. Then there exists a uniquely determined function field F'_s/k', such that*

$$F' \supseteq F'_s \supseteq Fk' \supseteq F$$

all are algebraic function field extensions, where Fk'/k' is a constant field extension of F/k, F'_s/k' is a finite separable extension of Fk'/k' and F'/k' is a purely inseparable extension of F'_s/k' of finite degree. Furthermore, $F' \cong F'_s$ are isomorphic if k' is perfect. If $\mathrm{char}(k) = 0$*, we even have $F' = F'_s$.*

Proof. Obviously, Fk'/k' is a constant field extension of F/k and F'/k' is a function field extension of Fk'/k'. As the latter function fields share the same constant field, F'/k' is a finite extension of Fk'/k' (by proposition I.15) and we only need to consider the ordinary field extension F'/Fk'. If $\mathrm{char}(k) = 0$, F'/Fk' needs to be separable since $\mathrm{char}(Fk') = \mathrm{char}(k) = 0$ (cf. [**vdW93a**, §44]). Thus, our claim is proved in the case $\mathrm{char}(k) = 0$. Let us consider the case $p := \mathrm{char}(k) > 0$, now. By [**Bos93**, Satz 3.7.4], there is a uniquely determined intermediate field F'_s, such that F'/F'_s is purely inseparable while F'_s/Fk' is separable. Of course both of these extensions are finite, since F'/Fk' is.

Finally, we prove the isomorphy $F' \cong F'_s$ if k' is perfect. From [**vdW93a**, §44] we obtain $[F' : F'_s] = p^n$ for some nonnegative integer n. [**Sti93**, proposition III.9.2] implies that $F'_s = \{x^{p^n} | x \in F'\}$ and that the Frobenius map $\varphi_n : F' \to F'_s$, $x \mapsto x^{p^n}$ is an isomorphism. □

Remark I.17. We are chiefly concerned in divisor class groups and Jacobians. Constant field extensions are quite easy to handle, since they are unramified[4] (cf. proposition I.24). As we have seen in proposition I.16, the purely inseparable part of a function field extension yields nothing but an isomorphic field. It is easy to see that isomorphic fields have isomorphic divisor groups, divisor class groups and Jacobians.[5] Thus, the finite separable part of a function field extension is the most interesting one. We will assume most function field extensions to be finite separable and sometimes even to share the same constant field. Inseparable extensions will not be discussed in the remainder of this thesis.

The connection between function fields and their extension fields depends heavily on the connection between their places. Therefore, we will examine the places of extension fields more closely.

Lemma I.18. *Let F'/k' be an extension of F/k, $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ and $P' \mid P$. Then there exists an embedding $\mathcal{O}_P/P \subseteq \mathcal{O}_{P'}/P'$, such that the latter inclusion is a field extension.*

Proof. Let $x + P \in \mathcal{O}_P/P$. As $\mathcal{O}_{P'} \cap F = \mathcal{O}_P$, we have $x \in \mathcal{O}_{P'}$. Furthermore, for each $y \in P = P' \cap F$, we have $y \in P'$. Thus, the mapping

$$\mathcal{O}_P/P \ni x + P \mapsto x + P' \in \mathcal{O}_{P'}/P'$$

is a well defined field homomorphism. As $P = P' \cap F$, this mapping is injective, i.e. it is an embedding. □

[4] Ramification is defined on page 17

[5] This can be proved analogously to [**Sti93**, lemma III.5.2], the special case stating that field automorphisms induce group automorphisms on the Jacobian is proved in proposition I.28

Ramification index and relative degree are essential properties of places of extension fields. Knowing the facts above, we are able to define both of them.

Definition I.16. Let F'/k' be an extension of F/k, $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ and $P' \mid P$.

(1) The *ramification index* of P' over P is the positive integer $\mathrm{e}(P'/P)$ such that
$$\mathrm{v}_{P'}(x) = \mathrm{e}(P'/P) \cdot \mathrm{v}_P(x)$$
for all $x \in F$. If $\mathrm{e}(P'/P) > 1$, we call P' *ramified* over P. Otherwise P' is called *unramified* over P. If all places of F' are unramified, we call F'/k' an *unramified* function field extension of F/k.

(2) The *relative degree* of P' over P is defined by
$$\mathrm{f}(P'/P) := [\mathcal{O}_{P'}/P' : \mathcal{O}_P/P].$$

(3) If P' is unramified and $\mathrm{f}(P'/P) = 1$, we call P' *regular.*

(4) If P' is unramified and $\mathrm{f}(P'/P) = [F' : F]$, we call P' *inert.*

The next proposition shows that both ramification indices and relative degrees behave well in towers of function fields. Furthermore, they are bounded by the degree of the field extension.

Proposition I.19. *Let F'/k' be an extension of a function field F/k.*

(1) *If $P' \in \mathbb{P}_{F'}$ lies over $P \in \mathbb{P}_F$. Then $\mathrm{f}(P'/P) < \infty$ iff $[F' : F] < \infty$.*

(2) *If F''/k'' is an extension of F'/k', $P'' \in \mathbb{P}_{F''}$, $P' \in \mathbb{P}_{P'}$ and $P \in \mathbb{P}_F$ such that $P'' \mid P'$ and $P' \mid P$. Then $P'' \mid P$ and we have*
$$\begin{aligned} \mathrm{e}(P''/P) =& \mathrm{e}(P''/P') \cdot \mathrm{e}(P'/P), \\ \mathrm{f}(P''/P) =& \mathrm{f}(P''/P') \cdot \mathrm{f}(P'/P). \end{aligned}$$

(3) *If F'/k' is a finite extension of F/k, $P \in \mathbb{P}_F$ and $P'_1, \dots P'_n \in \mathbb{P}_{F'}$ are all places of F' lying over P, then we have*
$$\sum_{i=1}^{n} \mathrm{e}(P'_i/P) \cdot \mathrm{f}(P'_i/P) = [F' : F].$$

Proof. In the second claim, $P'' \mid P$ is trivial. The remaining facts are proved in [**Sti93**, proposition III.1.6 and theorem III.1.11]. □

By proposition I.15, each place $P \in \mathbb{P}_F$ has only finitely many extensions $P' \in \mathbb{P}_{F'}$, $P' \mid P$. Thus, the sum of all such places P', multiplied by their ramification indices, is a divisor of F', the so called conorm of P. Extending this definition linearly, we obtain an embedding $\mathrm{Con}_{F'/F} : \mathcal{D}_F \to \mathcal{D}_{F'}$.

Definition I.17. Let F'/k' be a function field extension of F/k.

(1) Let $P \in \mathbb{P}_F$ be a place of F. The *conorm* of P is defined by
$$\mathrm{Con}_{F'/F}(P) := \sum_{P' \mid P} \mathrm{e}(P'/P) \cdot P',$$
where the P' are places of F'.

(2) Let $A = \sum_{P \in \mathbb{P}_F} n_P P \in \mathcal{D}_F$. The *conorm* of A is defined by
$$\mathrm{Con}_{F'/F}(A) := \sum_{P \in \mathbb{P}_F} n_P \cdot \mathrm{Con}_{F'/F}(P).$$

The following proposition shows that the conorm map is injective and induces homomorphisms $\mathcal{C}_F \to \mathcal{C}_{F'}$ and $\mathbb{J}_F \to \mathbb{J}_{F'}$, as well as some other elementary properties.

Proposition I.20. *Let F'/k' be a function field extension of F/k. Then the following holds:*

(1) $\mathrm{Con}_{F'/F} : \mathcal{D}_F \to \mathcal{D}_{F'}$ *is an injective group homomorphism.*
(2) *If F''/k'' is an extension of F'/k' and $A \in \mathcal{D}_F$, then*
$$\mathrm{Con}_{F''/F}(A) = \mathrm{Con}_{F''/F'}(\mathrm{Con}_{F'/F}(A)).$$
(3) *Let $0 \neq x \in F$. Then, we have*
$$\begin{aligned}\mathrm{Con}_{F'/F}((x)^F) &= (x)^{F'},\\ \mathrm{Con}_{F'/F}((x)_0^F) &= (x)_0^{F'},\\ \mathrm{Con}_{F'/F}((x)_\infty^F) &= (x)_\infty^{F'}.\end{aligned}$$
Hence, $\mathrm{Con}_{F'/F}$ *induces homomorphisms*
$$\mathrm{Con}_{F'/F} : \mathcal{C}_F \to \mathcal{C}_{F'}, \quad \mathrm{Con}_{F'/F} : \mathbb{J}_F \to \mathbb{J}_{F'}.$$
In general, these homomorphisms are neither injective nor surjective.
(4) *Let $A \in \mathcal{D}_F$. If F'/k' is a finite extension of F/k, we have the formula*
$$\deg(\mathrm{Con}_{F'/F}(A)) = \frac{[F':F]}{[k':k]} \cdot \deg(A).$$

Proof. Let us provide the proofs for our statements, separately:

(1) Obviously, $\mathrm{Con}_{F'/F}$ is a group homomorphism. We will show that it is injective: Let $A \in \mathcal{D}_F$ such that $\mathrm{Con}_{F'/F}(A) = 0$. Suppose $A \neq 0$ and let $P_1 \in \mathrm{supp}(A)$. Then $\mathrm{supp}(\mathrm{Con}_{F'/F}(P_1)) \neq \emptyset$ and for each $P_2 \in \mathrm{supp}(A)$, $P_2 \neq P_1$, we have
$$\mathrm{supp}(\mathrm{Con}_{F'/F}(P_1)) \cap \mathrm{supp}(\mathrm{Con}_{F'/F}(P_2)) = \emptyset$$
(otherwise, we had $P_1 = P_2' \cap F = P_2$ for some P_2' lying over P_2). Thus the coefficients of places lying over P_1 cannot be canceled by places lying over any $P_2 \neq P_1$. This implies $\emptyset \neq \mathrm{supp}(\mathrm{Con}_{F'/F}(P_1)) \subseteq \mathrm{supp}(\mathrm{Con}_{F'/F}(A)) = \emptyset$. Contradiction. Hence $\mathrm{Con}_{F'/F} : \mathcal{D}_F \to \mathcal{D}_{F'}$ is injective.
(2) Because ramification indices behave well in towers of function fields, this also holds for the conorm.
(3) [**Sti93**, proposition III.1.9] and the paragraphs below its proof.
(4) [**Sti93**, corollary III.1.12].

□

The genus of a subfield of a function field can be computed using the Hurwitz genus formula in many cases. In order to state this formula, we need to define the different of a function field extension.

Definition I.18. Let F'/k' be a finite separable function field extension of F/k.

(1) Let $P' \in \mathbb{P}_{F'}$ lie over $P \in \mathbb{P}_F$. If $\mathrm{char}(k) \nmid \mathrm{e}(P'/P)$, we call
$$\mathrm{d}(P'/P) := \mathrm{e}(P'/P) - 1$$
the *different exponent* of P' over P.
(2) If $\mathrm{char}(k) \nmid \mathrm{e}(P'/P)$ for all $P' \in \mathbb{P}_{F'}$ and all $P \in \mathbb{P}_F$ with $P' \mid P$, we define the *different* of F' over F by
$$\mathrm{Diff}(F'/F) := \sum_{\substack{P \in \mathbb{P}_F, P' \in \mathbb{P}_{F'},\\ P' \mid P}} \mathrm{d}(P'/P) \cdot P'.$$

Remark I.21. More generally, the different can be defined for arbitrary finite function field extensions using generators of so called complimentary modules of valuation rings. This general definition can be found in [**Sti93**, definition III.4.3]. In order to simplify the discussion, the author decided to use a constructive definition which is possible for the fields in which we are interested most: hyperelliptic function fields over constant fields of characteristic ≥ 2. By Dedekind's different theorem ([**Sti93**, theorem III.5.1]), our notion of the different is nothing but the ordinary different—whenever it can be defined.

Theorem I.22 (Hurwitz Genus Formula). *Let F'/k' be a finite separable function field extension of F/k. Then we have*

$$2\mathrm{g}_{F'} - 2 = \frac{[F' : F]}{[k' : k]} \cdot (2\mathrm{g}_F - 2) + \deg(\mathrm{Diff}(F'/F)).$$

Proof. [**Sti93**, theorem III.4.12]. □

As the Hurwitz genus formula holds for all finite separable function field extensions and $\mathrm{Diff}(F'/F) \geq 0$ even for the general definition, we deduce the following inequality.

Corollary I.23. *Let F'/k' be a finite separable function field extension of F/k. Then we have*

$$\mathrm{g}_{F'} - 1 \geq \frac{[F' : F]}{[k' : k]} \cdot (\mathrm{g}_F - 1)$$

Proof. By [**Sti93**, proposition III.4.2], we have $\mathrm{Diff}(F'/F) \geq 0$ even for the general different definition [**Sti93**, definition III.4.3], i.e. $\deg(\mathrm{Diff}(F'/F)) \geq 0$. The Hurwitz genus formula ([**Sti93**, theorem III.4.12]) implies our claim. □

We conclude this section by stating some facts on constant field extensions.

Proposition I.24. *Let F'/k' be a constant field extension of the function field F/k, i.e. $k' \supseteq k$ is an algebraic field extension and $F' = Fk'$. Then the following holds:*

1. *k' is the full constant field of F' (as stated above, we assume k to be the full constant field of F).*
2. *$[F : k(x)] = [F' : k'(x)]$ for any $x \in F \setminus k$.*
3. *F'/F is unramified, i.e. each place $P' \in \mathbb{P}_{F'}$ is unramified over $P := P' \cap F$.*
4. *$\mathrm{g}_{F'} = \mathrm{g}_F$.*
5. *For each divisor $A \in \mathcal{D}_F$, we have*

$$\begin{aligned}\deg(\mathrm{Con}_{F'/F}(A)) &= \deg(A),\\ \dim(\mathrm{Con}_{F'/F}(A)) &= \dim(A),\end{aligned}$$

6. *The conorm $\mathrm{Con}_{F'/F} : \mathcal{C}_F \to \mathcal{C}_{F'}$ for divisor classes is injective.*

Proof. [**Sti93**, proposition III.6.1 and theorem III.6.3]. □

5. Automorphisms of Algebraic Function Fields

In this section, we define the automorphism group of an algebraic function field and discuss the relation between subfields and automorphisms. We will see, that every separable function field extension can be split into a constant field extension and an extension generated by automorphisms. Thus, all separable subfields of a function field having the same constant field can be determined from its automorphism group.

As above we assume all constant fields to be full constant fields. Furthermore, all constant fields are supposed to be perfect.

Definition I.19. Let F/k be an algebraic function field. The *automorphism group* of F/k is the group $\mathrm{Aut}(F/k)$ consisting of all field automorphisms $\sigma : F \to F$ fixing k, i.e. $\sigma(x) = x$ for all $x \in k$. The group law is the composition.

Let $G \leq \mathrm{Aut}(F/k)$. We denote the *fixed field* of G by

$$F^G := \{x \in F \mid \sigma(x) = x \text{ for all } \sigma \in G\}.$$

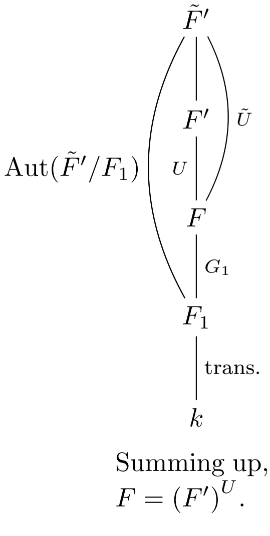
If $\sigma \in \mathrm{Aut}(F/k)$, we denote the fixed field of $\langle\sigma\rangle$ by $F^\sigma := F^{\langle\sigma\rangle}$.

We have already seen that the most interesting function field extensions are finite separable ones. Furthermore, it is commonly known that each finite subgroup G of the automorphism group of a field F defines a separable subfield $F^G \subseteq F$ of finite degree (cf. [**Art73**, Satz 15]). The following theorem shows the inverse fact: Each finite separable subfield of a function field is the fixed field of a group of automorphisms. Thus, if one is interested in all (finite separable) subfields of a function field, the knowledge of the automorphism group is essential.

In section 4 of chapter II, we will see that subfields of hyperelliptic function fields sometimes are dangerous in cryptographic applications. Hence, theorem I.25 yields one of the core motivations for constructing algorithms to compute the automorphism group of hyperelliptic function fields (cf. chapter V): We need to avoid hyperelliptic function fields with subfields which decrease security.

Theorem I.25. *Let F'/k be a finite separable extension of a function field F/k such that $\mathrm{Aut}(F'/k)$ is finite. Then there exists a subgroup $U \leq \mathrm{Aut}(F'/k)$ such that $F = (F')^U$.*

Proof. Let $G_1 := \{\sigma|_F : \sigma \in \mathrm{Aut}(F'/k)\}$ be the set of restrictions of automorphisms of F'/k to F. Obviously, $G_1 \leq \mathrm{Aut}(F/k)$. Let $F_1 := F^{G_1}$.



Then F/F_1 is finite and separable by [**Art73**, Satz 15], thus F'/F_1 also is finite and separable (transitivity of separability, [**Kun94**, Korollar 8.13]). Let $\tilde{F}'$ be the Galois closure of F'/F_1. Since $\tilde{F}'/F_1$ is Galois, there exists a subgroup $\tilde{U} \leq \mathrm{Aut}(\tilde{F}'/F_1)$, such that $F = (\tilde{F}')^{\tilde{U}}$. Let $U := \{\sigma|_{F'} : \sigma \in \tilde{U}\}$. Then $U \leq \mathrm{Aut}(F'/F_1) \leq \mathrm{Aut}(F'/k)$. We will show $F = (F')^U$.

Let $x \in F = (\tilde{F}')^{\tilde{U}}$. As $F \subseteq F'$, we know $x \in F'$. Let $\sigma \in U$. Then, there exists $\tilde{\sigma} \in \tilde{U}$ such that $\sigma = \tilde{\sigma}|_{F'}$. Hence $\sigma(x) = \tilde{\sigma}(x) = x$, since x is fixed by $\tilde{U}$. This proves $F \subseteq (F')^U$.

Conversely, let $x \in (F')^U$. Again, $x \in \tilde{F}'$ is obvious. Let $\tilde{\sigma} \in \tilde{U}$ and $\sigma := \tilde{\sigma}|_{F'} \in U$. This implies $\tilde{\sigma}(x) = \sigma(x) = x$, since $x \in F'$ is fixed by U. Thus $(F')^U \subseteq F$, implying $F = (F')^U$.

Summing up, we have proved the existence of a subgroup $U \leq \mathrm{Aut}(F'/k)$ such that $F = (F')^U$. □

Remark I.26. The assumption that $\mathrm{Aut}(F'/k)$ needs to be finite is met in our application: Hermann Ludwig Schmid proved in [**Sch38**] that each function field of genus > 1 over an arbitrary constant field has at most finitely many automorphisms.

The following proposition shows how automorphisms and places are related.

Proposition I.27. *Let F/k be a function field and F'/k' an algebraic extension of F/k. For a place $P' \in \mathbb{P}_{F'}$ and an automorphism $\sigma \in \operatorname{Aut}(F'/F)$, we denote $\sigma(P') := \{\sigma(x) \mid x \in P'\}$. Then the following holds:*

(1) *For each $\sigma \in \operatorname{Aut}(F'/F)$ and each $P' \in \mathbb{P}_{F'}$, we have $\sigma(P') \in \mathbb{P}_{F'}$. Furthermore, we have for each $x \in F'$*

$$\mathrm{v}_{P'}(x) = \mathrm{v}_{\sigma(P')}(\sigma(x)).$$

(2) *For each $\sigma \in \operatorname{Aut}(F'/F)$ and each $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ such that $P' \,|\, P$, we have $\sigma(P') \,|\, P$.*

(3) *If F'/F is Galois, $P'_1, P'_2 \in \mathbb{P}_{F'}$ and $P \in \mathbb{P}_F$ such that $P'_1 \,|\, P$ and $P'_2 \,|\, P$, there exists a $\sigma \in \operatorname{Aut}(F'/F)$ such that $P'_2 = \sigma(P'_1)$.*

(4) *For each $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ such that $P' \mid P$ we have $\mathrm{e}(\sigma(P')/P) = \mathrm{e}(P'/P)$ and $\mathrm{f}(\sigma(P')/P) = \mathrm{f}(P'/P)$.*

Proof. [**Sti93**, lemma III.5.2 and theorem III.7.1]. □

Finally, we will prove that automorphisms of function fields induce automorphisms of their Jacobians.

Proposition I.28. *Let F/k be a hyperelliptic function field and $\sigma \in \operatorname{Aut}(F/k)$. Then σ induces a group automorphism $\sigma : \mathbb{J}_F \to \mathbb{J}_F$.*

Proof. By proposition I.27, σ induces a group automorphism of $\mathcal{D}_F$. In order to prove our claim, we need to show $\sigma(\mathcal{P}_F) = \mathcal{P}_F$. This obviously follows from the second of the above facts. □

6. Hyperelliptic Function Fields

In this section, we define the fields most relevant to this thesis: Hyperelliptic function fields. We discuss their elementary properties and why the above facts can be applied to elliptic and hyperelliptic function fields.

Throughout this section, we assume all constant fields to be perfect.

Definition I.20. Let k be a field of characteristic $\neq 2$. A polynomial $D \in k[x]$ is said to be *separable*[6] if D has pairwise distinct roots over $\overline{k}$.

Definition I.21. Let k be a field of characteristic $\neq 2$ and $D \in k[x]$ a monic separable polynomial of degree ≥ 3. We define the function field F/k by $F := k(x, y)$, where x is transcendental over k and $y^2 = D(x)$. If $\deg(D) \leq 4$, we call F/k an *elliptic (function) field.* If $\deg(D) > 4$, we call F/k a *hyperelliptic (function) field.* The elements $x, y \in F = k(x, y)$ are called *generators* or *basis* of F/k. The equation $y^2 = D(x)$ is called *defining equation* of F/k.

If $\deg(D)$ is even, the basis x, y is called *real quadratic* and we call F/k to be in *real quadratic representation.* Otherwise, we call x, y an *imaginary quadratic* basis and F/k to be in *imaginary quadratic representation.*

Remark I.29. Although it is possible to consider (hyper-)elliptic function fields over constant fields of characteristic 2, we will not consider this case.

[6] Note that many authors use a different notion of separability for polynomials which are not irreducible: In many works, a polynomial is called *separable*, if all its irreducible factors are separable (in the sense of our definition). While the splitting field of a separable polynomial is separable for both of these definitions, our definition forbids some "irrelevant" polynomials.

Remark I.30. Let F/k be a (hyper-)elliptic function field with defining equation $y^2 = D(x)$. Then the *variety*

$$\{(t,u) \in k \times k \mid u^2 = D(t)\}$$

is called the *(hyper-)elliptic curve* of F. The curve's *function field* is our given field F. Of course, every (hyper-)elliptic curve defines a function field.

First of all, we prove that real and imaginary quadratic representations are essentially equivalent: Each real quadratic (hyper-)elliptic function field has a finite constant field extension which has an imaginary quadratic representation and vice versa.

Lemma I.31. *Let F/k be a (hyper-)elliptic function field in imaginary quadratic representation with defining equation $y^2 = D_x(x)$, i.e. we assume* $\deg(D_x)$ *to be odd. Then there exists a finite constant field extension Fk'/k' such that Fk'/k' has a real quadratic basis $Fk' = k'(t,u)$, $u^2 = D_t(t)$ with* $\deg_t(D_t) = \deg_x(D_x) + 1$.

Furthermore, if there exists a $\xi \in k$ such that $D_x(\xi) \neq 0$, k' can be chosen such that $[k' : k] \leq 2$.

Proof. Let $\xi \in k$ such that $D_x(\xi) \neq 0$. If necessary, we extend k by some such ξ. We set $x' := x - \xi$ and $D'_x(x') := D_x(x' + \xi)$. Then $D'_x \in k[x']$ is a separable polynomial of degree $d := \deg_x(D_x)$ and $F = k(x', y)$. Furthermore, $y^2 = D_x(x) = D_x(x' + \xi) = D'_x(x')$ and $D'_x(0) = D_x(\xi) \neq 0$. Thus, $y^2 = D'_x(x')$ is an imaginary quadratic defining equation of F and D'_x has a nontrivial constant term.

Let $k' = k(\eta)$, where $\eta^2 = D'_x(0)$. We set $t := \frac{1}{x'}$ and $u := \frac{t^{(d+1)/2}}{\eta}y$. Then $F = k(t,u)$ and we have $u^2 = \frac{t^{d+1}}{D'_x(0)}y^2 = \frac{t^{d+1}}{D'_x(0)}D'_x(x') = \frac{t^{d+1}}{D'_x(0)}D'_x(\frac{1}{t}) =: D_t(t)$. Then $D_t \in k[t]$ is a monic separable polynomial. Thus, $u^2 = D_t(t)$ is a defining equation for Fk'/k'. Furthermore, $\deg_t(D_t) = d + 1$, since D'_x has a nontrivial constant term. Hence, t, u is a real quadratic basis of Fk'/k'. □

Example I.1. We consider the hyperelliptic function field $\mathbb{C}(x,y)$ defined by $y^2 = D_x(x)$, where $D_x(x) := x^5 + 19x^4 + 5x^3 + 11x^2 + 80x$. As $D_x(1) \neq 0$, we set $x' = x - 1$ and substitute $x' + 1$ in D_x, obtaining $D'_x(x') = D_x(x' + 1) = (x')^5 + 24(x')^4 + 91(x')^3 + 150(x')^2 + 198x' + 116$. We immediately see $D'_x(0) \neq 0$, as claimed in the above proof.

Setting $t := \frac{1}{x'}$ and $u := \frac{t^3}{\sqrt{116}}y$, we get the real quadratic defining equation

$$\begin{aligned} u^2 =& \frac{t^6}{116}y^2 = \frac{t^6}{116}D_x(x) = \frac{t^6}{116}D_x(x' - 1) = \frac{t^6}{116}D'_x(x') = \frac{t^6}{116}D'_x(\frac{1}{t}) \\ =& \frac{1}{116}(116t^6 + 198t^5 + 150t^4 + 91t^3 + 24t^2 + t) \\ =& t^6 + \frac{99}{58}t^5 + \frac{75}{58}t^4 + \frac{91}{116}t^3 + \frac{2}{29}t^2 + \frac{1}{116}t. \end{aligned}$$

The inverse statement can be proved analogously.

Lemma I.32. *Let F/k be a (hyper-)elliptic function field in real quadratic representation with defining equation $y^2 = D_x(x)$, i.e. we assume $d := \deg(D_x)$ to be even. Then there exists a finite constant field extension Fk'/k' such that Fk'/k' has an imaginary quadratic basis $Fk' = k'(t,u)$, $u^2 = D_t(t)$ with* $\deg_t(D_t) = \deg_x(D_x) - 1$.

PROOF. Let $k'' \supseteq k$ be an extension field such that D_x has a root $\xi \in k''$. We set $x' := x - \xi$ and $D'_x(x') := D_x(x' + \xi)$. As above, $D'_x \in k''[x']$ is separable and we have $Fk'' = k''(x, y) = k''(x', y)$ with $y^2 = D_x(x) = D_x(x' + \xi) = D'_x(x')$. Furthermore, $D'_x(0) = D_x(\xi) = 0$, i.e. $D'_x(x')$ is divisible by x'.

We set $t := \frac{1}{x'}$ and $u' := t^{d/2}y$. Then $Fk'' = k''(t, u)$ and we have $(u')^2 = t^d y^2 = t^d D'_x(x') = t^d D'_x(\frac{1}{t}) =: D'_t(t)$. Then $D'_t \in k''[t]$ is a separable polynomial. In order to make it monic, let $k' = k''(\eta)$ with $\eta^2 = \mathrm{lc}_t(D'_t)$, $u := \frac{u'}{\eta}$ Then, $u^2 = (u')^2 \frac{D'_t(t)}{\mathrm{lc}_t(D'_t)} =: D_t(t)$ is a defining equation for Fk'/k'. Furthermore, $\deg_t(D_t) = d - 1$, since $D'_x(x')$ is divisible by x'. Hence, t, u is an imaginary quadratic basis of Fk'/k'. □

EXAMPLE I.2. We consider the hyperelliptic function field $\mathbb{F}_{109}(x, y)$, $y^2 = D_x(x)$, where $D_x(x) = x^6+23x^5+24x^4+82x^3+62x^2+91x+6$. We have $D_x(-2) = 0$. Hence we define $D'_x := D_x(x' - 2) = (x')^6 + 11(x')^5 + 72(x')^4 + 105(x')^3 + 72(x')^2 + 72x'$. Thus, $D'_t = 72t^5 + 72t^4 + 105t^3 + 72t^2 + 11t + 1$. Dividing by 72, we obtain $D_t = t^5 + t^4 + 6t^3 + t^2 + 38t + 53$. The corresponding basis is $t = \frac{1}{x-2}$, $u = \frac{t^3}{\sqrt{72}}y$.

Next, we prove that a (hyper-)elliptic function field is of genus g iff it has a defining equation $y^2 = D(x)$ with $\deg(D) \in \{2g + 1, 2g + 2\}$.

PROPOSITION I.33. *Let F/k be a (hyper-)elliptic function field with defining equation $y^2 = D(x)$. Then F is a function field of genus $\lfloor \frac{\deg(D)-1}{2} \rfloor$.*

PROOF. For hyperelliptic function fields, cf. [**Sti93**, proposition VI.2.3]. Let us consider the elliptic case. If F/k is in real quadratic representation, lemma I.32 yields a constant field extension Fk'/k' in imaginary quadratic representation $Fk' = k'(t, u)$, $u^2 = D_t(t)$ and $\deg_t(D_t) = 3$. We know from proposition I.24 that $\mathrm{g}_F = \mathrm{g}_{Fk'}$. Hence, it suffices to consider the imaginary quadratic case. Thus, [**Sti93**, proposition VI.1.3] implies our claim. □

REMARK I.34. From this proposition, it can be explained, why only separable polynomials are allowed in defining equations: If $D = f^2E \in k[x]$, then the function field $F = k(x, y)$, $y^2 = D$ would also be generated by x and $u = \frac{y}{f}$. Thus, we had $F = k(x, u)$, $u^2 = \frac{y^2}{f^2} = E$. This implies that the genus of F could not be computed from the degree of the defining equation.

In the sections above, we often assumed the given constant fields to be the full constant fields of their corresponding function fields. The following proposition justifies this assumption: (hyper-)elliptic function fields all have this property.

PROPOSITION I.35. *Let F/k be a (hyper-)elliptic function field. Then k is the full constant field of F/k, i.e. $k = \tilde{k}$.*

PROOF. [**Sti93**, proposition VI.3.1]. □

Obviously, (hyper-)elliptic function fields are cyclic extensions of degree 2 of rational function fields. We want to be able to compute valuations (or places) of (hyper-)elliptic function fields. To do so, we discuss the valuations of rational function fields, first. Afterwards, we will examine the ramification behavior of places of (hyper-)elliptic function fields.

PROPOSITION I.36. *Let $k(x)$ be a rational function field. Let $P \in \mathbb{P}_{k(x)}$. Then, either $\mathrm{v}_P(\varphi) = -\deg_x(\varphi)$ for all $\varphi \in k[x]$ or there exists an irreducible polynomial $p \in k[x]$, such that for all $\varphi \in k[x]$, we have $p^{\mathrm{v}_P(\varphi)} \parallel \varphi$. Obviously, for each $\frac{\varphi}{\psi} \in k(x)$, we have $\mathrm{v}_P(\frac{\varphi}{\psi}) = \mathrm{v}_P(\varphi) - \mathrm{v}_P(\psi)$.*

Proof. [**Sti93**, Section I.2]. □

Definition I.22. Let $k(x)$ be a rational function field and $P \in k[x]$ an irreducible polynomial. Then we denote the place associated with P by P, i.e. $\mathrm{v}_P(P^n \frac{\varphi}{\psi}) = n$ whenever $P \nmid \varphi, \psi \in k[x]$.

The place given by the degree with respect to x is called the *infinite place* with respect to x. We denote it by ∞_x or simply by ∞. Hence, $\mathrm{v}_{\infty_x}(\frac{\varphi}{\psi}) = \deg_x(\psi) - \deg_x(\varphi)$ for each $\varphi, \psi \in k[x]$.

Remark I.37. The infinite place ∞_x with respect to x is just the pole divisor of x, i.e. $\infty_x = (x)_\infty$.

The degrees of places of rational function fields are nothing but the degrees of the corresponding polynomials.

Proposition I.38. *Let $k(x)$ be a rational function field and $P \in \mathbb{P}_{k(x)}$. If $P \in k[x]$, we have $\deg(P) = \deg_x(P)$, i.e. the degree of the place P equals the degree of the polynomial P.*

If $P = \infty_x$, we have $\deg(P) = 1$.

Proof. [**Sti93**, proposition I.2.1]. □

Let us discuss the ramification behavior in (hyper-)elliptic over rational function fields, next.

Proposition I.39. *Let $F = k(x,y)$ be a (hyper-)elliptic function field with defining equation $y^2 = D(x)$. Then $k(x)$ is a rational subfield of F of degree $[F : k(x)] = 2$. The places lying over irreducible polynomials dividing D are ramified. If $\deg_x(D)$ is odd, the place lying over ∞_x also is ramified. All other places are unramified.*

In other words, if $P' \in \mathbb{P}_F$ lies over $P \in \mathbb{P}_{k(x)}$, the ramification index is given by

$$\mathrm{e}(P'/P) = \begin{cases} 2 & , \textit{ if } P \in k[x] \textit{ and } P \mid D, \\ 2 & , \textit{ if } P = \infty_x \textit{ and } \deg(D) \equiv 1 \mod 2, \\ 1 & , \textit{ otherwise.} \end{cases}$$

Proof. By [**Sti93**, proposition III.7.3], we have $\mathrm{e}(P'/P) = \frac{2}{(2, \mathrm{v}_P(D(x)))}$. If $P \in k[x]$, $P \mid D$, we have $\mathrm{v}_P(D) = 1$, i.e. $\mathrm{e}(P'/P) = 2$. If $P \in k[x]$, $P \nmid D$, we have $\mathrm{v}_P(D) = 0$, i.e. $(2, \mathrm{v}_P(D)) = 2$. Thus, $\mathrm{e}(P'/P) = 1$. If $P = \infty_x$, we have $\mathrm{v}_P(D) = -\deg_x(D)$. Thus, $\mathrm{e}(P'/P) = 2$, if $\deg_x(D)$ is odd and $\mathrm{e}(P'/P) = 1$, if $\deg_x(D)$ is even. □

For (hyper-)elliptic curves, it also is easy to compute the relative degree of places over $k(x)$. This can be done using the following proposition.

Proposition I.40. *Let $F = k(x,y)$ be a (hyper-)elliptic function field with defining equation $y^2 = D(x)$, $P \in \mathbb{P}_{k(x)}$ and $P' \in \mathbb{P}_F$ such that $P' \mid P$. Then the relative degree of P' over P is given by*

$$\mathrm{f}(P'/P) = \begin{cases} 1 & , \textit{ if } P \in k[x] \textit{ and } P \mid D, \\ 1 & , \textit{ if } P \in k[x],\ P \nmid D \textit{ and } D \textit{ is a square modulo } P, \\ 1 & , \textit{ if } P = \infty_x, \\ 2 & , \textit{ otherwise.} \end{cases}$$

Proof. Because of proposition I.19, whenever $P' \in \mathbb{P}_F$ is ramified over P, we need to have $\mathrm{f}(P'/P) = 1$. By proposition I.39, this proves our claim if $P \in k[x]$, $P \mid D$ or $P = \infty_x$, $\deg_x(D)$ odd.

We consider the unramified cases, next. By proposition I.19, we can compute the relative degree by counting the number of places over P: We have $\mathrm{f}(P'/P) = 1$ iff there are two places over P. By [**Neu92**, Satz II.8.2], P has as many extensions as $y^2 - D(x)$ has irreducible factors in the P-adic completion K of $k(x)$.

Let us consider the case $P \in k[x]$, $P \nmid D$, first: By Hensel's Lemma (cf. [**vdW93b**, §144]), $y^2 - D(x)$ has two factors over K iff there exists a polynomial $\alpha \in k[x]$ such that $D \equiv \alpha^2 \mod P$. This proves our claim in this case, i.e. for $P \in k[x]$, $P \nmid D$.

Finally, we have to consider the case $P = \infty_x$, $d := \deg_x(D)$ even. In order to factor D modulo P, we need to find a power series

$$\alpha = x^{\frac{d}{2}} + a_{-\frac{d}{2}+1} x^{\frac{d}{2}-1} + ... + a_0 + \sum_{i=1}^{\infty} a_i x^{-i},$$

such that $\alpha^2 \equiv D \mod P$. An explicit computation of the power series α^2 shows that α exists, since $\deg_x(D)$ is even. Thus, P has two extensions in F, which implies $\mathrm{f}(P'/P) = 1$. □

From our definition of the different, we obtain a formula for $\mathrm{Diff}(F/k(x))$:

Corollary I.41. *Let $F = k(x, y)$ be a (hyper-)elliptic function field with defining equation $y^2 = D(x)$. Then the different* $\mathrm{Diff}(F/k(x))$ *is just the sum of all ramified places, i.e.*

$$\mathrm{Diff}(F/k(x)) = \begin{cases} \sum_{P \mid D} P' & , \textit{ if } \deg(D) \equiv 1 \mod 2, \\ \sum_{P \mid D} P' + \infty_x' & , \textit{ if } \deg(D) \equiv 0 \mod 2, \end{cases}$$

where P' denotes the (uniquely determined) place of F lying over $P \in k[x] \subseteq \mathbb{P}_{k(x)}$.

Proof. Because of proposition I.19, all ramified places have ramification index 2 and are uniquely determined by the places lying under them. Thus, $\mathrm{char}(k) \neq 2$ implies that the different is the sum of all ramified places. Proposition I.39 yields our formula. □

7. Weierstraß Points

In [**Sch39**], Friedrich Karl Schmidt defined the Weierstraß points of an algebraic function field over an arbitrary constant field as generalization of those defined for curves over the field $\mathbb{C}$ of complex numbers. Weierstraß points of an algebraic function field are closely related to its automorphism group. This is why we investigate some of their properties.

In this section we give a definition of Weierstraß points and state some elementary properties. We will see that each function field has only finitely many Weierstraß points and we will characterize the Weierstraß points of (hyper-)elliptic function fields. Furthermore, we will see that automorphisms permute the set of Weierstraß points.

In order to define Weierstraß points we need the notions of pole and gap numbers of places.

Definition I.23. Let F/k be an algebraic function field with $k = \tilde{k}$, $P \in \mathbb{P}_F$ a place of F and $n \in \mathbb{N}$.

(1) We call n a *pole number* of P, if there exists an element $x \in F$ such that $(x)_\infty = nP$.
(2) We call n a *gap number* of P if $(x)_\infty \neq nP$ for each $x \in F$.

It is easy to see that the set of pole numbers is a sub-semigroup of $(\mathbb{N}, +)$:

PROPOSITION I.42. *Let F/k be an algebraic function field with $k = \tilde{k}$, $P \in \mathbb{P}_F$ a place of F and n_1, n_2 pole numbers of P. Then $n_1 + n_2$ also is a pole number of P. Thus, the set of pole numbers is a sub-semigroup of* $\mathbb{N}$.

PROOF. Let n_1, n_2 be pole numbers of P. Then there are $x_1, x_2 \in F$ such that $(x_1)_\infty = n_1 P$ and $(x_2)_\infty = n_2 P$. From the definitions of v_P and of pole divisors it is obvious that $(x_1 x_2)_\infty = (x_1)_\infty + (x_2)_\infty = (n_1 + n_2)P$. Thus $n_1 + n_2$ also is a pole number. This proves our claim. □

A well known property of gap numbers is the Weierstraß gap theorem which tells us that gap numbers are bounded by $2\mathrm{g} - 1$ for places of degree 1.

PROPOSITION I.43 (Weierstraß Gap Theorem). *Let F/k be an algebraic function field of genus* $\mathrm{g} > 0$ *with $k = \tilde{k}$ and $P \in \mathbb{P}_F$ a place of degree* $\deg(P) = 1$. *Then P has exactly* g *gap numbers* $1 = n_1 < \cdots < n_\mathrm{g} \leq 2\mathrm{g} - 1$.

If k is algebraically closed, almost all places have the same sequence of gap numbers.

PROOF. [**Sti93**, theorem I.6.7]. □

As almost all places have the same sequence of gap numbers (if k is algebraically closed), the places not sharing these gap numbers are of special interest. We will call them Weierstraß points of F/k. The following definition also considers the case where k is not algebraically closed.

DEFINITION I.24. Let F/k be an algebraic function field with $k = \tilde{k}$. A place $P \in \mathbb{P}_F$ is called *Weierstraß point* of F if only finitely many places of F have the same set of gap numbers as P.

From proposition I.43, we know that the set of Weierstraß points is finite whenever the constant field of an algebraic function field is algebraically closed. This also holds for arbitrary constant fields, as can easily be deduced from the first claim of proposition I.43, if we consider that rational function fields cannot have Weierstraß points.[7]

PROPOSITION I.44. *Let F/k be an algebraic function field with $k = \tilde{k}$. Then F has only finitely many Weierstraß points.*

PROOF. [**Sch39**, page 78, I.]. □

This fact becomes even more interesting, if we consider that each function field has infinitely many places, as is the content of the following proposition.

PROPOSITION I.45. *Let F/k be a function field such that $k = \tilde{k}$. Then F has an infinite number of places.*

PROOF. [**Sti93**, corollary I.3.2]. □

[7] Let us prove this statement: Because $(\frac{1}{p(x)^n})_\infty = np$ for each irreducible polynomial $p \in k[x]$ and each $n \in \mathbb{N}$, irreducible polynomials have no gap numbers. The analogous argument holds for ∞_x. Thus all (infinitely many) places of $k(x)$ share the same set $\emptyset$ of gap numbers, i.e. they are no Weierstraß points.

From this, we obtain that function fields over finite constant fields have an infinite number of places whose degree is larger than any given bound. In particular, for each finite field $\mathbb{F}_q$ and each $n \in \mathbb{N}$, there exist irreducible polynomials whose degree is at least n.

Corollary I.46. *Let F/k be a function field over a finite field k such that $k = \tilde{k}$ and $n \in \mathbb{N}$. Then F has an infinite number of places of degree $\geq n$.*

Proof. Let $k(t) \subseteq F$ be rational. For each place $p \in \mathbb{P}_{k(t)}$, we have only finally many places of F lying over p, as we know from proposition I.15. Apart from $\infty_t \in \mathbb{P}_{k(t)}$, all places of $k(t)$ can be identified with polynomials from $k[t]$. The degree of a place of $k(t)$ is just the degree of the corresponding polynomial. The degree of a place $P \in \mathbb{P}_F$ lying over $p \in \mathbb{P}_{k(t)}$ is $\mathrm{f}(P/p) \cdot \deg(p)$. Thus, $\deg(P) \geq \deg(p)$ whenever $P \mid p$. All of these facts have been discussed in section 6.

If $n \leq 1$, there are no places of degree $< n$. Let us assume $n > 1$, now. Since k is finite, the number of polynomials $p \in k[t]$ such that $\deg_t(p) < n$ is $|k|^n$, which is more than the number of corresponding places, since multiplying a polynomial by an element of k yields the same place. The infinite place ∞_t is the only additional place of degree $1 < n$. Thus, the number of places of $k(t)$ whose degree is less than n is finite. Because only finitely many places of F can lie over each place of $k(t)$ and because the degree of a place P of F can only be larger than that of the place below, F can only have finitely many places of degree less than n.

By proposition I.45, F has infinitely many places. Thus, F needs to have an infinite number of places whose degree is at least n. □

Next, we would like to characterize Weierstraß points of (hyper-)elliptic function fields—at least over finite as well as over algebraically closed constant fields. To do so, it is necessary to determine the gap numbers of arbitrary places. The following proposition solves this problem.

Proposition I.47. *Let $F = k(x, y)$ be a (hyper-)elliptic function field of genus g over an arbitrary constant field k and $P \in \mathbb{P}_F$ a place of F. Then*

1. *If P is regular over $k(x)$, i.e. if P is not ramified over $k(x)$ and the relative degree of P over $P \cap k(x)$ is 1, P has the gap numbers $1, 2, \ldots, \lfloor \frac{\mathrm{g}}{\deg(P)} \rfloor$. In other words, the gap numbers of a regular place P are the first $\lfloor \frac{\mathrm{g}}{\deg(P)} \rfloor$ positive integers.*
2. *If P is ramified over $k(x)$, then its gap numbers are $1, 3, 5, \ldots, 2\lfloor \frac{\mathrm{g}}{\deg(P)} \rfloor - 1$. In other words, the gap numbers of a ramified place P are the first $\lfloor \frac{\mathrm{g}}{\deg(P)} \rfloor$ positive odd integers.*
3. *If P is inert over $k(x)$, i.e. if P is not ramified over $k(x)$ and the relative degree of P over $P \cap k(x)$ is 2, then P has no gap numbers at all.*

Proof. [**Sch39**, Satz 7]. □

Note that proposition I.43 does not contradict the fact that inert places do not have Weierstraß points: Inert places have at least degree 2.

Proposition I.47 implies the following, very simple characterization of Weierstraß points in hyperelliptic function fields over algebraically closed constant fields: Weierstraß points are exactly the ramified places over the rational function field. Elliptic function fields do not have Weierstraß points. The part of proposition I.48 concerning hyperelliptic function fields also was proved in [**Sch39**, Satz 8].

Proposition I.48. *Let $F = k(x, y)$ be a hyperelliptic function field over an algebraically closed constant field k and $y^2 = D(x)$ a defining equation for F. Then the set of Weierstraß points of F is exactly the set of places which are ramified over $k(x)$.*

Elliptic function fields over algebraically closed constant fields do not have Weierstraß points at all.

Proof. Let's consider the inert, regular and ramified places separately:

1. By propositions I.39 and I.40, a place P lying over a polynomial $p \in k[x]$ is inert iff $p \nmid D$ and D is no square modulo p. Thus, even for arbitrary constant fields, there is an infinite number of inert places. Hence, an infinite number of places does not have gap numbers. Therefore, inert places are no Weierstraß points.
2. Since k is algebraically closed, each regular or ramified place has degree 1. Thus, each regular place has the gap numbers $1, 2, \ldots, \mathrm{g}$. As there is an infinite number of regular places, they also cannot be Weierstraß points.
3. Thus, each Weierstraß point needs to be ramified. If P is ramified, then $P \cap k(x)$ is a divisor of D or $P \cap k(x) = \infty_x$ (if F is in imaginary quadratic representation). Thus there are only finitely many ramified places. By proposition I.47, each ramified place has the gap numbers $1, 3, \ldots, 2\mathrm{g}-1$. Therefore, if $\mathrm{g} \geq 2$, the ramified places are Weierstraß points. If $\mathrm{g} = 1$, ramified places have the same gap numbers as regular places, i.e. they are no Weierstraß points.

□

Combining propositions I.39 and I.48 we obtain a concrete criterion for Weierstraß points of (hyper-)elliptic function fields:

Corollary I.49. *Let $F = k(x, y)$ be a hyperelliptic function field over an algebraically closed constant field k and $y^2 = D(x)$ a defining equation of F. Let $D = p_1 \cdots p_n$ be the factorization of D. For each p_i, let P_i be the place of F which lies above p_i. Then the set of Weierstraß points of F is given by*

1. $\{P_1, \ldots, P_n\}$, *if* $\deg(D) = n = 2\mathrm{g} + 2$ *(real quadratic representation).*
2. $\{P_1, \ldots, P_n, \infty_x\}$, *if* $\deg(D) = n = 2\mathrm{g} + 1$. *(imaginary quadratic representation).*

Proof. From proposition I.48 we know, that the set of Weierstraß points is equal to the set of ramified places of F over $k(x)$. By proposition I.39, the ramified places of F are just the places listed in our claim. □

In the cases of practical relevance, the constant field rarely is algebraically closed. Instead, we mostly have to consider finite constant fields. For these, the characterization of Weierstraß points is easy, too.

Proposition I.50. *Let $F = k(x, y)$ be a (hyper-)elliptic function field over a finite constant field k and $y^2 = D(x)$ a defining equation for F. Then the set of Weierstraß points of F is consists of the following places:*

1. *The infinite place ∞_x.*
2. *Regular places of degree $\leq \mathrm{g}$, i.e. places $P \in \mathbb{P}_F$ with $\deg(P) \leq \mathrm{g}$, $P \mid p$, $p \in k(x)$ and D is a square modulo p, as well as the infinite place ∞_x if $\deg_x(D) = 2\mathrm{g} + 2$.*

(3) *Ramified places of degree* $\leq \mathrm{g}$*, i.e. places* $P \in \mathbb{P}_F$ *with* $\deg \leq \mathrm{g}$*,* $P \,|\, p$*,* $p \in k(x)$ *and* p *divides* D *as well as the infinite place* ∞_x *if* $\deg_x(D) = 2\mathrm{g} + 1$*.*

Proof. By proposition I.47, inert places, as well as all places of degree $> g$ do not have gap numbers. By corollary I.46, there is an infinite number of such places, i.e. they are no Weierstraß points.

As we have seen in the proof of corollary I.46, the number of places of degree $< \mathrm{g}$ is finite. The infinite place either is regular of split. Thus, the number of places specified in our claim is finite and it remains to consider their gap numbers.

Since $\mathrm{g} \geq 1$ each regular or ramified place of degree $\leq \mathrm{g}$ has 1 as a gap number. Thus, all of the specified places are Weierstraß points. □

For finite constant fields, both deciding whether a given place is a Weierstraß point and constructing all Weierstraß points becomes easy using proposition I.50. A non-infinite place $P \in \mathbb{P}_F$ lies above some $p \in k[x]$. In order to decide whether P is ramified, we only have to check if $p \mid D$. If P is not ramified, we have to find out whether D is a square modulo p, i.e. we need to compute the Jacobi symbol $\left(\frac{D}{p}\right)$. Its definition and how to compute it efficiently can be found on page 36, at the end of section II.1.

We finish this section with a simple connection between automorphisms and Weierstraß points. It is folklore knowledge that automorphisms of hyperelliptic function fields permute the Weierstraß points. As the author was not able to find a proof of this fact in the common literature, an elementary one is presented, next.

Proposition I.51. *Let* F/k *be an algebraic function field with* $k = \tilde{k}$*,* $\sigma \in \mathrm{Aut}(F/k)$ *and* $P \in \mathbb{P}_F$ *a Weierstraß point. Then* $\sigma(P)$ *also is a Weierstraß point, i.e. each automorphism permutes the set of Weierstraß points.*

Proof. Let $n \in \mathbb{N}$ be a pole number of a place $P \in \mathbb{P}_F$. Then, there exists an $x \in F$ such that $(x)_\infty = nP$, i.e. $\mathrm{v}_P(x) = -n$ and $\mathrm{v}_Q(x) \geq 0$ for all $Q \in \mathbb{P}_F$, $Q \neq P$. By proposition I.27 we have $\mathrm{v}_{\sigma(P)}(\sigma(x)) = \mathrm{v}_P(x) = -n$ and $\mathrm{v}_{\sigma(Q)}(\sigma(x)) = \mathrm{v}_Q(x) \geq 0$ for all $Q \neq P$. Thus, $(\sigma(x))_\infty = n\sigma(P)$. Hence, n is a pole number of $\sigma(P)$. Analogously, each pole number of $\sigma(P)$ also is a pole number of P.

Because P and $\sigma(P)$ share the same set of pole numbers, they also have the same set of gap numbers, i.e. $\sigma(P)$ is a Weierstraß point whenever P is one. □

Remark I.52. The facts that automorphisms permute Weierstraß points and that each algebraic function field of genus > 1 has only finitely many Weierstraß points can be used to prove that each hyperelliptic function field has only finitely many automorphisms. As this was shown in [**Sch38**], we only give the idea of this proof: Because of $\mathrm{g} > 1$, our function field has (finitely many) Weierstraß points. By proposition I.51, each automorphism yields a permutation of the Weierstraß points. If two automorphisms induce the same permutation, they differ by an automorphism fixing all Weierstraß points. [**Sch38**, Sätze 8 und 10] imply that the set of automorphisms fixing all Weierstraß points is finite. Thus, there can only be finitely many automorphisms.

8. Cantor's Representation of Divisor Classes

For hyperelliptic function fields to be usable for cryptographic purposes, it is essential to be able to compute effectively in Jacobians. In order to do so, it is necessary to find a unique representation of divisor classes (of degree 0) in a form which can easily be stored on a computing device. Furthermore, algorithms to compute the group law of the Jacobian need to be available.

David G. Cantor to presented such a representation and the corresponding algorithms (cf. [**Can87**]) for imaginary quadratic (hyper-)elliptic function fields over finite constant fields (of characteristic $\neq 2$). Hence, most cryptographers speak of the "Cantor representation" of divisors. Actually, Cantor's representation for a divisor class in $\mathbb{J}_{k(x,y)}$ is essentially a uniquely determined pair of generators of a so called reduced ideal in the integral closure of $k[x]$. These reduced ideals are uniquely determined elements of ideal class groups (i.e. fractional ideals modulo fractional principal ideals). Most of the theory on ideals in the integral closure of $k[x]$ and on ideal class groups was developed by Emil Artin ([**Art24**]). The connection between the geometric aspects like places, divisors or divisor class groups and the number theoretic point of view (prime ideals, ideals, ideal class groups) is explained in [**Kux03**, chapter 1] as well as in [**Ste01**, section 2].

Let us discuss Cantor's representation of divisor classes, now.

PROPOSITION I.53. *Let F/k be a (hyper-)elliptic function field in imaginary quadratic representation*[8] *and $y^2 = D(x)$ its defining equation. Then each divisor class $A \in \mathbb{J}_F$ can uniquely represented by a pair $a, b \in k[x]$ of polynomials with* $\mathrm{lc}(a) = 1$, $\deg_x(a) \leq \mathrm{g}_F$, $\deg_x(b) < \deg_x(a)$ *and* $a \mid b^2 - D$.

PROOF. [**Can87**, section 2] □

DEFINITION I.25. Let F/k be a (hyper-)elliptic function field in imaginary quadratic representation and $y^2 = D(x)$ its defining equation. Let $A \in \mathbb{J}_F$ and $a, b \in k[x]$, $\mathrm{lc}_x(a) = 1$, $\deg_x(a) \leq \mathrm{g}_F$, $\deg_x(b) < \deg_x(a)$ and $a \mid b^2 - D$ its representation as stated in proposition I.53. Then we denote A by $\mathrm{div}(a, b)$ and call this representation A's *Cantor representation.*

REMARK I.54. Actually, the Cantor representation specifies a specific type of divisors, the so called reduced divisors. If we drop the condition $\deg(a) \leq g$, we obtain semi-reduced divisors. Cantor's algorithm for adding divisor classes is split into two steps: First, a semi-reduced divisor equivalent to the sum is computed (composition step). In the second step, this divisor is reduced to obtain a Cantor representation of the sum as defined above (reduction step).

Let us start describing the composition step, first:

ALGORITHM I.1. Let F/k be a hyperelliptic function field in imaginary quadratic representation and $y^2 = D(x)$ its defining equation. Furthermore let $A_1, A_2 \in \mathbb{J}_F$ have the Cantor representations $A_1 = \mathrm{div}(a_1, b_1)$, $A_2 = \mathrm{div}(a_2, b_2)$. We compute polynomials $a, b \in k[x]$ which define a semi-reduced divisor in the class $A_1 + A_2 \in \mathbb{J}_F$.

(1) Compute $d_0 := (a_1, a_2)$ and $d := (d_0, b_1 + b_2)$ using the extended Euclidean algorithm, also obtaining $h_1, h_2, h_3 \in k[x]$ such that

$$d = h_1 a_1 + h_2 a_2 + h_3(b_1 + b_2).$$

(2) Let $a := \frac{a_1 a_2}{d^2} \in k[x]$.

(3) Let $b :\equiv \frac{1}{d}(h_1 a_1 b_2 + h_2 a_2 b_1 + h_3(b_1 b_2 + D)) \mod a$, such that $\deg_x(b) < \deg_x(a)$.

[8] Note that $\mathrm{char}(k) \neq 2$ was one of our preliminaries for (hyper-)elliptic function fields.

After computing a, b, we need to reduce it in order to obtain the Cantor representation $\operatorname{div}(a_3, b_3) = \operatorname{div}(a_1, b_1) + \operatorname{div}(a_2, b_2) \in \mathbb{J}_F$ of the sum of the given divisor classes. This is achieved by the following algorithm. Performance improvements of this algorithm have been described by Cantor himself ([**Can87**]) as well as by Sachar Paulus and Andreas Stein ([**PS98**]).

Algorithm I.2. We use the notations of algorithm I.1 and compute $a_3, b_3 \in k[x]$ such that $\operatorname{div}(a_3, b_3) = A_1 + A_2$.

```
(1) Let $u := a$, $v := b$.
(2) While $\deg(u) > g$, do
    (a) Let $u := \frac{D - v^2}{u}$.
    (b) Let $u := \frac{u}{\operatorname{lc}(u)}$.
    (c) Let $v :\equiv -v \mod u$, with $\deg(v) < \deg(u)$.
(3) Let $a_3 := u$, $b_3 := v$.
```

The correctness of the above algorithms is proved in [**Can87**]. As these algorithms enable us to compute effectively in the Jacobian of a (hyper-)elliptic curve, it is possible to use the Jacobian in crypto systems like Diffie-Hellman, ElGamal or DSA. This application will be discussed in chapter II.

CHAPTER II

Cryptographic Aspects

Neal Koblitz suggested Jacobians of hyperelliptic function fields to be used in public key crypto systems which are based on the discrete logarithm problem ([**Kob89**]). We will give some algorithms of this kind in section 1. Furthermore, we will introduce a method to encode text in divisor classes. In section 2, we will enumerate several known attacks on the hyperelliptic curve discrete logarithm problem. Of course, we will also give conditions under which these attacks are infeasible. We will see that it is essential to know the order of the Jacobian to be able to avoid most of these attacks. In section 3, we give an overview of the algorithms known to compute this order. There are two kinds of such algorithms: On the one hand, ones which are restricted to a small family of hyperelliptic function fields (e.g. fields with small characteristic or with complex multiplication), but which can be used to construct fields yielding secure key sizes. On the other hand, there are algorithms which compute the order of Jacobians of general hyperelliptic function fields. Unfortunately, these algorithms are too slow to construct fields with reasonable large Jacobians. Thus, it is desirable to have methods at hand which help to decide if the application of expensive divisor class counting algorithms is worthwhile for a given hyperelliptic function field. Finally, we will see in section 4 that the automorphism group of a hyperelliptic function field has an influence on the order of its Jacobian. Hence, a fast algorithm to compute automorphism groups is a promising method to decide, whether an expensive order counting algorithm should be applied to a given function field. This is one of the core motivations to compute automorphism groups (cf. chapter V).

1. Hyperelliptic Crypto Systems

In this section we present the most common cryptographic algorithms which use the discrete logarithm in Jacobians of hyperelliptic function fields as their trapdoor function. An introduction to cryptography can be found in [**Kob99**], [**Sch96**] or [**MvOV96**]. The shortest and most "mathematical" of these books is the one by Koblitz. Schneier's book is a computer science book, while the "handbook" ([**MvOV96**]) is best to be used as a reference book. [**Sin02**] is an amusing but nonscientific introduction to cryptography.

> *We assume all hyperelliptic function fields in this section to be in imaginary quadratic representation.*

This assumption is needed here, since we only gave a representation of divisor classes as well as algorithms to perform the arithmetic on the Jacobian of hyperelliptic function fields in imaginary quadratic representation (cf. section I.8). As described in [**PS98**], it also is possible to compute in the Jacobian of hyperelliptic function fields in real quadratic representation. According to Paulus and Stein, there is no real difference in the efficiency of the arithmetic in both of these cases. Therefore and because the representation is easier to describe in the imaginary quadratic case, the author decided to consider the latter case, only.

First of all, we recall the definition of the discrete logarithm problem. We state it specifically for Jacobians:

Definition II.1. Let F/k be a hyperelliptic function field, $A, B \in \mathbb{J}_F$ such that $B = nA$ for some unknown $n \in \mathbb{N}$. The *hyperelliptic curve discrete logarithm problem* (*HECDL*) is the problem to compute n from A and B.

For an arbitrary group the similar problem is called *discrete logarithm problem* (*DL*).

Koblitz conjectured the HECDL to be intractable for general hyperelliptic function fields—and most cryptographers share this opinion. Thus, the Jacobian seems to be suitable to be used in DL-based crypto systems. To achieve security, the Jacobian needs to yield key sizes of at least 160 bits, i.e. its group order has to exceed 2^{160}. Currently, the BSI ("Bundesamt für Sicherheit in der Informationstechnik", German Federal Office for Information Security) recommends to use 256 bit keys for elliptic and hyperelliptic crypto systems.

We continue describing the Diffie-Hellman key exchange protocol[1], an algorithm which allows two parties to obtain a common secret key.

Algorithm II.1. Two users A and B want to exchange a common secret key over public channels. To do so, they perform the following steps.

(1) First, A and B publicly negotiate a secure hyperelliptic function field F/k over a finite field and a divisor class $G \in \mathbb{J}_F$ such that $\operatorname{ord}(G) > 2^{160}$.
(2) A chooses a (secret) integer a with $1 < a < \operatorname{ord}(G)$, computes aG and sends it (publicly) to B.
(3) B chooses a (secret) integer b with $1 < b < \operatorname{ord}(G)$, computes bG and sends it (publicly) to B.
(4) A computes the shared key $a(bG) = (ab)G$, which B computes by $b(aG) = (ab)G$.

Using Cantor's algorithms (cf. section I.8), it obviously is possible to apply this algorithm in practice. The only difficulties are to choose a secure hyperelliptic function field as well as to compute the order of G, which is nearly as hard as computing the order of $\mathbb{J}_F$. We will discuss the choice of the field in section 2 and the order counting in section 3.

In addition to the Diffie-Hellman key exchange protocol, Jacobians can also be used for public key encryption and signature schemes. As an example, we present the ElGamal encryption algorithm[2], which essentially consists of an asymmetrically interpreted Diffie-Hellman key exchange and the addition of the "shared" key to the message.

Algorithm II.2. User A wants to send a message m to user B. Like in other public key protocols, B has to generate a pair of keys, first ("key generation"):

(1) B chooses a secure hyperelliptic function field F/k over a finite constant field, as well as a divisor class $G \in \mathbb{J}_F$ such that $\operatorname{ord}(G) > 2^{160}$.
(2) B chooses an integer b with $1 < b < \operatorname{ord}(G)$ and computes bG.
(3) B publishes F, G and bG, keeping b secret.

In order to send the message m to B, A has to do the following ("encryption"):

(1) A obtains B's public key (F, G, bG).

[1] [**MvOV96**, protocol 12.47 and remark 12.49]

[2] [**MvOV96**, algorithms 8.25 and 8.26]

(2) A chooses a random integer x with $1 < x < \operatorname{ord}(G)$.
(3) A computes xG and $x(bG) = bxG$.
(4) A encodes the message m in a divisor class $M \in \mathbb{J}_F$.
(5) A computes $M + bxG$ and sends xG and $M + bxG$ to B.

In order to recover the plain text ("decryption"), B computes $b(xG) = bxG$ and $(M + bxG) - bxG = M$. Decoding M yields the message m.

To be able to implement the ElGamal scheme, we need to know how to encode text in divisor classes. Furthermore, it is necessary to be able to compute the inverse of a divisor class. The latter problem is easy: If $G \in \mathbb{J}_F$ has the Cantor representation $G = \operatorname{div}(a, b)$, it is well known that $-G = \operatorname{div}(a, -b)$. This formula can easily be verified using the composition step of Cantor's addition algorithm (algorithm I.1).

Next, we present a possibility to encode text in divisor classes. The idea is to convert the text via an integer in the polynomial a of a class $M = \operatorname{div}(a, b)$. Unfortunately, b needs to be a square root of D (where $y^2 = D$ is a defining equation of F), which does not exist for every choice of a. Thus, it is necessary to include random bits in a.

Algorithm II.3. Encoding text in divisor classes.

Input: Let $F/\mathbb{F}_q$ be a hyperelliptic function field with defining equation $y^2 = D(x)$ and $m = (m_i)_{i=1,\dots,n}$ with $m_i \in \mathbb{Z}$, $0 \le m_i \le 255$ a string of bytes. Since typical key lengths[3] of hyperelliptic crypto systems are 160 to 256 bits, we can assume $2^{3 \cdot 8} \le q^{\mathrm{g}} \le 2^{256 \cdot 8}$.

Output: We encode the beginning of m in a divisor class $M = \operatorname{div}(a, b) \in \mathbb{J}_F$.

Steps:

(1) Let $b := \lfloor \log_2(q^{\mathrm{g}}) \rfloor$ be the number of bits encodeable in a monic polynomial $a \in \mathbb{F}_q[x]$ of degree $\le$ g and $l := \lfloor \frac{b}{8} \rfloor$ the number of encodeable bytes. If $l \ge n$, let $l := n + 1$.
(2) We set
$$a_{\mathrm{int}} := (l-1) + \sum_{i=1}^{l-1} 256^i m_i + 256^l r,$$
where r is a random integer such that $0 \le r < 2^{b-8l}$.
(3) We encode a_{int} in a monic polynomial $a \in \mathbb{F}_q[x]$. To do so, we compute a q-adic representation of a_{int} and use its digits $a_0, \dots, a_{\mathrm{g}-1}$ as coefficients of $a = x^{\mathrm{g}} + a_{\mathrm{g}-1}x^{\mathrm{g}-1} + \cdots + a_1 x + a_0$.
(4) We check if D is a square modulo a. If so, we compute one of the square roots b and continue with step 5. Otherwise, we return to step 2, decreasing l, if all possible paddings r failed for the current l.
(5) Finally, we define $M := \operatorname{div}(a, b)$ to be the encoding of $m_1, m_2, \dots, m_{l-1}$. The remainder of m needs to be encoded in additional divisor classes.

Our assumption $2^{3 \cdot 8} \le q^{\mathrm{g}} \le 2^{256 \cdot 8}$ has two implications: On the one hand, $q^{\mathrm{g}} \le 2^{256 \cdot 8}$ implies $l \le 256$, i.e. it is possible to encode $l - 1$ in a single byte. Thus it is easily possible to reconstruct l, as well as $m_1, \dots, m_{l-1}$ from a_{int}. On the other hand, practical tests suggest that a random padding of one byte suffices to find an a such that D is a square modulo a. Thus, $q^{\mathrm{g}} \ge 2^{3 \cdot 8}$ implies that each divisor class contains at least one byte of our message.

[3] i.e. group sizes, by the Hasse-Weil theorem (proved in [**Art24**, §24], assuming Riemann's hypothesis, a proof of which can be found in [**Roq53**]), we have $|\mathbb{J}_F| \approx q^g$.

If we want to implement algorithm II.3, we need to be able to check, whether D is a square modulo a and to construct a square root b, if it is (step (4))—the remaining obstacles have been discussed, above.

In order to check, if D possibly is a square modulo a, we compute the *Jacobi symbol* $\left(\frac{D}{a}\right)$, which is the product of all $\left(\frac{D}{P}\right)$, where $P \mid a$ is a prime polynomial and

$$\left(\frac{D}{P}\right) := \begin{cases} -1 & \text{, if } P \nmid D \text{ and } D \text{ is no square} \mod P, \\ 0 & \text{, if } P \mid D, \\ 1 & \text{, if } P \nmid D \text{ and } D \text{ is a square} \mod P. \end{cases}$$

Thus, if $\left(\frac{D}{a}\right) \neq 1$, we know that D is no square modulo a. If, on the other hand, $\left(\frac{D}{a}\right) = 1$, we cannot infer that D is a square, because $\left(\frac{D}{a}\right)$ may as well be the product of several -1-s. At least $\left(\frac{D}{a}\right) = 1$ is a necessary condition that D is a square modulo a, which can be computed fast. To obtain the Jacobi symbol, we use the law of reciprocity and Euler's criterion in the obvious way. Both of these can be found in [**Art24**, §15–16].

If $\left(\frac{D}{a}\right) = 1$, we hope that D is a square modulo a and try to compute its square root in the following way: We start factoring $a = a_1^{e_1} \cdots a_n^{e_n}$ into irreducible factors such that the a_i are pairwise relatively prime. For each a_i we try to compute a square root b_i' of D modulo a_i using the algorithm of Tonelli-Shanks, which can for example be found in [**Lin97**]. If D is no square modulo a_i, Tonelli-Shanks will fail and report this fact. Then, D can also be no square modulo a. Otherwise, we obtain a square root b_i' modulo a_i for each $i = 1, \ldots, n$. In order to obtain square roots b_i modulo $a_i^{e_i}$, we compute a p-adic approximation of such a root using Newton iterations. Finally, we construct a square root b modulo a from the b_i using the Chinese remainder theorem.

2. Attacks on HECC

The security of crypto algorithms like the ones presented in section 1 depends mostly on the condition whether the HECDL is hard. In fact, the only known attacks against Diffie-Hellman, ElGamal and the like actually try to solve the corresponding DL. Thus, in this section, we list attacks against HECDL and provide countermeasures against them.

The Pohlig-Hellman Attack: The Pohlig-Hellman algorithm ([**PH78**]) is both the oldest and the most general of the attacks against DL crypto systems. It solves a discrete logarithm over a group G in each of its subgroups separately and constructs the solution for G using the Chinese remainder theorem. If G consists of many small subgroups, this obviously is easy, since the subgroup's DL can be solved by Pollard's ρ-method ([**Pol78**], [**Pol00**]), Shank's baby-step giant-step algorithm or even by brute force. Because the subgroups of any finite group G are in 1-1 relation to the divisors of $\operatorname{ord}(G)$, it is necessary that $|\mathbb{J}_F|$ contains a large[4] prime factor in order for $\mathbb{J}_F$ to be secure against Pohlig-Hellman attacks.

The Duursma-Gaudry-Morain Attack: Iwan M. Duursma, Pierrick Gaudry and Francois Morain proposed a possibility to speed up Pollard's ρ-method by a factor of $\sqrt{m}$, if there is an automorphism α of order m on the group $\mathbb{J}_F$, which can be evaluated easily ([**DGM99**]). Let $A = \langle \alpha \rangle$ be the cyclic group generated by α. Duursma, Gaudry and Morain applied the ρ-method to the quotient group G/A, i.e. the group of equivalence classes

[4] i.e. greater than 2^{160}.

of elements of G, where $f \sim g$ iff $g = \alpha^i(f)$ for some $i \in \mathbb{Z}$. Numerical experiments yielded complexities which are close to those predicted by theory.

By proposition I.28, each field automorphism of F/k induces a group automorphism of $\mathbb{J}_F$. Thus, it is sensible to avoid hyperelliptic function fields with large automorphism groups.

The Frey-Rück Attack: In [**FR94**], Gerhard Frey and Hans-Georg Rück generalized the MOV attack ([**MOV93**]) to hyperelliptic function fields using the so called Tate pairing, which embeds the Jacobian of $F/\mathbb{F}_q$ into $\mathbb{F}_{q^l}$ for some $l \in \mathbb{N}$. Using, for example, the index calculus method, the DL in this field has subexponential complexity.

In order to render the Frey-Rück attack unfeasible, we have to assure that $\mathbb{F}_{q^l}$ is so large that the DL cannot be solved effectively. To do so, we follow the advice from [**SSI98**]: Let p_0 be the largest prime divisor of $|\mathbb{J}_F|$. We only allow hyperelliptic function fields, where p_0 does not divide $q^l - 1$ for all positive integers l with $l < (\log_2(q))^2$.

The Adleman-DeMarrais-Huang Attack: Leonard M. Adleman, Jonathan DeMarrais and Ming-Deh Huang presented an index-calculus like algorithm to solve the hyperelliptic curve discrete logarithm problem which is efficient for hyperelliptic function fields of high genus ([**ADH94**]). Their method was improved by Pierrick Gaudry ([**Gau00**]), rendering fields of genus > 4 to be insecure.

This attack can easily be prevented, if we use hyperelliptic function fields of genus ≤ 4, only.

The Rück Attack: If $\mathbb{J}_F$ has a cyclic subgroup of order p^n, where $p = \mathrm{char}(k)$ and $n \in \mathbb{N}$, Hans-Georg Rück presented an algorithm to compute the discrete logarithm in this subgroup by $\mathcal{O}(n^2 \log(p))$ operations in k ([**Rüc99**]).

This attack can be prevented, if we assert $p \nmid |\mathbb{J}_F|$ or $p \nmid \mathrm{ord}(G)$, where G is the generator used in our crypto system.

Summing up, the Adleman-DeMarrais-Huang attack can easily be avoided, since the genus of a hyperelliptic function field is obvious from the degree of its defining polynomial. In order to prevent the Duursma-Gaudry-Morain attack, we need to assure that the automorphism group is small. Ideally, $\mathrm{Aut}(F/k)$ ought to be trivial, i.e. it should not contain any automorphism beside the hyperelliptic involution $x \mapsto x$, $y \mapsto -y$. The remaining attacks can most easily be guarded against, if $|\mathbb{J}_F|$ is known. We will see in section 4 that the order of $\mathbb{J}_F$ also depends on the automorphism group. Thus, it is sensible to compute $\mathrm{Aut}(F/k)$ in order to avoid insecure hyperelliptic function fields.

3. Known Algorithms for Computing the Order of Jacobians

As we have seen in section 2, many attacks on hyperelliptic crypto systems can be prevented, if the order of the Jacobian is known. In this section we will see some of the currently available methods to compute this group order and to construct secure hyperelliptic function fields.

3.1. Zeta Functions. If $F/\mathbb{F}_p$ is a hyperelliptic function field with small constant field of characteristic p, it is quite easy to compute $|\mathbb{J}_F|$ using F's zeta function

$$\zeta(s) := \sum_{n=0}^{\infty} A_n s^n, \quad \text{where } A_n := |\{A \in \mathcal{D}_F \mid A \geq 0 \text{ and } \deg(A) = n\}|,$$

which has been developed by Artin ([**Art24**]). If F has an imaginary quadratic defining equation $y^2 = D(x)$, Artin proved that

$$\zeta(s) = \frac{1}{1-p^{1-s}} \sum_{n=0}^{2\mathrm{g}} \frac{\sigma_n}{p^{ns}}, \quad \text{where } \sigma_n := \sum_{\substack{P \in \mathbb{F}_p[x], \deg(P)=n,\\ \mathrm{lc}(P)=1}} \left(\frac{D}{P}\right).$$

In order to compute the σ_n, the formula $\sigma_{2g-n} = p^{g-n}\sigma_n$ is essential, since it allows to compute only $\sigma_0, \ldots, \sigma_g$ by adding the corresponding Jacobi symbols. The order of $\mathbb{J}_F$ can be obtained via

$$|\mathbb{J}_F| = \zeta(0) = \sum_{n=0}^{2\mathrm{g}} \sigma_n.$$

Furthermore, zeta functions can be used to compute the order of the Jacobian of constant field extensions of F. To do so, we factor

$$L(s) := (1-s)(1-ps)\zeta(s) =: \prod_{i=1}^{\mathrm{g}} (1-\alpha_i s)(1-\overline{\alpha_i} s)$$

over $\mathbb{C}$, where $\overline{\alpha_i}$ denotes the complex conjugate of α_i. Then the Weil conjecture (e.g. [**Kob99**, chapter 6, theorem 5.1]) implies

$$|\mathbb{J}_{F\mathbb{F}_{p^r}}| = \prod_{i=1}^{\mathrm{g}} |1-\alpha_i^r|^2$$

for each $r \in \mathbb{N}_+$. This method to compute the cardinality of Jacobians was proposed by Koblitz ([**Kob89**]) for char$(k) = 2$. For odd characteristic, it can be found in [**Sti93**, chapter V] or in [**Kob99**, chapter 6]. It was used by Yasuyuki Sakai and Kouichi Sakurai to construct secure hyperelliptic function fields ([**SS98**]). For example, they provided the following secure hyperelliptic function fields:

- $\mathbb{F}_{3^{59}}(x,y)$, $y^2 = x^5 + x^4 + x^3 + x + 1$ has a 185-bit prime divisor of $|\mathbb{J}|$.
- $\mathbb{F}_{5^{43}}(x,y)$, $y^2 = u^5 + u^2 + 1$ has a 200-bit prime divisor of $|\mathbb{J}|$.
- $\mathbb{F}_{7^{37}}(x,y)$, $y^2 = u^5 + u^3 + u^2 + u + 1$ has a 208-bit prime divisor of $|\mathbb{J}|$.

Using his own implementation, the author was also able to find secure hyperelliptic function fields of small characteristic. One such example[5] is given by $\mathbb{F}_{3^{61}}(x,y)$, $y^2 = x^5 + x^4 + x$. Here $|\mathbb{J}| = 8q$, where q is a prime of 191 bit.

Nowadays, zeta functions can also be computed in hyperelliptic function fields over large constant fields of small characteristic: The defining equations no longer need to be defined over the prime field. Instead they may be defined over any field of small characteristic. The most famous of these algorithms was presented by Kiran Kedlaya ([**Ked01**]). It uses the so called Monsky-Washnitzer cohomology to compute the trace of the Frobenius endomorphism, which in turn yields the divisor class number $|\mathbb{J}|$. Kedlaya's algorithm works for hyperelliptic function fields of characteristic $\neq 2$. It has been extended to characteristic 2 by Jan Denev and Frederik Vercauteren ([**DV02**]).

3.2. CM-Method. Annegret Weng proposed a totally different approach to obtain secure hyperelliptic function fields ([**Wen03**]). Instead of choosing a random field and computing its Jacobian's order Weng chooses the desired order of the Jacobian, first and tries to construct a hyperelliptic function field with complex multiplication, which has exactly the given divisor class number.

[5] cf. example VI.1.

Weng's algorithm is a generalization of the CM-method used to construct elliptic curves of given size. It was implemented and can be used online at cv cryptovision's "Kurvenfabrik" ([**ccG**]).

3.3. Weil Descent. Pierrick Gaudry, Florian Hess and Nigel P. Smart presented the strategy of Weil descent in [**GHS00**], which yields a homomorphism ϕ between an elliptic curve E over $\mathbb{F}_{q^n}$ and the Jacobian $\mathbb{J}$ of a hyperelliptic curve H over $\mathbb{F}_q$, where q is a power of 2. Using ϕ, it becomes possible to translate the discrete logarithm problem of E to $\mathbb{J}$. Furthermore Weil descent can be used to construct hyperelliptic curves from elliptic ones in such a way that the order of the Jacobian has a large prime factor: We choose an elliptic curve whose order has such a large prime factor. This can be done choosing random elliptic curves and counting their $\mathbb{F}_{q^n}$-rational points by `SEA`[6] or Satoh's algorithm[7]. Then the order of the Jacobian of H shares this prime factor, if the generator of the corresponding subgroup of E does not lie in the kernel of ϕ. Of course, the latter property can be tested easily.

We will give a crude sketch of the Weil descent idea. Let $E : y^2 + xy = x^3 + \alpha x^2 + \beta$, $\alpha, \beta \in \mathbb{F}_{q^n}$ be an elliptic curve, where q is a power of 2. We choose a basis $\{\psi_0, \ldots, \psi_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and use it to express E over $\mathbb{F}_q$. This yields an n-dimensional variety A over $\mathbb{F}_q$, which is called the *Weil restriction* of E. The process constructing A from E is called *Weil descent*.

We restrict $x = x_0\psi_0 + \cdots + x_{n-1}\psi_{n-1}$ to lie in $\mathbb{F}_q$, which yields a subvariety $\mathcal{C}$ of A, which is birationally equivalent to the curve $\mathcal{D}$ over $\mathbb{F}_{q^n}$, given by

$$\mathcal{D} : \begin{cases} w_0^2 + xw_0 + x^3 + \alpha_0 x^2 + \beta_0 = 0, \\ \vdots \\ w_{n-1}^2 + xw_{n-1} + x^3 + \alpha_{n-1}x^2 + \beta_{n-1} = 0, \end{cases}$$

where $\alpha_i = \sigma^i(\alpha)$, $\beta_i = \sigma^i(\beta)$, σ is the Frobenius endomorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $(x, y) \in E$, $x \in \mathbb{F}_q$ implies $w_i = \sigma^i(y)$ for some i.

Let F be the splitting field of the equations defining $\mathcal{D}$ over $\mathbb{F}_{q^n}(x)$ and $[F : \mathbb{F}_{q^n}(x)] =: 2^m$. Furthermore let $\sigma : F \to F$ be the automorphism induced by the Frobenius $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and $F' \subseteq F$ be its fixed field. Then, $\mathcal{C}$ has an irreducible reduced component H, which is a hyperelliptic curve of genus 2^{m-1} or $2^{m-1} - 1$ over $\mathbb{F}_q$ and F' is its function field.

According to [**GHS00**], the method of Weil descent can be used to construct hyperelliptic curves from most elliptic curves over $\mathbb{F}_{q^n}$, where q is a power of 2 and n is quite small. For elliptic curves over $\mathbb{F}_{2^p}$, where p is prime, it is very unlikely to find a hyperelliptic curve whose genus is low enough to be secure. For odd characteristic, Weil descent techniques are not well developed.

Florian Hess, Gadiel Saroussi and Nigel Smart used Weil descent to construct secure hyperelliptic curves provably at random ([**HSS00**]). Applying `SHA-1`[8] to a random text, a string of random bits is generated, which is used to construct an elliptic curve E. Using `SEA`[9], the order of E is computed. Weil descend yields a hyperelliptic curve H such that possible divisors of $|\mathbb{J}|$ are known. If H does not resist the common attacks, another curve is generated in the same way. Otherwise, H is used.

[6] the Schoof-Elkies-Atkin algorithm, which is an improvement of [**Sch95**]

[7] [**Sat00**], which was generalized and implemented in [**FGH00**].

[8] [**MvOV96**, algorithm 9.53]

[9] Today, Satoh's algorithm ought to be preferred

Steven Galbraith generalized the technique of Weil descent from elliptic to hyperelliptic curves ([**Gal01**]). If a hyperelliptic curve C of genus g over $\mathbb{F}_{q^n}$, q even, satisfies several conditions, it is possible to construct a curve H of genus at most $\mathrm{g}2^{m-1}$ to which discrete logarithm problems on C can be transmitted. The constant m is defined like above.

Galbraith even successfully applied Weil descent to some curves of odd characteristic, although theory does not guarantee this to work.

3.4. AGM Method (Gaudry-Harley). Pierrick Gaudry and Robert Harley describe several algorithms which yield information about the order of the Jacobian $\mathbb{J}$ of an imaginary quadratic hyperelliptic curve C of genus 2 over a finite field $\mathbb{F}_q$ of characteristic $p \neq 2$ ([**GH00**]). This information can be combined to compute the actual order. The most important of these algorithms is a generalization of `SEA`, the Schoof-Atkin-Elkies algorithm.

(1) The *birthday paradox algorithm*, which is a distributed version of Pollard's lambda method ([**Pol78**]), searches for $|\mathbb{J}|$ in the *Hasse-Weil interval* ([**Art24**, §24], [**Roq53**])
$$\lceil(\sqrt{q}-1)^{2g}\rceil \leq |\mathbb{J}| \leq \lfloor(\sqrt{q}+1)^{2g}\rfloor,$$
whose width is $w := 2\lfloor 4\sqrt{q}(q+1)\rfloor$ and whose center is $c := q^2+6q+1$.
Given a divisor D, its order is computed in the following way using M machines: Choose some uncommon[10] property P of divisors, a hash function h that maps divisors to a small set of integers $\{1,\ldots,l\}$ and l random positive integers l_i, $1 \leq i \leq l$, which are near $M\sqrt{w}$. Precompute $D_i := l_i D$ and $E := cD$.
Now, each computer picks some integer $r < w$ and a bit b at random and computes
$$R := \begin{cases} rD & \text{if } b = 0, \\ rD + E & \text{if } b = 1. \end{cases}$$
While R does not satisfy P, we update $r := r + l_{h(R)}$ and $R := R + D_{h(R)}$. The triple (R, b, r), where R has the property P, is stored on a central server. If there are triples $(R, 0, r)$ and $(R, 1, r')$ with $r \neq r' + c$, we may stop, since $r' + c - r$ is a multiple of $\mathrm{ord}(D)$, which is factored to find $\mathrm{ord}(D)$.
To compute $|\mathbb{J}|$, we compute the order of several random divisors, whose least common multiple n is usually greater than w. Then $|\mathbb{J}|$ is the unique multiple of n in the Hasse-Weil interval. However, in rare cases $n \geq w$ cannot be obtained. Gaudry and Harley "do not yet have a completely satisfactory solution for such a rare case".

(2) The *Hasse-Witt matrix* A of C can be used for calculating $|\mathbb{J}|$ modulo $p := \mathrm{char}(\mathbb{F}_q)$: Let $C : y^2 = f(x)$ be a hyperelliptic curve and $(f(x))^{(p-1)/2} = \sum c_i x^i$. Then $A = (c_{i,p-j})_{1 \leq i,j \leq g}$. Let $\kappa(t)$ be the characteristic polynomial of the matrix $AA^pA^{p^2}\cdots A^{q/p}$ and $\chi(t)$ the characteristic polynomial of the Frobenius endomorphism ϕ of $\mathbb{J}$. Then $\chi(t) \equiv (-1)^g t^g \kappa(t) \mod p$, which yields $|\mathbb{J}| \equiv (-1)^g \kappa(1) \mod p$.

(3) The afore mentioned *Schoof-like algorithm* is used to find divisors D with $lD = 0$, where $l \neq p$ is some small prime. Using several such divisors, $\chi(t)$ may be computed modulo l, since $\chi(\phi) = 0$, i.e.
$$(\chi \bmod l)(\phi(D)) = 0.$$

[10] i.e. P occurs with a probability substantially less than $\sqrt{w}/M$.

This algorithm, which is too complex to be presented here, depends on the assumption $g = 2$.

(4) A *lifting of* 2*-power torsion divisors* can be used to determine $|\mathbb{J}|$ modulo small powers of 2. Factoring f yields a 2-torsion[11] divisor $D = \operatorname{div}(u, 0)$ of $\mathbb{J}$, where $u \mid f$ and $\deg(u) \leq g$. Repeated halving of D, which is done using Gröbner bases, yields a 2^k-torsion divisor, which gives information on $|\mathbb{J}| \bmod 2^k$ again. To be able to halve a divisor, it is often necessary to extend the constant field.

Combining these algorithms, Gaudry and Harley were able to deduce $|\mathbb{J}|$ for random curves, where $|\mathbb{J}|$ has about 30 decimal digits, in a few days. Improving these algorithms, Gaudry computed $|\mathbb{J}|$ of a hyperelliptic function field over $\mathbb{F}_{5\cdot 10^{24}+41}$ whose Jacobian's order had even 50 decimal digits ([**Gau02**]).

4. A Theorem by Madan and its Practical Consequences

By investigating the involutions in $\operatorname{Aut}(F/k)$, Tony Shaska characterized the genus 2 function fields over an algebraically closed field k of $\operatorname{char}(k) \neq 2$, which contain degree 2 elliptic subfields ([**Sha00**]): $\operatorname{Aut}(F/k)$ is isomorphic to one of the following groups: $\mathcal{C}_2, \mathcal{C}_{10}$, Klein's four-group $\mathcal{D}_2$, the dihedral groups $\mathcal{D}_4$ or $\mathcal{D}_6$, $\mathcal{C}_3 \rtimes \mathcal{D}_4$, $\mathcal{C}_2 \times \mathcal{S}_5$ or W_1, where W_1 is a central extension[12] of the permutation group $\mathcal{S}_4$. Therefore, $\operatorname{Aut}(F/k)$ has (exactly) two conjugation classes of elliptic involutions[13] in the cases $\mathcal{D}_2$, $\mathcal{D}_4$, $\mathcal{D}_6$ and $\mathcal{C}_3 \rtimes \mathcal{D}_4$. If $\operatorname{Aut}(F/k)$ is isomorphic to $\mathcal{C}_2 \times \mathcal{S}_5$ or W_1, there is exactly one class; in the remaining cases, there are no elliptic involutions at all. Since each elliptic involution fixes a degree 2 elliptic subfield of F and vice versa, this characterizes the degree 2 elliptic subfields completely.

In the case $\operatorname{char}(k) = 0$, Shaska has shown that each genus 2 function field, which contains a degree 2 elliptic subfield, is of the form $F = k(x, y)$, where $y^2 = D_x := x^6 - s_1x^4 + s_2x^2 - 1$, $s_1, s_2 \in k$ and $27 - 18s_1s_2 - s_1^2s_2^2 + 4s_1^3 + 4s_2^3 \neq 0$. The elliptic subfield is given by $u^2 = D_t := x^3 + s_1x^2 + s_2x - 1$. It is obvious that these formulas define genus 2 hyperelliptic function fields with degree 2 elliptic subfields in each characteristic $\neq 2$. The above facts can also be deduced from Brandt's theorem (theorem V.6). The inequality $27 - 18s_1s_2 - s_1^2s_2^2 + 4s_1^3 + 4s_2^3 \neq 0$ assures that D_x and D_t both are separable[14].

Example II.1. We choose $k := \mathbb{F}_{101}$, $s_1 := 17$ and $s_2 := 6$. Then $27 - 18s_1s_2 - s_1^2s_2^2 + 4s_1^3 + 4s_2^3 \equiv 21 \not\equiv 0 \mod 101$ and we obtain the hyperelliptic function field $F := \mathbb{F}_{101}(x, y)$, $y^2 = x^6 - 17x^4 + 6x^2 - 1$. Using `KASH` ([**DFK$^+$97**]), we obtain $|\mathbb{J}_F| = 7728$.

The elliptic subfield $E := \mathbb{F}_{101}(x^2, y)$ has $|\mathbb{J}_E| = 92$, which is a divisor of 7728.

Examining several such examples, one conjectures that $|\mathbb{J}_E|$ divides $|\mathbb{J}_F|$ whenever $E \subseteq F$ is a degree 2 elliptic subfield of a genus 2 hyperelliptic function field.

Madan's theorem (theorem II.1 below) implies that this actually is the case. Furthermore, the property $|\mathbb{J}_F| \bigm| |\mathbb{J}_{F'}|$ even holds in the more general case, where F'/F is a finite Galois extension of function fields over a finite constant field.

As seen in section 2, the order of a secure Jacobian needs to contain a large prime factor. If $F \subseteq F'$ is a hyperelliptic subfield with reasonably large Jacobian, $|\mathbb{J}_{F'}|$ is divided by $|\mathbb{J}_F|$. Thus, if $\mathbb{J}_F$ is secure, considering $\mathbb{J}_{F'}$ may not yield bigger security.

[11] i.e. a divisor D with $2D = 0$

[12] Please refer to Shaska's paper for a definition of W_1.

[13] i.e. involutions which are different from the hyperelliptic one.

[14] $27 - 18s_1s_2 - s_1^2s_2^2 + 4s_1^3 + 4s_2^3$ is the discriminant of D_x

On the other hand, if $\mathbb{J}_F$ is large but insecure, $|\mathbb{J}_{F'}|$ shares the small prime divisors of $|\mathbb{J}_F|$, which implies that $\mathbb{J}_{F'}$ is either insecure or much larger than necessary for its level of security.

Example II.2. Let $k := \mathbb{F}_{53}$, $F := k(x, y)$, $y^2 = x^5 + 2x^4 + 37x^3 + 18x^2 + 6x + 52$ and $F' := k(t, u)$, $u^2 = t^{10} + 30t^9 + 36t^8 + 2t^7 + 8t^6 + t^5 + 2t^4 + 14t^3 + 31t^2 + 11t + 8$ Setting $x := (t + 3)^2$ and $y := u$ we see $F \subseteq F'$. Using KASH, we obtain $|\mathbb{J}_F| = 2940$ and $|\mathbb{J}_{F'}| = 8596560 = 2940 \cdot 2924$.

Let us state Madan's theorem, now.

Theorem II.1. *(Madan) Let F/k be a function field over a finite constant field k and let F'/k' be a finite Galois extension of F/k, i.e. F'/k' is a function field and F'/F is a finite Galois extension. Furthermore, we assume $k = \tilde{k}$ and $k' = \tilde{k}'$. Then $|\mathbb{J}_F|$ divides $|\mathbb{J}_{F'}|$.*

A purely algebraic proof using cohomological methods can be found in [**Mad70**], while a purely analytical one is given in [**Ros02**, chapter 14]. We will present a proof similar to Madan's first one ([**Mad68**], [**Mad69**]) in the remainder of this section.

We start proving another fact due to Madan which implies Madan's theorem in some cases (theorem II.4): Let $e_1, \dots e_m$ be the ramification indices of the places ramified in a finite Galois extension F'/F of degree n, where both F' and F are function fields over the same constant field. Then $e_1 \cdots e_m \cdot |\mathbb{J}_F|$ is a divisor of $n^2 \cdot |\mathbb{J}_{F'}|$. The connection to Madan's theorem is that theorem II.4 implies $d \bigm| |\mathbb{J}_{F'}|$ for each divisor d of $|\mathbb{J}_F|$ which is relatively prime to n.

In order to do prove theorem II.4, we need the following lemmas.

Lemma II.2. *Let F/k be a function field over a finite constant field, F'/k a finite Galois extension of F/k such that $k = \tilde{k}$, $G := \operatorname{Aut}(F'/F)$ the corresponding Galois group and $\mathcal{D}_{F'}^G \leq \mathcal{D}_{F'}$ and $\mathcal{D}_{F'}^{0G} \leq \mathcal{D}_{F'}^0$ the subgroups of divisors fixed by G.*

Then $\mathcal{D}_{F'}^{0G} + \operatorname{Con}_{F'/F}(\mathcal{D}_F) \leq \mathcal{D}_{F'}^G$ and $[\mathcal{D}_{F'}^G : \mathcal{D}_{F'}^{0G} + \operatorname{Con}_{F'/F}(\mathcal{D}_F)]$ divides $[F' : F]$.

Proof. $\mathcal{D}_{F'}^{0G} + \operatorname{Con}_{F'/F}(\mathcal{D}_F) \leq \mathcal{D}_{F'}^G$ is obvious, since both $\mathcal{D}_{F'}^{0G}$ and $\operatorname{Con}_{F'/F}(\mathcal{D}_F)$ are subgroups of $\mathcal{D}_{F'}^G$. Reducing the degree of a divisor modulo $n := [F' : F]$ obviously is a group homomorphism

$$\varphi : \mathcal{D}_{F'}^G \to \mathbb{Z}/n\mathbb{Z}, \quad A \mapsto \deg(A) \bmod n.$$

By proposition I.20, $n \bigm| \deg(\operatorname{Con}_{F'/F}(A))$ for each $A \in \mathcal{D}_F$, i.e. $\mathcal{D}_{F'}^{0G} + \operatorname{Con}_{F'/F}(\mathcal{D}_F)$ is a subgroup of $\operatorname{Ker}(\varphi)$.

Conversely, let $A \in \operatorname{Ker}(\varphi)$, i.e. $A \in \mathcal{D}_{F'}^G$ with $n \bigm| \deg(A)$. By [**Sch31**, page 27], the greatest common divisor of the degrees of all places of F is 1. Thus, there exists a divisor $B \in \mathcal{D}_F$ such that $\deg(B) = 1$. Then $\deg(A - \frac{\deg(A)}{n} \cdot \operatorname{Con}_{F'/F}(B)) = 0$, i.e. $A \in \mathcal{D}_{F'}^{0G} + \operatorname{Con}_{F'/F}(\mathcal{D}_F)$.

Thus, $\operatorname{Ker}(\varphi) = \mathcal{D}_{F'}^{0G} + \operatorname{Con}_{F'/F}(\mathcal{D}_F)$, i.e. $[\mathcal{D}_{F'}^G : \mathcal{D}_{F'}^{0G} + \operatorname{Con}_{F'/F}(\mathcal{D}_F)] \bigm| n$. □

Lemma II.3. *Let F/k be a function field over a finite constant field k. Let F'/k be a finite Galois extension of F/k with $k = \tilde{k}$, $G := \operatorname{Aut}(F'/F)$ the corresponding Galois group and $\mathcal{P}_{F'}^G \leq \mathcal{P}_{F'}$ the subgroup of divisors fixed by G.*

Then $\operatorname{Con}_{F'/F'}(\mathcal{P}_F) \leq \mathcal{P}_{F'}^G$ and $[\mathcal{P}_{F'}^G : \operatorname{Con}_{F'/F'}(\mathcal{P}_F)]$ divides $n := [F' : F]$. If $|k^*| > n$, we even have $[\mathcal{P}_{F'}^G : \operatorname{Con}_{F'/F'}(\mathcal{P}_F)] = 1$.

PROOF. That $\mathrm{Con}_{F'/F'}(\mathcal{P}_F)$ is a subgroup of $\mathcal{P}_{F'}^G$ is obvious. Let $m = |k^*|$, $A := \{x \in (F')^* \mid x^m \in F^*\}$ and

$$\varphi : A \to \mathcal{P}_{F'}^G, \quad x \mapsto (x)^{F'}.$$

First, we show that $(x)^{F'}$ is indeed fixed by G. Let $x \in A$ and $\sigma \in G$. Then $x^m \in F$, i.e. $\sigma(x^m) = x^m$. We obtain $\left(\frac{\sigma(x)}{x}\right)^m = \frac{\sigma(x^m)}{x^m} = 1$. Hence, $\frac{\sigma(x)}{x}$ is algebraic over k, i.e. $\frac{\sigma(x)}{x} \in \tilde{k} = k$. Thus $(\sigma(x)) - (x) = (\frac{\sigma(x)}{x}) = 0$, which yields $(x) \in \mathcal{P}_{F'}^G$. Therefore, φ can be defined in the above way.

Next, we will see that φ is surjective. Let $x \in F'$ such that $(x) \in \mathcal{P}_{F'}^G$. Then $(\sigma(x)) = (x)$ for each $\sigma \in G$. Thus $(\frac{\sigma(x)}{x}) = 0$ for each σ, from which we infer $\frac{\sigma(x)}{x} \in k$ by proposition I.7. Because of $m = |k^*|$, we obtain $\left(\frac{\sigma(x)}{x}\right)^m = 1$, i.e. $\sigma(x^m) = x^m$ for each $\sigma \in G$. Thus, $x^m \in (F')^G = F$, i.e. $x \in A$. Therefore, φ is surjective.

Let $\varphi(x) = 0$, i.e. $(x)^{F'} = 0$. Then we have $x \in k^* \subseteq F^*$. Thus, the kernel of φ is contained in F^*. Next, we will see that F^* is the pre-image of $\mathrm{Con}_{F'/F}(\mathcal{P}_F)$. The inclusion $\varphi(F^*) \subseteq \mathrm{Con}_{F'/F}(\mathcal{P}_F)$ follows from proposition I.20. Let $x \in A$ and $y \in F$, such that $(x)^{F'} = \mathrm{Con}_{F'/F}((y)^F) = (y)^{F'} \in \mathrm{Con}_{F'/F}(\mathcal{P}_F)$. Then $(\frac{x}{y})^{F'} = (x)^{F'} - (y)^{F'} = 0$. Thus $\frac{x}{y} \in k \subseteq F$ as above, i.e. $x \in F^*$. Hence $\varphi^{-1}(\mathrm{Con}_{F'/F}(\mathcal{P}_F)) = F^*$.

Summing up, we proved that φ induces a group isomorphism

$$A/F^* \cong \mathcal{P}_{F'}^G/\mathrm{Con}_{F'/F}(\mathcal{P}_F).$$

Let $F_0 := F(A)$. By Kummer theory ([**Art73**, Satz 32]), the character group C of $\mathrm{Aut}(F_0/F)$ is isomorphic to A/F^*. Since $C \cong \mathrm{Aut}(F_0/F)$ (cf. [**Art73**, pages 60f]), we obtain

$$[\mathcal{P}_{F'}^G : \mathrm{Con}_{F'/F}(\mathcal{P}_F)] = [A : F^*] = |\mathrm{Aut}(F_0/F)| = [F_0 : F] \bigm| [F' : F] = n.$$

If $|k^*| > n$, i.e. $m > n$ we have $[F_0 : F] = 1$. Otherwise we had $m \bigm| [F_0 : F] \bigm| n$, which is impossible. □

Using these lemmas, we can prove theorem II.4:

THEOREM II.4. *Let F/k be a function field over a finite constant field k. Let F'/k be a finite Galois extension of F/k of degree $[F' : F] = n$ with $k = \tilde{k}$ and $P_1', \dots, P_m' \in \mathbb{P}_{F'}$ the ramified places of F'/F. We denote their ramification indices by $e_i := \mathrm{e}(P_i'/P_i' \cap F)$.*

Then $e_1 \cdots e_m \cdot |\mathbb{J}_F|$ divides $n^2 \cdot |\mathbb{J}_{F'}|$. If $|k^*| > n$, we even have that $e_1 \cdots e_m \cdot |\mathbb{J}_F|$ divides $n \cdot |\mathbb{J}_{F'}|$.

PROOF. Let $G := \mathrm{Aut}(F'/F)$ and $\mathcal{D}_{F'}^G \leq \mathcal{D}_{F'}$, $\mathcal{P}_{F'}^G \leq \mathcal{P}_{F'}$ and $\mathcal{D}_{F'}^{0G} \leq \mathcal{D}_{F'}^0$ be the subgroups of divisors fixed by G.

We deduce from proposition I.27 that $\mathcal{D}_{F'}^G$ is generated by all divisors of the form

$$\sum_{P' \in \mathbb{P}_{F'},\, P'|P} P',$$

where $P \in \mathbb{P}_F$. A divisor $a \sum_{P'|P} P' \in \mathcal{D}_{F'}^G$ is an element of $\mathrm{Con}_{F'/F}(\mathcal{D}_F)$ iff $\mathrm{e}(P'/P) \bigm| a$, where $P' \in \mathbb{P}_{F'}$ is any divisor lying over P. Thus, $\mathcal{D}_{F'}^G/\mathrm{Con}_{F'/F}(\mathcal{D}_F)$ is the direct product of cyclic groups of order $e_1, \dots, e_m$, i.e.

$$[\mathcal{D}_{F'}^G : \mathrm{Con}_{F'/F}(\mathcal{D}_F)] = e_1 \cdots e_m.$$

Furthermore, we have

$$|\mathbb{J}_{F'}| = [\mathcal{D}^0_{F'} : \mathcal{P}_{F'}] = [\mathcal{D}^0_{F'} : \mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'}] \cdot [\mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'} : \mathcal{P}_{F'}].$$

By the first isomorphism theorem (cf. [**vdW93a**, §50]) we know that we can reduce fractions of groups in the following way

$$(\mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'})/(\mathcal{P}_{F'}) \cong (\mathcal{D}^{0G}_{F'})/(\mathcal{D}^{0G}_{F'} \cap \mathcal{P}_{F'}) \cong (\mathcal{D}^{0G}_{F'})/(\mathcal{P}^{G}_{F'}).$$

This implies

$$\begin{aligned}
&[\mathcal{P}^G_{F'} : \mathrm{Con}_{F'/F}(\mathcal{P}_F)] \cdot |\mathbb{J}_{F'}| \\
=&[\mathcal{P}^G_{F'} : \mathrm{Con}_{F'/F}(\mathcal{P}_F)] \cdot [\mathcal{D}^0_{F'} : \mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'}] \cdot [\mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'} : \mathcal{P}_{F'}] \\
=&[\mathcal{P}^G_{F'} : \mathrm{Con}_{F'/F}(\mathcal{P}_F)] \cdot [\mathcal{D}^0_{F'} : \mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'}] \cdot [\mathcal{D}^{0G}_{F'} : \mathcal{P}^G_{F'}] \\
=&[\mathcal{D}^0_{F'} : \mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'}] \cdot [\mathcal{D}^{0G}_{F'} : \mathcal{P}^G_{F'}] \cdot [\mathcal{P}^G_{F'} : \mathrm{Con}_{F'/F}(\mathcal{P}_F)] \\
=&[\mathcal{D}^0_{F'} : \mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'}] \cdot [\mathcal{D}^{0G}_{F'} : \mathrm{Con}_{F'/F}(\mathcal{D}^0_F)] \\
&\cdot [\mathrm{Con}_{F'/F}(\mathcal{D}^0_F) : \mathrm{Con}_{F'/F}(\mathcal{P}_F)] \\
=&[\mathcal{D}^0_{F'} : \mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'}] \cdot [\mathcal{D}^{0G}_{F'} : \mathrm{Con}_{F'/F}(\mathcal{D}^0_F)] \cdot |\mathbb{J}_F|, \qquad (1)
\end{aligned}$$

since $\mathrm{Con}_{F'/F}$ is injective (cf. proposition I.20). Reducing fractions of subgroups we compute

$$(\mathcal{D}^{0G}_{F'} + \mathrm{Con}_{F'/F}(\mathcal{D}_F))/\mathrm{Con}_{F'/F}(\mathcal{D}_F) \cong \mathcal{D}^{0G}_{F'}/\mathrm{Con}_{F'/F}(\mathcal{D}^0_F).$$

Multiplying (1) with $[\mathcal{D}^G_{F'} : \mathcal{D}^{0G}_{F'} + \mathrm{Con}_{F'/F}(\mathcal{D}_F)]$, we obtain

$$\begin{aligned}
&[\mathcal{D}^G_{F'} : \mathcal{D}^{0G}_{F'} + \mathrm{Con}_{F'/F}(\mathcal{D}_F)] \cdot ([\mathcal{P}^G_{F'} : \mathrm{Con}_{F'/F}(\mathcal{P}_F)] \cdot |\mathbb{J}_{F'}|) \\
=&[\mathcal{D}^G_{F'} : \mathcal{D}^{0G}_{F'} + \mathrm{Con}_{F'/F}(\mathcal{D}_F)] \cdot ([\mathcal{D}^0_{F'} : \mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'}] \cdot [\mathcal{D}^{0G}_{F'} : \mathrm{Con}_{F'/F}(\mathcal{D}^0_F)] \cdot |\mathbb{J}_F|) \\
=&[\mathcal{D}^G_{F'} : \mathcal{D}^{0G}_{F'} + \mathrm{Con}_{F'/F}(\mathcal{D}_F)] \cdot [\mathcal{D}^0_{F'} : \mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'}] \\
&\cdot [\mathcal{D}^{0G}_{F'} + \mathrm{Con}_{F'/F}(\mathcal{D}_F) : \mathrm{Con}_{F'/F}(\mathcal{D}_F)] \cdot |\mathbb{J}_F| \\
=&[\mathcal{D}^0_{F'} : \mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'}] \cdot [\mathcal{D}^G_{F'} : \mathrm{Con}_{F'/F}(\mathcal{D}_F)] \cdot |\mathbb{J}_F| \\
=&[\mathcal{D}^0_{F'} : \mathcal{D}^{0G}_{F'} + \mathcal{P}_{F'}] \cdot e_1 \cdots e_m \cdot |\mathbb{J}_F|
\end{aligned}$$

Hence, $e_1 \cdots e_m \cdot |\mathbb{J}_F|$ divides

$$[\mathcal{D}^G_{F'} : \mathcal{D}^{0G}_{F'} + \mathrm{Con}_{F'/F}(\mathcal{D}_F)] \cdot [\mathcal{P}^G_{F'} : \mathrm{Con}_{F'/F}(\mathcal{P}_F)] \cdot |\mathbb{J}_{F'}|.$$

By lemma II.2 and lemma II.3 the latter divides $n^2 \cdot |\mathbb{J}_{F'}|$ or even just $n|\mathbb{J}_{F'}|$ if $|k^*| > n$, which proves our claim. □

In order to show the usefulness and limits of this theorem, we take a look at some examples.

Example II.3. Let us consider example II.1, again. We have $k = \mathbb{F}_{101}$, $F = k(x, y)$, $E = k(x^2, y)$. We already know $|\mathbb{J}_F| = 7728$, $|\mathbb{J}_E| = 92$. Using [**Sti93**, proposition III.7.3], we see that F is unramified over E. Thus $e_1 \cdots e_m = 1$. Because of $|k^*| = 100 > 2 = [F : E]$, theorem II.4 implies that

$$|\mathbb{J}_E| \text{ divides } 2 \cdot |\mathbb{J}_F|, \text{ i.e. } 92 \text{ divides} 2 \cdot 7728 = 2 \cdot 84 \cdot 92,$$

which is a weaker statement than $|\mathbb{J}_E| \mid |\mathbb{J}_F|$, which we obtain from theorem II.1.

On the other hand, there also are examples for which theorem II.4 is stronger than theorem II.1:

Example II.4. Let $k := \mathbb{F}_{61}$, $F := k(x,y)$, $y^2 = x^3 + 30x + 31$. Setting $t^3 := x + 3$, we obtain the hyperelliptic function field $F' := k(t,y)$, $y^2 = t^9 + 52t^6 + 57t^3 + 36$. Using [**Sti93**, proposition III.7.3], we see that F' has two places which are ramified over F: The pole and zero divisors of $x + 3$. Thus, $e_1 \cdots e_m = 3 \cdot 3 = 9$. Because of $|{\mathbb{F}_{61}}^*| = 60 > 3 = [F' : F]$, we obtain

$$9 \cdot \mathbb{J}_F \mid 3 \cdot \mathbb{J}_{F'}, \text{ i.e. } 3 \cdot \mathbb{J}_F \mid \mathbb{J}_{F'}$$

from theorem II.4, while theorem II.1 only yields $\mathbb{J}_F \mid \mathbb{J}_{F'}$. Using `KASH`, we compute the following class numbers: $|\mathbb{J}_F| = 52$, $|\mathbb{J}_{F'}| = 13855296 = 3 \cdot 52 \cdot 88816$.

Let us proceed with our proof of Madan's theorem (theorem II.1). In many cases, it can be proved using zeta functions as presented by Helmut Hasse. We only have to show why some formulas from [**Has34b**] imply our claim.

Proposition II.5. *Let F/k be a function field over a finite constant field k of characteristic p and F'/k a cyclic extension of prime degree $[F' : F] =: n$ with $k = \tilde{k}$ such that*

(1) *either $n \neq p$ and k contains n-th roots of unity*
(2) *or $n = p$.*

Then $|\mathbb{J}_F|$ divides $|\mathbb{J}_{F'}|$.

Proof. Let $k = \mathbb{F}_q$. The following three equations on zeta functions are due to Helmut Hasse ([**Has34b**, equations (30) and (31), page 51]):

$$\begin{aligned} \zeta_{F'}(s) =& \zeta_F(s) \prod_{\nu=1}^{n-1} L(s,\chi^\nu), \\ L_F(s) =& \frac{\zeta_F(s)}{\zeta_0(s)}, \\ L_{F'}(s) =& \frac{\zeta_{F'}(s)}{\zeta_0(s)}. \end{aligned}$$

Here $\zeta_F(s)$, $\zeta_{F'}(s)$ are the zeta-functions of F and F' resp., $L(s,\chi^\nu)$ is the L-series of the extension F'/F and of the proper character χ^ν of this extension (see also [**Art24**]). $L_F(s)$ and $L_{F'}(s)$ are polynomials in q^{-s} (see also section 3.1), i.e. $L_F(s), L_{F'}(s) \in \mathbb{Z}[q^{-s}]$. We have $L_F(0) = |\mathbb{J}_F|$ and $L_{F'}(0) = |\mathbb{J}_{F'}|$. Furthermore, $\prod_{\nu=1}^{n-1} L(s,\chi^\nu) \in \mathbb{Z}[q^{-s}]$ also is a polynomial in q^{-s}. Hence, $\prod_{\nu=1}^{n-1} L(0,\chi^\nu) \in \mathbb{Z}$. We infer

$$L_{F'}(s) = \frac{\zeta_{F'}(s)}{\zeta_0(s)} = \frac{\zeta_F(s)}{\zeta_0(s)} \cdot \prod_{\nu=1}^{n-1} L(s,\chi^\nu) = L_F(s) \cdot \prod_{\nu=1}^{n-1} L(s,\chi^\nu),$$

which immediately yields

$$|\mathbb{J}_{F'}| = L_{F'}(0) = L_F(0) \cdot \prod_{\nu=1}^{n-1} L(0,\chi^\nu) = |\mathbb{J}_F| \cdot \prod_{\nu=1}^{n-1} L(0,\chi^\nu),$$

where $\prod_{\nu=1}^{n-1} L(0,\chi^\nu) \in \mathbb{Z}$. Thus, $|\mathbb{J}_F| \mid |\mathbb{J}_{F'}|$. □

For the remaining case, where $n \neq p$ and k does not contain n-th roots of unity, it suffices to prove that the conorm on divisor classes of order n^m is injective for any $m \in \mathbb{N}_+$.

PROPOSITION II.6. *Let F/k be a function field over a finite constant field and F'/k a finite Galois extension with $k = \tilde{k}$. Let $d \in \mathbb{N}$ be a prime such that k does not contain d-th roots of unity. Then for each divisor $A \in \mathcal{D}_F^0 \setminus \mathcal{P}_F$ such that $d^m A \in \mathcal{P}_F$ for some $m \in \mathbb{N}_+$, we have $\mathrm{Con}_{F'/F}(A) \notin \mathcal{P}_{F'}$.*

PROOF. Without loss of generality, let m be minimal such that $d^m A \in \mathcal{P}_F$. Then $d^{m-1}A \notin \mathcal{P}_F$. If we show that $\mathrm{Con}_{F'/F}(B) \notin \mathcal{P}_{F'}$ for all $B \in \mathcal{D}_F^0 \setminus \mathcal{P}_F$ such that $dB \in \mathcal{P}_F$, we can infer $\mathrm{Con}_{F'/F}(d^{m-1}A) \notin \mathcal{P}_{F'}$. Thus, $\mathrm{Con}_{F'/F}(A) \notin \mathcal{P}_{F'}$ because $\mathcal{P}_{F'}$ is a subgroup of $\mathcal{D}_{F'}$. Hence we may assume $m = 1$.

Suppose $B \in \mathcal{D}_F^0 \setminus \mathcal{P}_F$, $dB \in \mathcal{P}_F$ and $\mathrm{Con}_{F'/F}(B) = (x)^{F'}$ for some $x \in F' \setminus F$. We denote $dB =: (y)^F$ with $y \in F$ and obtain

$$(y)^{F'} = \mathrm{Con}_{F'/F}((y)^F) = \mathrm{Con}_{F'/F}(dB) = d\mathrm{Con}_{F'/F}(B) = d(x)^{F'}.$$

Therefore, there exists some $a \in k$ such that $y = ax^d$. Since F'/F is Galois, there are $x_1, \ldots, x_d \in F'$ such that $x = x_1$ and $y = ax_i^d$. Thus, there exists a primitive d-th root $\zeta \in F'$ of unity such that $x_i = \zeta^i x$, if the x_i are ordered appropriately. Obviously, $\zeta \in \tilde{k} = k$, which contradicts our assumption $\zeta \notin k$. □

Using the above propositions, we are able to prove Madan's theorem:

PROOF OF THEOREM II.1. We have to prove that $|\mathbb{J}_F|$ divides $|\mathbb{J}_{F'}|$ whenever F'/k' is a finite Galois extension of a function field F/k with finite constant field and $k = \tilde{k}$, $k' = \tilde{k}'$.

By proposition I.16, we can split up our extension into $F' \supseteq Fk' \supseteq F$, where Fk'/F is a constant field extension. By proposition I.24, the conorm map $\mathrm{Con}_{Fk'/F}$ on divisor classes is injective. Since it maps divisor classes of degree 0 to divisor classes of degree 0, we obtain $|\mathbb{J}_F| \mid |\mathbb{J}_{Fk'}|$. It remains to show that $|\mathbb{J}_{Fk'}|$ divides $|\mathbb{J}_{F'}|$. To simplify the notation, we assume $k = k'$, i.e. we consider a finite Galois extension F'/k over F/k, where $k = \tilde{k}$.

Let $p := \mathrm{char}(k)$ and $n := [F' : F]$. Since F'/F is Galois, we can split up this extension into cyclic extensions of prime degree. Thus, if we can prove $|\mathbb{J}_F| \mid |\mathbb{J}_{F'}|$ for cyclic extensions of prime degree, our theorem is shown. Thus, we will assume F'/F to be cyclic and n to be prime.

We consider several cases, separately:

(1) If $p = n$ or k contains n-th roots of unity, we deduce $|\mathbb{J}_F| \mid |\mathbb{J}_{F'}|$ from proposition II.5.

(2) Let us consider the case where $p \neq n$ and k does not contain n-th roots of unity.

Let $d \in \mathbb{N}$ be a prime and $l \in \mathbb{N}_+$ such that $d^l \parallel |\mathbb{J}_F|$. We will show that $d^l \mid |\mathbb{J}_{F'}|$.

(a) If $d \neq n$, we apply theorem II.4 and obtain

$$d^l \mid |\mathbb{J}_F| \mid e_1 \cdots e_m \cdot |\mathbb{J}_F| \mid n^2 |\mathbb{J}_{F'}|,$$

where the e_i are the ramification indices of all ramified places. Hence $d^l \mid |\mathbb{J}_{F'}|$, since $(d, n) = 1$.

(b) Now, only the case $d = n \neq p$, where k does not contain n-th roots of unity, remains to be investigated. Let $U \leq \mathbb{J}_F$ such that $|U| = d^l$. We will show that $\mathrm{Con}_{F'/F} : U \to \mathbb{J}_{F'}$ is injective.

Let $0 \neq A \in U$ be any nonzero element. Then, $d^l A = 0$ is obvious. Since $d = n$, our constant field k does not contain d-th roots of unity. Thus, proposition II.6 implies $\mathrm{Con}_{F'/F}(A) \neq 0$, i.e. $\mathrm{Con}_{F'/F} : U \to \mathbb{J}_{F'}$ is injective. This implies $d^l \mid |\mathbb{J}_{F'}|$.

Thus, we have $|\mathbb{J}_F| \mid |\mathbb{J}_{F'}|$ if $p \neq n$ and k does not contain n-th roots of unity.

$\square$

CHAPTER III

Defining Equations

In this chapter, we are interested in conditions which determine whether two given hyperelliptic function fields—which are defined over the same constant field—are isomorphic. We will prove in section 4 that all we need to decide isomorphy are the defining equations of the corresponding fields: Two function fields are isomorphic iff they have the same defining equation.

Since defining equations of function fields are not uniquely determined, we need criteria to decide whether a given function field has a given defining equation. In section 1, we will present a very simple necessary condition: If a hyperelliptic function field has two defining equations $y^2 = D_x$, $u^2 = D_t$, the degrees of the irreducible factors of D_x and D_t are essentially equal. Sections 2 and 3 culminate in a condition which is both necessary and sufficient: Theorem III.16.

In section 2 we prove a proposition by Lockhart (proposition III.4, theorem III.6), which provides somewhat unique normal forms for the defining equations of hyperelliptic function fields. Although this uniqueness needs additional conditions which are not met if we wish to compute isomorphisms (cf. remark III.7), the theorem points in the correct direction. In fact, it was the starting point for the development of theorem III.16, a generalization of theorem III.6, which enables us to check, whether a given field has a given defining equation (cf. section 3).

1. A Simple Criterion

In this section, we will see that the irreducible factors of D_t and D_x are essentially the same whenever $k(t,u) = k(x,y)$, $u^2 = D_t$, $y^2 = D_x$. Hence, we obtain a necessary condition for a hyperelliptic function field to have a given defining equation, which can be checked very efficiently.

In order to prove this criterion, we need the following proposition stating that each hyperelliptic function field contains exactly one rational function field of degree 2.

PROPOSITION III.1. *Let $k(t,u) = k(x,y)$ be a hyperelliptic function field, $u^2 = D_t$, $y^2 = D_x$, where $D_t \in k[t]$ and $D_x \in k[x]$ are separable monic polynomials. Then $k(t) = k(x)$.*

PROOF. [**Sti93**, proposition VI.2.4]. □

REMARK III.2. This fact does not hold for elliptic function fields:[1] Let F be an elliptic function field which has at least two distinct places P, Q of degree 1. By proposition I.47, 2 is no gap number of P, i.e. 2 is a pole number. Thus, there exists an $x \in F$ such that $(x)_\infty = 2P$. From proposition I.4 we know $2 = \deg((x)_\infty) = [F : k(x)]$. Let us show that $k(x)$ indeed is rational: Because we assumed $\mathrm{char}(k) \neq 2$, the different $\mathrm{Diff}(F/k(x))$ is defined to be the sum of all ramified places of $F/k(x)$.

[1] The author thanks Henning Stichtenoth for pointing out this fact.

We deduce $\deg(\mathrm{Diff}(F/k(x))) = 4$ from proposition I.39. In our case, the Hurwitz genus formula (theorem I.22) becomes

$$0 = 2\mathrm{g}_F - 2 = [F : k(x)] \cdot (2\mathrm{g}_{k(x)} - 2) + \deg(\mathrm{Diff}(F/k(x))) = 2 \cdot (2\mathrm{g}_{k(x)} - 2) + 4.$$

Hence we have $\mathrm{g}_{k(x)} = 0$, i.e. $k(x)$ is rational. Analogously, Q yields a different rational subfield of degree 2.

If k is algebraically closed, there even is an infinite number of regular places of degree 1, i.e. we have an infinite number of rational subfields of degree 2.

Since a hyperelliptic function field has a uniquely determined rational subfield of degree 2, it is easy to see that a place is ramified over $k(t)$ iff it is ramified over $k(x)$. From this, we conclude that given two defining equations $u^2 = D_t(t)$, $y^2 = D_x(x)$ of a function field $F = k(t, u) = k(x, y)$ the degrees of the prime divisors of D_t and D_x are essentially equal:

THEOREM III.3. *Let $F = k(t, u) = k(x, y)$ be a hyperelliptic function field with $u^2 = D_t(t)$ and $y^2 = D_x(x)$, where $D_t \in k[t]$ and $D_x \in k[x]$ both are separable polynomials. Furthermore, let $D_t = p_1 \cdots p_m$ and $D_x = q_1 \cdots q_n$ be prime factor decompositions over k.*

(1) *If $\deg_t(D_t) = \deg_x(D_x)$, then $m = n$ and for a suitable numbering we have $\deg_t(p_i) = \deg_x(q_i)$ for all $i = 1, \ldots, m$.*
(2) *If $\deg_t(D_t) = \deg_x(D_x) + 1$, then $m = n + 1$ and for a suitable numbering we have $\deg_t(p_i) = \deg_x(q_i)$ for all $i = 1, \ldots, m$. and $\deg_x(q_n) = 1$.*
In the case $\deg_x(D_x) = \deg_t(D_t) + 1$ the analogous statement is true.
(3) *There are no further cases.*

PROOF. By proposition I.33, we have $\deg_t(D_t), \deg_x(D_x) \in \{2\mathrm{g}+1, 2\mathrm{g}+2\}$. Therefore, we only have the cases stated above.

We denote the place of F lying above p_i by P_i; the place above q_j is called Q_j (for all i, j). By proposition I.39, the P_i and Q_j are ramified over p_i and q_j respectively. Thus P_i indeed is uniquely determined by p_i as well as Q_j is the unique place lying over q_j.

(1) Let us consider the case $\deg_t(D_t) = \deg_x(D_x) \equiv 0 \mod 2$ first. By proposition I.39, $P_1, \ldots, P_m$ are exactly the places of F which are ramified over $k(t)$, while $Q_1, \ldots, Q_n$ are the ramified places over $k(x)$. By proposition III.1, we have $k(t) = k(x)$. Hence, we get $\{P_1, \ldots, P_m\} = \{Q_1, \ldots, Q_n\}$, from which we conjecture $m = n$. Furthermore, we have $P_i = Q_i$ for all $i = 1, \ldots, m$ if the numbering is chosen appropriately. Thus, the places p_i and q_i are equal. Hence, we have $\deg_t(p_i) = \deg(p_i) = \deg(q_i) = \deg_x(q_i)$ for all i.
(2) We consider the case $\deg_t(D_t) = \deg_x(D_x) \equiv 1 \mod 2$, next. Analogously to the above, we deduce $\{P_1, \ldots, P_m, \infty_t\} = \{Q_1, \ldots, Q_n, \infty_x\}$, where ∞_t is the place above $(t)_\infty^{k(t)}$ and ∞_x is above $(x)_\infty^{k(x)}$. Again, we infer $m = n$ and for suitable numbering $P_i = Q_i$ for $i = 1, \ldots, m - 1$. If $P_m = Q_m$, the claim is proved like in the above case. Otherwise, we have $P_m = \infty_x$, $Q_m = \infty_t$, i.e. $\deg_t(p_m) = \deg(P_m) = \deg(\infty_x) = 1$ and $\deg_x(q_m) = \deg(Q_m) = \deg(\infty_t) = 1$. Therefore, we have $\deg_t(p_m) = \deg_x(q_m) = 1$, which proves our claim.
(3) If $\deg_t(D_t) = \deg_x(D_x) + 1$ we infer $\deg_t(D_t) \equiv 0 \mod 2$. Like above, we get

$$\{P_1, \ldots, P_m\} = \{Q_1, \ldots, Q_n, \infty_x\},$$

i.e. $m = n + 1$ and for a suitable numbering $P_i = Q_i$ for $i = 1, \ldots, m$ as well as $Q_n = \infty_t$. This proves our claim.

□

Let us give an example which shows the usefulness of theorem III.3.

Example III.1. Let $F = \mathbb{F}_{41}(t, u)$, $u^2 = D_t := t^6 + 35t^5 + 34t^4 + 9t^3 + 6t + 8$ and $D_x := 6x + 25x^2 + 5x^4 + 26x^5 + x^6 + 13$. If we had $F = \mathbb{F}_{41}(x, y)$, $y^2 = D_x$, the irreducible factors of D_t and D_x needed to have the same degrees. Factoring over $\mathbb{F}_{41}$, we obtain

$$\begin{aligned} D_t =&(t + 7)(t^5 + 28t^4 + 2t^3 + 36t^2 + 35t + 7) \\ D_x =&(x + 18)(x + 38)(x^2 + 28x + 35)(x^2 + 24x + 7) \end{aligned}$$

Thus, $F \neq \mathbb{F}_{41}(x, y)$.

2. A Theorem by Lockhart

Paul Lockhart proved the existence and a certain kind of uniqueness of normal forms for defining equations of hyperelliptic function fields (cf. [**Loc94**, proposition 1.2]). Let us state the existence part, first:

Proposition III.4 (Lockhart). *Let F be a hyperelliptic function field of genus* g *over k,* $\mathrm{char}(k) \neq 2$, *and P a Weierstraß point of degree* 1 *of F. Then there exist $x, y \in F$ such that $F = k(x, y)$ with $x \in \mathcal{L}(2P)$, $y \in \mathcal{L}((2\mathrm{g} + 1)P)$, $y^2 = D(x)$, D monic and* $\deg(D) = 2\mathrm{g} + 1$.

Proof. Cf. [**Loc94**, proposition 1.2, remark]. □

As the uniqueness part of the before mentioned proposition (theorem III.6) is a special case of theorem III.16, which motivated the development of the latter, we will prove it. In order to do so, we need the following lemma:

Lemma III.5. *Let $k(t, u)$ be a (hyper-)elliptic function field, $u^2 = D(t)$, where D is a separable monic polynomial over k. Let t have a double pole at P (i.e. $(t)_\infty = 2P$). Then* $\dim(2P) = 2$ *and $\{1, t\}$ is a basis of $\mathcal{L}(2P)$ over k.*

Proof. Since $1, t \in \mathcal{L}(2P)$ and as $1, t$ are linearly independent over k, we have $\dim(2P) \geq 2$. Furthermore, $\mathcal{L}(2P) \subseteq \mathcal{L}(2\mathrm{g}P)$, and the Riemann-Roch theorem yields $\dim(2\mathrm{g}P) = \deg(2\mathrm{g}P) + 1 - \mathrm{g} = \mathrm{g} + 1$ (cf. proposition I.13). In the elliptic case, this proves our claim.

Let us suppose $\dim(2P) > 2$ and $\mathrm{g} > 1$. It is easy to see that $1, t, t^2, \ldots, t^{\mathrm{g}} \in \mathcal{L}(2\mathrm{g}P)$ form a basis. Thus we need to have $t^i \in \mathcal{L}(2P)$ for some $i \in \{2, \ldots, \mathrm{g}\} \neq \emptyset$. Evaluating t^i at P leads to $\mathrm{v}_P(t^i) = i\mathrm{v}_P(t) = 2i > 2$, i.e. $t^i \notin \mathcal{L}(2P)$. Contradiction.

As $1, t \in \mathcal{L}(2P)$ are linearly independent and $\dim(2P) = 2$, these elements form a basis of $\mathcal{L}(2P)$. □

Now we prove the uniqueness part of Lockhart's proposition. It essentially states that the defining equation of a hyperelliptic function field is unique up to basis transformations $x = \alpha^2 t + \beta$, $y = \alpha^{2\mathrm{g}+1}u$, provided x and t share the same pole divisor.

Theorem III.6 (Lockhart). *Let $F = k(t, u) = k(x, y)$ be a hyperelliptic function field*[2] *of genus* g *and $u^2 = D_t$, $y^2 = D_x$ be imaginary quadratic defining equations of F. Furthermore let $P \in \mathbb{P}_F$ be a Weierstraß point of degree* 1 *such that $t, x \in \mathcal{L}(2P)$, $u, y \in \mathcal{L}((2\mathrm{g} + 1)P)$. Then there are $\alpha, \beta \in k$, $\alpha \neq 0$, such that $x = \alpha^2 t + \beta$, $y = \alpha^{2\mathrm{g}+1}u$.*

[2] Recall that our definition implies $\mathrm{g} \geq 2$ and $\mathrm{char}(k) \neq 2$.

Proof. As $\deg_t(D_t) = 2\mathrm{g}+1$, the pole divisor of t is ramified over $k(t)$, as is proved in proposition I.39. Thus, $(t)_\infty = 2P$. By lemma III.5, we obtain $\dim(2P) = 2$, i.e. there are $\beta, \gamma \in k$, $\gamma \neq 0$ such that $x = \gamma t + \beta$.

As $\mathrm{v}_P(u^2) = \mathrm{v}_P(D_t) = -2\deg_t(D_t) = -2(2\mathrm{g}+1)$, we have $\mathrm{v}_P(u) = -(2\mathrm{g}+1)$. In a similar way, we see that $\mathrm{v}_Q(u) \geq 0$ for each $Q \neq P$, i.e. $u \in \mathcal{L}((2\mathrm{g}+1)P) \setminus \mathcal{L}(2\mathrm{g}P)$. Similarly, $y \in \mathcal{L}((2\mathrm{g}+1)P) \setminus \mathcal{L}(2\mathrm{g}P)$. As $\deg(2\mathrm{g}P) = 2\mathrm{g} \geq 2\mathrm{g}-1$, proposition I.13 implies $\dim(2\mathrm{g}P) = 2\mathrm{g}+1-\mathrm{g} = \mathrm{g}+1$ and $\dim((2\mathrm{g}+1)P) = \mathrm{g}+2$. Therefore, $y = \delta u + \eta$, where $\delta \in k^*$ and $\eta \in \mathcal{L}(2\mathrm{g}P)$. Because $\eta \in F = k(t,u)$, there are $f, h \in k(t)$ such that $\eta = f + hu$. Hence, $y = \delta u + \eta = (\delta + h)u + f$. This implies

$$D_x = y^2 = (\delta+h)^2u^2 + 2(\delta+h)fu + f^2 = (\delta+h)^2D_t + 2(\delta+h)fu + f^2.$$

Because $k(x) = k(t)$, this equation yields

$$2(\delta+h)fu = D_x - (\delta+h)^2D_t - f^2 \in k(t).$$

Since $u \notin k(t)$, we need to have $2(\delta+h)f = 0$. Thus $(\delta+h) = 0$ or $f = 0$, because $\mathrm{char}(k) \neq 2$. Suppose $f \neq 0$. Then $(\delta+h) = 0$ and the above equation becomes $D_x = f^2$, which contradicts the separability of D_x. Thus, $f = 0$. We obtain $D_x = (\delta+h)^2D_t$. As $2\deg_x(D_x) = \mathrm{v}_P(D_x) = 2\deg_t(D_x)$, we have $\deg_t(D_x) = 2\mathrm{g}+1 = \deg_t(D_t)$. Thus $\deg_t(h) = 0$, i.e. $h \in k$. Since $hu = \eta \in \mathcal{L}(2\mathrm{g}P)$ and $u \notin \mathcal{L}(2\mathrm{g}P)$, we infer $h = 0$, i.e. $\eta = 0$. Therefore, we have

$$D_x = \delta^2 D_t$$

with $\delta \in k^*$. Computing leading coefficients yields $\mathrm{lc}_t(D_x) = \mathrm{lc}_t(\delta^2D_t)$. Because $x = \gamma t + \beta$ and D_x, D_t both are monic, we obtain

$$\gamma^{2\mathrm{g}+1} = \mathrm{lc}_t(D_x) = \mathrm{lc}_t(\delta^2D_t) = \delta^2.$$

Let $\alpha := \delta\gamma^{-\mathrm{g}}$. Then $\alpha^2 = \delta^2\gamma^{-2\mathrm{g}} = \gamma$ and $\alpha^{2\mathrm{g}+1} = \alpha^{2\mathrm{g}} \cdot \alpha = \gamma^{\mathrm{g}}\alpha = \gamma^{\mathrm{g}}\delta\gamma^{-\mathrm{g}} = \delta$, i.e. $x = \alpha^2t + \beta$, $y = \alpha^{2\mathrm{g}+1}u$. □

Remark III.7. Unfortunately, given a hyperelliptic function field $F = k(t,u)$, $u^2 = D_t$ and a defining equation $y^2 = D_x$ of a hyperelliptic function field over k, we cannot assume that $F = k(x,y)$ implies the condition $t, x \in \mathcal{L}(2P)$, $u, y \in \mathcal{L}((2\mathrm{g}+1)P)$ for any P, as we will see in the following example III.2. Thus we cannot check, whether $F = k(x,y)$ using theorem III.6.

Example III.2. Let $k := \mathbb{F}_{13}$, $F := k(t,u)$, $u^2 = t^5 + t + 1$. If $(t)_\infty =: 2P$, we have $t \in \mathcal{L}(2P)$ and $u \in \mathcal{L}((2\mathrm{g}+1)P) = \mathcal{L}(5P)$. Setting $x := \frac{t}{4t+1}$, $y := 8u(4x-1)^3$, i.e. $t = -\frac{x}{4x-1}$, $u = \frac{y}{8(4x-1)^3}$, we easily see $F = k(x,y)$. Since $\mathrm{v}_P(x) = 2(\deg_t(4t+1) - \deg_t(t)) = 0$ and $x \notin k$, there is a place $Q \neq P$ such that $\mathrm{v}_Q(x) < 0$. Thus $x \notin \mathcal{L}(2P)$. This shows that the condition $x, t \in \mathcal{L}(2P)$ does not necessarily hold for each pair of bases of a hyperelliptic function field.

The necessity of the condition $x \in \mathcal{L}(2P)$, $y \in \mathcal{L}((2\mathrm{g}+1)P)$ in theorem III.6 can also be demonstrated using this example: Computing y^2 yields the equation

$$y^2 = -(4x-1)^6u^2 = x^5 - 2x^4 + 2x^3 + x^2 - 3x - 1.$$

If the assumption on x, y to lie in the mentioned Riemann-Roch spaces was optional, we needed to have $x = \alpha^2t + \beta$, $y = \alpha^{2\mathrm{g}+1}u$ with $\alpha, \beta \in k$, which does not hold.

3. Basis Transformations

In this section we show the connection between different bases of a hyperelliptic function field (cf. theorem III.16): If $k(t,u) = k(x,y)$, is a hyperelliptic function field, then x needs to be a fraction of linear polynomials in t and the relation between u and y can be computed easily for each choice of t and x.

As we will see in section 2 of chapter IV this theorem can be used to check two given hyperelliptic function fields for isomorphy (cf. also section 4 of this chapter). This algorithm is one of the core components of our method for computing the automorphism group of a hyperelliptic function field (cf. chapter V).

3.1. Relations Between the Variable Symbols. In this section, we show that x can be represented as a fraction of linear polynomials in t. In order to do so, the first step is to recall proposition III.1, which states that for hyperelliptic function fields $k(t,u) = k(x,y)$, $u^2 = D_t$, $y^2 = D_x$ implies $k(t) = k(x)$. This reduces the question of the relation between t and x to rational function fields. The following proposition states that in rational function fields, any variable symbol is a fraction of linear polynomials in any other variable symbol.

Proposition III.8. *Let $k(t)$ be a rational function field and $x \in k(t)$ such that $k(t) = k(x)$. Then there are $\alpha_0, \ldots, \alpha_3 \in k$ with $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}$ and $\alpha_0\alpha_3 - \alpha_1\alpha_2 \neq 0$.*

Proof. As $x \in k(t)$, there are polynomials $\varphi, \psi \in k[t]$, such that $x = \frac{\varphi}{\psi}$ and $(\varphi, \psi) \in k$. We consider the principal divisor of x. Proposition I.4 implies

$$\deg((x)_0) = \deg((x)_\infty) = [k(t) : k(x)] = 1.$$

Let us consider the case $\infty_t \notin \operatorname{supp}(x)$ first. Then $\mathrm{v}_{\infty_t}(x) = 0$, i.e. $\deg_t(\varphi) = \deg_t(\psi)$. As $\varphi, \psi \in k[t]$, we get $(\varphi)_\infty = \deg_t(\varphi)\infty_t = \deg_t(\psi)\infty_t = (\psi)_\infty$. We have $(x) = (\varphi) - (\psi) = (\varphi)_0 - (\varphi)_\infty - ((\psi)_0 - (\psi)_\infty) = (\varphi)_0 - (\psi)_0$, i.e. $(x)_0 = (\varphi)_0$ and $(x)_\infty = (\psi)_0$. Thus,

$$\begin{aligned}\deg_t(\varphi) &= \deg((\varphi)_\infty) = \deg((\varphi)_0) = \deg((x)_0) \\ &= 1 = \deg((x)_\infty) = \deg((\psi)_0) = \deg((\psi)_\infty) = \deg_t(\psi).\end{aligned}$$

Thus there are $\alpha_i \in k$ such that $\varphi = \alpha_0 t + \alpha_1$, $\psi = \alpha_2 t + \alpha_3$ and $\alpha_0\alpha_3 - \alpha_1\alpha_2 \neq 0$ as claimed.

If $\infty_t \in \operatorname{supp}(x)$, we obviously have $\deg_t(\varphi) \neq \deg_t(\psi)$. Without loss of generality we assume $\mathrm{v}_{\infty_t}(x) < 0$ (consider $\frac{1}{x}$ in the other case). As $\deg((x)_\infty) = 1$, we need to have $\mathrm{v}_{\infty_t}(x) = -1$. Thus

$$-1 = \mathrm{v}_{\infty_t}(x) = \mathrm{v}_{\infty_t}(\frac{\varphi}{\psi}) = \deg_t(\psi) - \deg_t(\varphi),$$

i.e. $\deg_t(\psi) = \deg_t(\varphi) - 1$. As $(\varphi)_\infty = \deg_t(\varphi)\infty_t$ and $(\psi)_\infty = \deg_t(\psi)\infty_t$, we infer

$$(x) = (\varphi) - (\psi) = (\varphi)_0 - (\varphi)_\infty - (\psi)_0 + (\psi)_\infty = (\varphi)_0 - (\psi)_0 - \infty_t.$$

Thus, we have $(x)_0 = (\varphi)_0$, i.e.

$$\deg_t(\varphi) = \deg((\varphi)_\infty) = \deg((\varphi)_0) = \deg((x)_0) = 1.$$

We obtain $x = \frac{\varphi}{\psi} = \frac{\alpha_0 t + \alpha_1}{\alpha_3}$ with $\alpha_i \in k$, $\alpha_0\alpha_3 \neq 0$ as claimed. □

Combining propositions III.1 and III.8, we obtain the afore mentioned fact: In a hyperelliptic function field with two bases t, u and x, y, the variable symbol x is a fraction of linear polynomials in t.

Corollary III.9. *Let $k(t,u) = k(x,y)$ be a hyperelliptic function field, and $u^2 = D_t$, $y^2 = D_x$ the corresponding defining equations. Then there are $\alpha_0, \ldots, \alpha_3 \in k$ with $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}$ and $\alpha_0\alpha_3 - \alpha_1\alpha_2 \neq 0$.*

Proof. By proposition III.1, we have $k(t) = k(x)$. Thus proposition III.8 implies the existence of the α_i. □

Remark III.10. For algebraically closed k the assertion of corollary III.9 can in all probability also be derived from [**Gey74**, Satz 1], which states the following: The isomorphism classes of curves of genus g over k are in one-to-one correspondence to the $\mathrm{PGL}_2(k)$-orbits on

$$\{S \subseteq \mathbb{P}_1(k) \,:\, |S| = 2\mathrm{g}+2\}.$$

The fact that two (hyperelliptic) function fields are isomorphic iff they possess the same defining equation is proved in section 4.

3.2. Relation Between the Square Roots. Since we know now, how t and x are related in a hyperelliptic function field for which we have two bases $k(t,u) = k(x,y)$, we proceed studying the relationship between u and y. We will see that y is a multiple of u over $k(t)$ in proposition III.11. Later, we will see that the factor φ we need to multiply u with to obtain y is the inverse of a polynomial in t (lemma III.13). Furthermore, we will find out that φ is (up to a constant factor) the denominator of x when interpreted as a function in t (lemma III.14) and we will determine its degree in proposition III.15.

Proposition III.11. *Let $k(t,u) = k(x,y)$ be a hyperelliptic function field and let $u^2 = D_t$, $y^2 = D_x$ be the corresponding defining equations. Then there exists a $\varphi \in k(t)^*$, such that $y = \varphi u$.*

Proof. As $y \in k(t,u)$ and $[k(t,u) : k(t)] = 2$, there are $\varphi, \psi \in k(t)$ such that $y = \varphi u + \psi$. Let us suppose $\varphi = 0$. Then we had $y \in k(t)$. From proposition III.1 we know that $k(x) = k(t)$. Thus we had $y \in k(x)$, i.e. $k(x,y) = k(x)$, contradicting $[k(x,y) : k(x)] = 2$. Therefore $\varphi \neq 0$.

Substituting our representation of y into its minimal polynomial we get

$$D_x = y^2 = (\varphi u + \psi)^2 = \varphi^2 u^2 + 2\varphi\psi u + \psi^2 = \varphi^2 D_t + 2\varphi\psi u + \psi^2,$$

thus $2\varphi\psi u \in k(t) = k(x)$. As $u \notin k(t)$, this leads to $2\varphi\psi = 0$, from with we conclude $\psi = 0$ because $\mathrm{char}(k) \neq 2$ and $\varphi \neq 0$. □

Knowing that $y = \varphi u$, we will examine φ more closely. We start with the following lemma, which is quite technical, but will be useful in the subsequent proofs: It will lead to explicit formulas for the relation between u and y, if the relation between t and x is known.

Lemma III.12. *Let $F = k(t,u) = k(x,y)$ be a hyperelliptic function field and $u^2 = D_t$, $y^2 = D_x$ be the corresponding defining equations. Let $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}$, $\alpha_i \in k$, $\alpha_0\alpha_3 - \alpha_1\alpha_2 \neq 0$ as stated in corollary III.9 and $y = \varphi u$, $\varphi \in k(t)^*$ as in proposition III.11. Let $\eta_1, \dots, \eta_{d_x} \in \overline{k}$, $d_x := \deg_x(D_x)$ be the zeroes of D_x. Furthermore, let $p_i := (\alpha_0 - \alpha_2\eta_i)t + \alpha_1 - \alpha_3\eta_i$ for each i. Then the p_i are pairwise relatively prime and we have*

$$D_t = \varphi^{-2}(\alpha_2 t + \alpha_3)^{-d_x} \prod_{i=1}^{d_x} p_i.$$

Furthermore we have

1. $d_x - 1 \leq \deg_t\left(\prod_{i=1}^{d_x} p_i\right) \leq d_x$.
2. *Let $q \in \overline{k}[t]$ be linear. Then $q^2 \nmid \prod_{i=1}^{d_x} p_i$. In particular, $(\alpha_2 t + \alpha_3)^2 \nmid \prod_{i=1}^{d_x} p_i$.*

Proof. Because D_x is square-free, we have $\eta_i \neq \eta_j$ for all $i \neq j$. The definition of the p_i implies $x - \eta_i = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3} - \eta_i = \frac{\alpha_0 t + \alpha_1 - (\alpha_2 t + \alpha_3)\eta_i}{\alpha_2 t + \alpha_3} = \frac{p_i}{\alpha_2 t + \alpha_3}$. Suppose there were indices $i \neq j$ such that $(p_i, p_j) \notin \overline{k}$. Then we had $p_i = \beta p_j$ for some $\beta \in \overline{k}^*$, i.e. $(x-\eta_i)=\frac{p_i}{\alpha_2 t+\alpha_3}=\beta\frac{p_j}{\alpha_2 t+\alpha_3}=\beta(x-\eta_j)$. Thus, D_x were not square-free. Contradiction. Therefore, the p_i are pairwise relatively prime. We compute

$$\begin{aligned} D_t =& u^2=\varphi^{-2}y^2=\varphi^{-2}D_x=\varphi^{-2}\prod_{i=1}^{d_x}(x-\eta_i)=\varphi^{-2}\prod_{i=1}^{d_x}\frac{p_i}{\alpha_2 t+\alpha_3}\\ =&\varphi^{-2}(\alpha_2 t+\alpha_3)^{-d_x}\prod_{i=1}^{d_x}p_i. \end{aligned}$$

This proves our main claim. Let us proceed by examining the supplementary statements. Obviously,

$$\deg_t\left(\prod_{i=1}^{d_x}p_i\right)\le d_x.$$

If $\deg_t\left(\prod_{i=1}^{d_x}p_i\right)<d_x-1$, there were two indices $i\neq j$ such that $p_i,p_j\in\overline{k}$, thus $\alpha_0-\alpha_2\eta_i=\alpha_0-\alpha_2\eta_j=0$, i.e. $\alpha_0=\alpha_2\eta_i=\alpha_2\eta_j$ or $\alpha_2(\eta_i-\eta_j)=0$ which yields $\alpha_2=0$ since $\eta_i\neq\eta_j$. Now we can easily deduce $\alpha_0=0$ from $\alpha_0-\alpha_2\eta_i=0$. Since $\alpha_0\alpha_3-\alpha_1\alpha_2\neq 0$, this is not possible. Thus $\deg_t\left(\prod_{i=1}^{d_x}p_i\right)\ge d_x-1$.

Finally, we suppose $q^\nu \mid \prod_{i=1}^{d_x}p_i$ for some linear $q\in k[t]$ and $\nu\in\mathbb{N}_+$. As $\deg_t(p_i)\le 1$, there are ν factors $p_{i_1},\ldots,p_{i_\nu}$, which are multiples of q. Thus $p_{i_1},\ldots,p_{i_\nu}$ are scalar multiples of each other. If $\nu>1$, this contradicts the relative primality of the p_i. This proves the last claim. □

The following lemma states, that φ^{-1} is a non-zero polynomial in t.

Lemma III.13. *Let $F=k(t,u)=k(x,y)$ be a hyperelliptic function field and $u^2=D_t$, $y^2=D_x$ be the corresponding defining equations. Let $x=\frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$ as stated in corollary III.9 and $y=\varphi u$ as in proposition III.11. Then we have $\varphi^{-1}\in k[t]\setminus\{0\}$.*

Proof. $\varphi\neq 0$ was proved in proposition III.11. Hence, it remains to show $\varphi^{-1}\in k[t]$. Lemma III.12 implies $D_t=\varphi^{-2}(\alpha_2 t+\alpha_3)^{-d_x}\prod_{i=1}^{d_x}p_i$. Suppose $\varphi^{-1}=\frac{\varphi_1}{\varphi_0}\notin k[t]$. As $D_t\in k[t]$, φ_0^2 needs to be canceled by $\prod_{i=1}^{d_x}p_i$. Let $q\in\overline{k}[t]$ be a linear factor of φ_0. Thus $q^2 \mid \prod_{i=1}^{d_x}p_i$, which contradicts lemma III.12. Therefore, we need to have $\varphi^{-1}\in k[t]$. □

We will prove next, that φ^{-1} is a power of the denominator of x, multiplied by some constant from k.

Lemma III.14. *Let $F=k(t,u)=k(x,y)$ be a hyperelliptic function field and $u^2=D_t$, $y^2=D_x$ be the corresponding defining equations. Let $x=\frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$ as stated in corollary III.9 and $y=\varphi u$ as in proposition III.11. Then there are $\gamma\in k^*$ and $m\in\mathbb{N}$ such that*

$$\varphi^{-1}=\gamma(\alpha_2 t+\alpha_3)^m.$$

Proof. By lemma III.13 we know $\varphi^{-1}\in k[t]\setminus\{0\}$. Factoring it over k yields $\varphi^{-1}=\gamma\cdot(\alpha_2 t+\alpha_3)^m$, where $\gamma\in k[t]\setminus\{0\}$ such that $(\alpha_2 t+\alpha_3)\nmid\gamma$ (γ does not need to be irreducible). By lemma III.12 we have

$$D_t=\varphi^{-2}(\alpha_2 t+\alpha_3)^{-d_x}\prod_{i=1}^{d_x}p_i=\gamma^2(\alpha_2 t+\alpha_3)^{m-d_x}\prod_{i=1}^{d_x}p_i.$$

As D_t is separable, we need to have $\gamma\in k^*$ which proves our claim. □

Computing the degree of φ^{-1}, we see that it is a scalar multiple of the (g + 1)-th power of the denominator of x.

Proposition III.15. *Let $F = k(t,u) = k(x,y)$ be a hyperelliptic function field and $u^2 = D_t$, $y^2 = D_x$ be the corresponding defining equations. Let $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$ as stated in corollary III.9 and $y = \varphi u$ as in proposition III.11. Then we have*

1. *If $x \in k[t]$, then $\varphi \in k^*$.*
2. *If $x \in k(t)\backslash k[t]$, then there exists some $\gamma \in k^*$ such that $\varphi^{-1} = \gamma(\alpha_2 t+\alpha_3)^{\mathrm{g}+1}$.*

Proof. By lemma III.12, there are $p_i \in \overline{k}[t]$, such that

$$D_t = \varphi^{-2}(\alpha_2 t+\alpha_3)^{-d_x}\prod_{i=1}^{d_x} p_i, \quad d_x - 1 \le \deg_t\left(\prod_{i=1}^{d_x} p_i\right) \le d_x.$$

Let us consider the given cases, separately.

1. Let us assume $x \in k[t]$, i.e. $x = \frac{\alpha_0 t+\alpha_1}{\alpha_3}$, first. We already know $\varphi^{-1} \in k[t]\backslash\{0\}$ (lemma III.13) and $D_t = \varphi^{-2}\alpha_3^{-d_x}\prod_{i=1}^{d_x} p_i$. If $\varphi^{-1} \notin k$, then φ^{-2} were a non trivial square polynomial in t dividing D_t. This contradicts the separability of D_t. Thus $\varphi^{-1} \in k$, which immediately implies $\varphi \in k^*$.
2. We assume the case $x \notin k[t]$, i.e. $\alpha_2 \neq 0$, now. As $\varphi^{-1} \in k[t]$, we get

$$\begin{aligned}\deg_t(D_t) =& 2\deg_t(\varphi^{-1}) - d_x \deg_t(\alpha_2 t+\alpha_3) + \deg_t\left(\prod_{i=1}^{d_x} p_i\right)\\ =& 2\deg_t(\varphi^{-1}) - d_x + \deg_t\left(\prod_{i=1}^{d_x} p_i\right),\end{aligned}$$

which implies

$$2\deg_t(\varphi^{-1}) = \deg_t(D_t) + d_x - \deg_t\left(\prod_{i=1}^{d_x} p_i\right).$$

Thus, the inequality $d_x - 1 \le \deg_t\left(\prod_{i=1}^{d_x} p_i\right) \le d_x$ yields

$$\begin{aligned}\deg_t(D_t) &= \deg_t(D_t) + d_x - d_x\\ &\le \deg_t(D_t) + d_x - \deg_t\left(\prod_{i=1}^{d_x} p_i\right)\\ &= 2\deg_t(\varphi^{-1})\\ &\le \deg_t(D_t) + d_x - d_x + 1\\ &= \deg_t(D_t) + 1.\end{aligned}$$

As $\deg_t(D_t) \in \{2\mathrm{g}+1, 2\mathrm{g}+2\}$ we conclude $\deg_t(\varphi^{-1}) = \mathrm{g}+1$. From lemma III.14 we know that there is some $\gamma \in k^*$ and some $m \in \mathbb{N}$ such that $\varphi^{-1} = \gamma(\alpha_2 t+\alpha_3)^m$. As $\deg_t(\varphi^{-1}) = \mathrm{g}+1$ and $\alpha_2 \neq 0$, this implies our claim.

□

3.3. Putting Both Relations Together. In this section, we completely characterize the relation between any two bases of a hyperelliptic function field. The main result is theorem III.16. It states that, given a hyperelliptic function field $k(t,u) = k(x,y)$ with two bases, the variable symbol x is a fraction of linear polynomials in the variable symbol t. Furthermore, theorem III.16 gives an explicit formula to compute y from t and u if its minimal polynomial $y^2 = D_x$ and the relation between t and x are known. We also see, that theorem III.16 is a generalization of theorem III.6 as claimed in section 2.

In order to use this theorem to check, if a hyperelliptic function field has two given defining equations, we also need to know the inverse implication. Its easy proof is given in theorem III.18. Hence, the facts proved in this section allow us to check whether a hyperelliptic function field has a given defining equation.

Most of the proof of theorem III.16 has already been completed in the previous sections. Mainly, it remains to compute the constant factor γ whose existence was verified in proposition III.15. Furthermore, we reduce the fraction $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$ such that $\alpha_2 = 1$ or $\alpha_3 = 1$ in order to obtain simpler formulas.

Theorem III.16. *Let $k(t,u) = k(x,y)$ be a hyperelliptic function field and $u^2 = D_t$, $y^2 = D_x$ be the corresponding defining equations. We denote $d_x := \deg_x(D_x)$.*

(1) *If $x \in k[t]$, then there are $\alpha_0, \alpha_1 \in k$ such that $x = \alpha_0 t + \alpha_1$, $\alpha_0 \neq 0$. Furthermore we have $y = \varphi u$ with $\varphi \in k^*$,*
$$\varphi^2 = \alpha_0^{d_x}.$$
(2) *If $x \notin k[t]$, then there are $\alpha_0, \alpha_1, \alpha_3 \in k$, such that $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3}$, $\alpha_0\alpha_3 - \alpha_1 \neq 0$. Furthermore we have $y = \varphi u$ where*
$$\varphi = \frac{\beta}{(t+\alpha_3)^{g+1}},$$
with $\beta \in k$. For β we have the formula
$$\beta^2 = \begin{cases} D_x(\alpha_0) & \text{, if } D_x(\alpha_0) \neq 0 \\ (\alpha_1 - \alpha_0\alpha_3)\tilde{D}_x(\alpha_0) & \text{, if } D_x(\alpha_0) = 0, \end{cases}$$
where $\tilde{D}_x(x) := \frac{D_x(x)}{x-\alpha_0}$.

Proof. Corollary III.9 gives the existence of $\alpha_0, \dots, \alpha_3 \in k$ such that $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$ and $\alpha_0\alpha_3 - \alpha_1\alpha_2 \neq 0$. Proposition III.11 yields some $\varphi \in k(t)^*$ such that $y = \varphi u$. By proposition III.15, we know $\varphi \in k^*$ if $x \in k[t]$ and $\varphi^{-1} = \gamma(\alpha_2 t + \alpha_3)^{g+1}$ with $\gamma \in k^*$ otherwise. Lemma III.12 implies
$$D_t = \varphi^{-2}(\alpha_2 t + \alpha_3)^{-d_x} \prod_{i=1}^{d_x} p_i \tag{2}$$
where $p_i = (\alpha_0 - \alpha_2\eta_i)t + \alpha_1 - \alpha_3\eta_i$ and the $\eta_i \in \overline{k}$ are the zeroes of D_x.

Let us consider the different cases, now:

(1) If $x \in k[t]$, we have $\alpha_2 = 0$. Reducing the fraction $\frac{\alpha_0 t+\alpha_1}{\alpha_3}$, we may assume without loss of generality that $\alpha_3 = 1$, i.e. $x = \alpha_0 t + \alpha_1$. Thus equation (2) becomes
$$D_t = \varphi^{-2} \prod_{i=1}^{d_x} (\alpha_0 t + \alpha_1 - \eta_i).$$

As $\alpha_0 \neq 0$ (which we conclude from $\alpha_0\alpha_3 - \alpha_1\alpha_2 = \alpha_0 \neq 0$) and $\varphi \in k$, the leading coefficient of D_t is

$$1 = \mathrm{lc}_t(D_t) = \varphi^{-2}\alpha_0^{d_x},$$

because D_t is monic by assumption. This implies $\varphi^2 = \alpha_0^{d_x}$.

(2) If $x \notin k[t]$, we have $\alpha_2 \neq 0$. Reducing the fraction $\frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$, we may assume $\alpha_2 = 1$, i.e. $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3}$. We already know $\varphi^{-1} = \gamma(\alpha_2 t + \alpha_3)^{\mathrm{g}+1}$. Setting $\beta := \gamma^{-1}$, it remains to compute β^2. From equation (2), we get

$$D_t = \beta^{-2}(t+\alpha_3)^{2\mathrm{g}+2-d_x}\prod_{i=1}^{d_x} p_i. \tag{3}$$

As before, we compute the leading coefficients:

$$1 = \mathrm{lc}_t(D_t) = \mathrm{lc}_t\left(\beta^{-2}(t+\alpha_3)^{2\mathrm{g}+2-d_x}\prod_{i=1}^{d_x} p_i\right) = \beta^{-2}\mathrm{lc}_t\left(\prod_{i=1}^{d_x} p_i\right).$$

We obtain

$$\beta^2 = \mathrm{lc}_t\left(\prod_{i=1}^{d_x} p_i\right).$$

From lemma III.12, we know $d_x - 1 \leq \deg_t(\prod_{i=1}^{d_x} p_i) \leq d_x$. Thus, there are two cases: $\deg_t(\prod_{i=1}^{d_x} p_i) = d_x$ and $\deg_t(\prod_{i=1}^{d_x} p_i) = d_x - 1$. In the latter case, there is some index j such that $p_j = (\alpha_0 - \eta_j)t + \alpha_1 - \alpha_3\eta_j \in k$, i.e. $\alpha_0 - \eta_j = 0$. Hence $\alpha_0 = \eta_j$, which implies $D_x(\alpha_0) = 0$. In the former case, there is no such index, i.e. we have $D_x(\alpha_0) \neq 0$.

(a) If $D_x(\alpha_0) \neq 0$, we have $\alpha_0 - \eta_i \neq 0$ for all i. Thus we get

$$\begin{aligned}\beta^2 =& \mathrm{lc}_t\left(\prod_{i=1}^{d_x} p_i\right) = \mathrm{lc}_t\left(\prod_{i=1}^{d_x}(\alpha_0-\eta_i)t + \alpha_1 - \alpha_3\eta_i\right)\\ =&\prod_{i=1}^{d_x}(\alpha_0 - \eta_i) = D_x(\alpha_0).\end{aligned}$$

as claimed.

(b) If $D_x(\alpha_0) = 0$, there is some exactly one index j such that $\alpha_0 - \eta_j = 0$. Without loss of generality, we assume $j = d_x$. Thus, $p_{d_x} = \alpha_1 - \alpha_0\alpha_3$. Hence, equation (3) implies

$$\begin{aligned}\beta^2 =& \mathrm{lc}_t\left(\prod_{i=1}^{d_x} p_i\right) = \mathrm{lc}_t\left(\prod_{i=1}^{d_x}(\alpha_0-\eta_i)t + \alpha_1 - \alpha_3\eta_i\right)\\ =&\mathrm{lc}_t\left((\alpha_1 - \alpha_3\eta_{d_x})\prod_{i=1}^{d_x-1}(\alpha_0-\eta_i)t + \alpha_1 - \alpha_3\eta_i\right)\\ =&(\alpha_1 - \alpha_3\eta_{d_x})\prod_{i=1}^{d_x-1}(\alpha_0 - \eta_i)\\ =&(\alpha_1 - \alpha_3\eta_{d_x})\tilde{D}_x(\alpha_0) = (\alpha_1 - \alpha_0\alpha_3)\tilde{D}_x(\alpha_0),\end{aligned}$$

because $\tilde{D}_x(x) = \frac{D_x(x)}{x-\alpha_0} = \frac{D_x(x)}{x-\eta_{d_x}} = \prod_{i=1}^{d_x-1}(x-\eta_i)$.

□

Example III.3. Let $F := \mathbb{F}_{191}(x, y)$,

$$y^2 = D_x := x^6 + 8x^4 + 3x^3 + 5x^2 + 7x + 7.$$

We choose $t := \frac{54x+1}{x-1}$, i.e. $x = \frac{t+1}{t+137}$, and want to have $F = \mathbb{F}_{191}(t,u)$. By theorem III.16 we need to choose u in such a way that $y = \frac{\beta}{(t+137)^3}u$, where

$$\beta^2 = D_x(1) = 31.$$

Euler's criterion yields that $\mathbb{F}_{191}$ does not contain a square root of 31, because $31^{(191-1)/2} \equiv -1 \mod 191$. Hence, there is no $u \in F$ such that $F = \mathbb{F}_{191}(t,u)$.

Nevertheless, we can continue our construction in a constant field extension: The field $\mathbb{F}_{191^2}$ contains a square root[3] of 31 because $31^{(191^2-1)/2} \equiv 1 \mod 191^2$, i.e. $\beta \in \mathbb{F}_{191^2}$. Thus, we can define u such that $F\mathbb{F}_{191^2} = \mathbb{F}_{191^2}(t,u)$. From $y = \varphi u$ we obtain

$$\begin{aligned} D_t =& u^2 = \varphi^{-2}y^2 = \frac{(t+137)^6}{31} \cdot D_x \\ =& t^6 + 36t^5 + 134t^4 + 23t^3 + 94t^2 + 21t. \end{aligned}$$

Since $D_t \in \mathbb{F}_{191}[t]$, we can use it to define a hyperelliptic function field over $\mathbb{F}_{191}$: Let $F' := \mathbb{F}_{191}(t,u)$, $u^2 = t^6+36t^5+134t^4+23t^3+94t^2+21t$. Because $F\mathbb{F}_{191^2} = F'\mathbb{F}_{191^2}$, but $F \neq F'$, we get the following diagram of hyperelliptic function fields.

$$\begin{tikzcd}
 & \mathbb{F}_{191^2}(t,u) = \mathbb{F}_{191^2}(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{F}_{191}(t,u) & & \mathbb{F}_{191}(x,y)
\end{tikzcd}$$

Remark III.17. In section 2, we mentioned that theorem III.16 is a generalization of Lockhart's uniqueness theorem (theorem III.6). Let us examine this fact, now: If $k(t,u) = k(x,y)$ is a hyperelliptic function field as in theorem III.6, then Lockhart proposes $x = \alpha^2 t + \beta$. Theorem III.16 implies $y = \varphi u$ with $\varphi^2 = (\alpha^2)^{d_x} = (\alpha^2)^{2g+1} = (\alpha^{2g+1})^2$, because theorem III.6 applies to imaginary representations, only. From this we get $\varphi = \pm\alpha^{2g+1}$, which is exactly what Lockhart proposes (if $\varphi = -\alpha^{2g+1}$ we interpret the α^2 in $x = \alpha^2 t + \beta$ as $(-\alpha')^2$, which in turn yields $\varphi = (\alpha')^{2g+1}$).

In order to be able to check whether a given hyperelliptic function field has a given defining equation, it is necessary that the inverse implication also holds. Fortunately, this can be proved easily:

Theorem III.18. *Let $k(x,y)$ be a hyperelliptic function field and $y^2 = D_x$ the corresponding defining equation. Let $D_t \in k[T]$ be a monic separable polynomial.*

There exists a basis $t,u \in k(x,y)$ such that $k(x,y) = k(t,u)$, $u^2 = D_t(t)$ iff there exist $t,u \in k(x,y)$ for which $u^2 = D_t(t)$ and the relations $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$, $y = \varphi u$ given in theorem III.16 hold.

Proof. It remains to show that the existence of t,u, $u^2 = D_t(t)$ such that $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$, $y = \varphi u$ as given in theorem III.16 implies $k(x,y) = k(t,u)$. It is obvious, that $k(x) \subseteq k(t)$ and $k(t)(u) = k(t)(y)$. Solving $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$ for t, we see $k(t) \subseteq k(x)$. Thus $k(t) = k(x)$, i.e. $k(t,u) = k(t)(u) = k(t)(y) = k(x)(y) = k(x,y)$. □

[3] One such square root is given by $\beta := 31^{(191^2+1)/4} \in \mathbb{F}_{191^2}$, but we do not need its value—all we need to know is that β is an element of our constant field.

4. Isomorphisms

In this section, we study the implications of the above results for isomorphisms of hyperelliptic function fields. This will enable us to check given function fields for isomorphy and compute the corresponding isomorphisms, as we will see in chapter IV.

The following proposition states that function fields over the same constant field that have the same defining equation are isomorphic.

Proposition III.19. *Let k be an arbitrary field, and $f(T,U) \in k[T,U]$ an irreducible polynomial. Let $F = k(t,u)$, $f(t,u) = 0$ and $G = k(x,y)$, $f(x,y) = 0$ be two function fields. Then the mapping $\Phi : t \mapsto x$, $u \mapsto y$ defines a k-isomorphism $\Phi : F \cong G$.*

Proof. Obviously, the mapping Φ defines a ring-isomorphism $\Phi : k[t,u] \to k[x,y]$ which fixes k. As

$$k(t,u) = k[t,u]/\left(f(t,u) \cdot k[t,u]\right) \text{ and } k(x,y) = k[x,y]/\left(f(x,y) \cdot k[x,y]\right),$$

it suffices to show that $\Phi\left(f(t,u)) \cdot k[t,u]\right) = f(x,y) \cdot k[x,y]$. Let $\varphi \in f(t,u) \cdot k[t,u]$, i.e. $\varphi = f(t,u) \cdot \psi$. Then we have

$$\begin{aligned}\Phi(\varphi) =& \Phi(f(t,u) \cdot \psi)\\ =& \Phi(f(t,u)) \cdot \Phi(\varphi)\\ =& f(\Phi(t),\Phi(u)) \cdot \Phi(\varphi)\\ =& f(x,y) \cdot \Phi(\varphi) \in f(x,y) \cdot k[x,y].\end{aligned}$$

Thus we have $\Phi\left(f(t,u)) \cdot k[t,u]\right) \subseteq f(x,y) \cdot k[x,y]$. In order to show the inverse inclusion let $f(x,y) \cdot \xi \in f(x,y) \cdot k[x,y]$. We obtain

$$\begin{aligned}\Phi^{-1}\left(f(x,y) \cdot \xi\right) =& \Phi^{-1}(f(x,y)) \cdot \Phi^{-1}(\xi)\\ =& f(\Phi^{-1}(x),\Phi^{-1}(y)) \cdot \Phi^{-1}(\xi)\\ =& f(t,u) \cdot \Phi^{-1}(\xi) \in f(t,u) \cdot k[t,u],\end{aligned}$$

i.e. $f(x,y) \cdot \xi \in \Phi\left(f(t,u) \cdot k[t,u]\right)$. □

The above proposition tells us that two function fields having the same defining equation are isomorphic. In the following statement, we will see that the inverse implication also is true: If two function fields are isomorphic, then they have bases such that their defining equations are equal. Together, these facts enable us to check two function fields for isomorphy by testing whether one of them has a basis which satisfies the defining equation of the other.

Proposition III.20. *Let k be a field, F and G function fields over k. Let $F = k(t,u)$, $f(t,u) = 0$, where $f \in k[t,u]$ is irreducible, and let $\Phi : F \to G$ be a k-isomorphism. Then setting $x := \Phi(t)$, $y := \Phi(u)$ implies $G = k(x,y)$, $f(x,y) = 0$, i.e. $f = 0$ is a defining equation for G.*

Proof. Because f is a polynomial, we have

$$f(x,y) = f(\Phi(t),\Phi(u)) = \Phi(f(t,u)) = \Phi(0) = 0.$$

Obviously, this implies $k(x,y) \subseteq G$. It remains to show that $G \subseteq k(x,y)$. Let $\xi \in G$. Then $\Phi^{-1}(\xi) = \frac{\varphi(t,u)}{\psi(t,u)} \in F = k(t,u)$ with polynomials $\varphi, \psi \in k[t,u]$. Applying Φ yields $\xi = \frac{\varphi(\Phi(t),\Phi(u))}{\psi(\Phi(t),\Phi(u))} = \frac{\varphi(x,y)}{\psi(x,y)} \in k(x,y)$. □

Thus, in order to check, whether two hyperelliptic function fields F, G are isomorphic over k, we only need to check whether G has a basis which satisfies the defining equation of F. If $F = k(t, u)$, $u^2 = D_t(t)$ and $G = k(x, y)$, $y^2 = D_x(x)$, where $D_t \in k[t]$ and $D_x \in k[x]$ both are separable, are hyperelliptic function fields, we "just" need to check, whether G has a basis $G = k(t', u')$, such that $(u')^2 = D_t(t')$. This can be done using theorem III.16 as we will see in chapter IV.

Remark III.21. [**Gey74**, Satz 12, Folgerung 2] contains an assertion[4] which is similar to theorem III.18 (if we take propositions III.19 and III.20 into account) and holds in the case, where k is algebraically closed: The set of isomorphism classes of hyperelliptic function fields is given by the spectre[5] of a specific ring.

From Geyer's work it is not obvious how to check two hyperelliptic function fields for isomorphy, algorithmically. In addition, such an algorithm needed to check a given field to be isomorphic to a field whose defining equation contains parameters. Otherwise it would be useless to our intended application of computing automorphism groups.

[4] The author thanks Arieh Cohen for referring him to this result at the MEGA 2003 conference, shortly before this thesis was finished.

[5] i.e. the set of prime ideals, cf. [**Fis56**]

CHAPTER IV

Isomorphisms and Normal Forms

In chapter III we have seen that two hyperelliptic function fields are isomorphic iff they possess the same defining equations. Furthermore, we have proved a necessary and sufficient condition for a hyperelliptic function field to have a given defining equation. In this chapter, we turn our knowledge into explicit algorithms which check hyperelliptic function fields for isomorphisms and defining equations.

In section 1 we present algorithms which check whether a given hyperelliptic function field has a given defining equation. This check can be performed over the given constant field as well as over its algebraic closure. Furthermore, it is possible to construct the smallest constant field extension which has the desired defining equation. As the results of section III.4 suggest, these algorithms can be used to compute isomorphisms, explicitly. We discuss how to do this, in section 2.

Finally, we define a normal form for hyperelliptic function fields in section 3, which enables us to devise a different algorithm for checking isomorphy of hyperelliptic function fields: Two hyperelliptic function fields are equal iff they have the same normal forms.

1. Checking for Defining Equations

In this section, we present an algorithm to check whether a given hyperelliptic function field $k(x, y)$, $y^2 = D_x$ has a given defining equation $u^2 = D_t$, i.e. whether there are $t, u \in k(x, y)$ such that $k(x, y) = k(t, u)$ and $u^2 = D_t$. We consider the case of arbitrary constant fields, first (section 1.1). In section 1.2, we will see, that our algorithm can also be used to construct the minimal constant field extension $k'(x, y)$ which has the defining equation $u^2 = D_t$, whenever such an extension exists. If the constant field is algebraically closed and we are not interested in an explicit formula for a basis, our algorithms can be improved considerably with respect to speed: We replace solving a set of polynomials by checking its solvability, in this situation (section 1.3).

Let us give a crude sketch of our algorithm. According to theorem III.18, there are $t, u \in k(x, y)$ such that $u^2 = D_t$ and $k(x, y) = k(t, u)$ iff there are $t, u \in k(x, y)$ such that $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$ and $y = \varphi u$, where the $\alpha_i \in k$ and φ can be computed from the α_i using theorem III.16. This, in turn, is equivalent to the existence of $t, u \in k(x, y)$ such that $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$, and $D_t = \varphi^{-2} D_x$.

Hence, in order to check, whether $k(x, y) = k(t, u)$, $u^2 = D_t$, we suppose this to be true. We set $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$ symbolically, i.e. we leave the α_i unknown. Next we compute φ from the α_i, which is also done symbolically. Substituting $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$ in D_x and simplifying $D_t = \varphi^{-2} D_x$, we obtain a polynomial equation in t, whose coefficients depend on the α_i. Comparing coefficients yields a set of equations for the α_i. We try to solve this set of equations, together with the inequality $\alpha_0\alpha_3 - \alpha_1\alpha_2 \neq 0$ using Gröbner basis techniques. If a solution exists, we have proved that $k(x, y) = k(t, u)$, $u^2 = D_t$ and we have constructed t and u from x and y. Otherwise, $k(x, y)$ can have no basis t, u satisfying $u^2 = D_t$.

As can even be seen from this sketch of the algorithm, the polynomial D_t does not need to be known, completely. If D_t contains several parameters in its coefficients, which are unknown elements of k, our algorithm is capable to solve for these parameters, as well. This feature will be needed for computing the automorphism group of a hyperelliptic function field, as we will see in chapter V.

1.1. Solving Over the Given Constant Field. In this section, we will give a detailed description of our algorithm to check whether a hyperelliptic function field has a given defining equation. As Gröbner basis techniques are both well known and beyond the scope of this work, we will not discuss them. If a set of polynomial equations has to be solved, we will only say that it is solved using Gröbner basis methods. Nevertheless, such a solving step involves a profound knowledge of Gröbner basis techniques.

We describe our algorithm top down, i.e. we start giving its overall structure, using sub-algorithms which will be discussed later.

Algorithm IV.1. Check a hyperelliptic function field for a defining equation and construct the corresponding basis.

Input: Let $k(x, y)$ be a hyperelliptic function field and $y^2 = D_x$, $D_x \in k[x]$ the corresponding defining equation. Let $s \in \mathbb{N}$, $\theta_0, \ldots, \theta_{s-1}$ be variable symbols and C_0, $C_{\neq 0} \subseteq k[\theta_0, \ldots, \theta_{s-1}]$ finite sets of polynomials. Let $D_t \in k[\theta_0, \ldots, \theta_{s-1}][t]$ be a monic, separable polynomial of degree $\deg_t(D_t) \in \{2\mathrm{g}+1, 2\mathrm{g}+2\}$.

Output: This algorithm reports, whether there exist

$$t, u \in k(x, y) \quad \text{and} \quad \theta_0, \ldots, \theta_{s-1} \in k$$

such that

- $u^2 = D_t$,
- $k(x, y) = k(t, u)$,
- $f(\theta_0, \ldots, \theta_{s-1}) = 0$ for each $f \in C_0$ and
- $h(\theta_0, \ldots \theta_{s-1}) \neq 0$ for each $h \in C_{\neq 0}$.

If this is the case, the algorithm returns $\theta_0, \ldots, \theta_{s-1}, \alpha_0, \ldots, \alpha_3 \in k$ and $\varphi \in k(t)$ such that setting $x =: \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}$ and $y =: \varphi u$, i.e. $t := \frac{\alpha_3 x - \alpha_1}{\alpha_0 - \alpha_2 x}$, $u := \varphi^{-1} y$, implies the above conditions.

Steps:

(1) If $s = 0$, we check the degrees of the factors of D_t and D_x using algorithm IV.2. If this implies that $u^2 = D_t$ is no defining equation of $k(x, y)$, we quit reporting this fact.

(2) We try to construct t, u such that $x \in k[t]$ using algorithm IV.3. If this is possible, we quit returning the constructed parameters.

(3) We try to construct t, u such that $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3} \in k(t)$ and $D_x(\alpha_0) \neq 0$ using algorithm IV.4. If this is possible, we quit returning the constructed parameters.

(4) We try to construct t, u such that $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3} \in k(t)$ and $D_x(\alpha_0) = 0$ using algorithm IV.5. If this is possible, we quit returning the constructed parameters.

(5) Since we did not quit till now, it is impossible to construct t, u. Thus, we report that there exist no $t, u \in k(x, y)$, $\theta_0, \ldots, \theta_{s-1} \in k$ such that the above conditions hold.

As explained above, the correctness of algorithm IV.1 follows from theorem III.18 and the correctness of algorithms IV.2, IV.3, IV.4 and IV.5.

We continue stating algorithm IV.2, which is an application of theorem III.3.

Algorithm IV.2. Check factor degrees of defining equations for compatibility.

Input: Let $k(x, y)$ be a hyperelliptic function field and $y^2 = D_x$, $D_x \in k[x]$ the corresponding defining equation. Let $D_t \in k[t]$ be a monic, separable polynomial.

Output: This algorithm reports, whether we can infer from theorem III.3 that there are no $t, u \in k(x, y)$ such that $k(x, y) = k(t, u)$ and $u^2 = D_t$. If this is not the case, we can deduce nothing from the result of this algorithm.

Steps:

(1) We factor $D_t =: p_1 \cdots p_m$ and $D_x =: q_1 \cdots q_n$ into their non-constant, irreducible factors over k.
(2) If $n \notin \{m - 1, m, m + 1\}$ we report that $u^2 = D_t$ is no defining equation for $k(x, y)$.
(3) Let $\tilde{m} := \max(m, n)$.
Let $d_{t,i} := \deg_t(p_i)$ for $i = 1, \ldots, m$ and $d_{t,i} := 1$ for $i = m + 1, \ldots, \tilde{m}$.
Let $d_{x,i} := \deg_x(q_i)$ for $i = 1, \ldots, n$ and $d_{x,i} := 1$ for $i = n + 1, \ldots, \tilde{m}$.
(4) We sort $(d_{t,i})_{i=1,\ldots,\tilde{m}}$ and $(d_{x,i})_{i=1,\ldots,\tilde{m}}$ such that $d_{t,i} \geq d_{t,j}$ and $d_{x,i} \geq d_{x,j}$ whenever $1 \leq i < j \leq \tilde{m}$.
(5) If there exists an $i \in \{1, \ldots, \tilde{m}\}$ such that $d_{t,i} \neq d_{x,i}$, we report that $u^2 = D_t$ is no defining equation for $k(x, y)$. Otherwise, report that it is unknown, if $u^2 = D_t$ is a defining equation for $k(x, y)$.

Let us prove the correctness of algorithm IV.2:

Proposition IV.1. *Let $k(x, y)$ be a hyperelliptic function field and $y^2 = D_x$, $D_x \in k[x]$ the corresponding defining equation. Let $D_t \in k[t]$ be a monic, separable polynomial. If algorithm IV.2 reports that $u^2 = D_t$ is no defining equation for $k(x, y)$, then this statement is true.*

Proof. We use the notation from algorithm IV.2. Suppose $u^2 = D_t$ is a defining equation of $k(x, y)$ even though the algorithm tells us it is not. There are two possible reasons for the algorithm's statement. We will find a contradiction in both of these cases:

(1) If step (2) quits the algorithm, we have $n \notin \{m-1, m, m+1\}$, which contradicts theorem III.3.
(2) If step (5) quits the algorithm reporting that $u^2 = D_t$ is no defining equation, there needs to be some $i \in \{1, \ldots, \tilde{m}\}$ such that $d_{t,i} \neq d_{x,i}$.
Let us consider the cases given in theorem III.3, separately: If $\deg_t(D_t) = \deg_x(D_x)$, we have $m = n$, i.e. $m = n = \tilde{m}$ and there is a numbering such that $\deg_t(p_i) = \deg_x(q_i)$ for all i. Sorting these degrees, we obtain $d_{t,i} = \deg_t(p_i) = \deg_x(q_i) = d_{x,i}$. Contradiction.
If $\deg_t(D_t) = \deg_x(D_x) + 1$, we have $m = n + 1$, i.e. $\tilde{m} = m = n + 1$. There exists a numbering such that $\deg_t(p_i) = \deg_x(q_i)$ for all $i = 1, \ldots, n$, and $\deg_t(p_m) = 1$. After sorting these degrees, we have $d_{t,i} = \deg_t(p_i) = \deg_x(q_i) = d_{x,i}$ for all $i = 1, \ldots, n$ and $d_{t,m} = \deg_t(p_m) = 1$. Since $d_{x,m} = 1$ was defined in steps (3) and (4), this implies $d_{t,i} = d_{x,i}$ for all i, contradicting the existence of an index i such that $d_{t,i} \neq d_{x,i}$.
If $\deg_t(D_t) + 1 = \deg_x(D_x)$, we obtain a similar contradiction.

□

The following example shows the usefulness of algorithm IV.2 and demonstrates how it works:

Example IV.1. Let $\mathbb{F}_{43}(x,y)$,

$$y^2 = D_x := x^9 + 17x^8 + 24x^7 + 39x^5 + 41x^4 + 13x$$

and $D_t := t^{10} + 31t^9 + 23t^8 + 16t^7 + 14t^6 + 5t^4 + 15t^3 + 3t^2 + 2t + 10$. We apply algorithm IV.2 literally:

(1) Factoring yields:

$$\begin{aligned} D_t =&(t^2 + 26t + 7) \cdot (t^4 + 29t^3 + 25t^2 + 22t + 16) \\ &\cdot (t^2 + 42t + 26) \cdot (t^2 + 20t + 35) \\ D_x =&(x^2 + 26x + 35) \cdot x \cdot (x^2 + 18x + 9) \cdot (x^4 + 16x^3 + 12x^2 + 5x + 4) \end{aligned}$$

(2) Since $m = n = 4$, we continue.

(3) $\tilde{m} := 4, \quad d_{t,1} := 2, \quad d_{t,2} := 4, \quad d_{t,3} := 2, \quad d_{t,4} := 2,$
$d_{x,1} := 2, \quad d_{x,2} := 1, \quad d_{x,3} := 2, \quad d_{x,4} := 4.$

(4) Sorting yields $d_{t,1} := 4, \quad d_{t,2} := 2, \quad d_{t,3} := 2, \quad d_{t,4} := 2,$
$d_{x,1} := 4, \quad d_{x,2} := 2, \quad d_{x,3} := 2, \quad d_{x,4} := 1.$

(5) Because of $d_{t,4} \neq d_{x,4}$, we infer that $u^2 = D_t$ is no defining equation for $\mathbb{F}_{43}(x,y)$

Although algorithm IV.2 cannot decide, whether a given hyperelliptic function field has a given defining equation, it still is useful. Because it is very efficient, we do not loose much time in algorithm IV.1, if we use it. On the contrary, we may save a huge amount of time in the remaining steps of algorithm IV.1, if algorithm IV.2 can already tell us that t, u do not exist.

Let us describe the first of the remaining steps of algorithm IV.1 which corresponds to the first case of theorem III.16.

Algorithm IV.3. Check a hyperelliptic function field $k(x,y)$ for having a defining equation $u^2 = D_t$ with $x \in k[t]$.

Input: Let $k(x,y)$ be a hyperelliptic function field and $y^2 = D_x$, $D_x \in k[x]$ the corresponding defining equation. Let $s \in \mathbb{N}$, $\theta_0, \ldots, \theta_{s-1}$ be variable symbols and C_0, $C_{\neq 0} \subseteq k[\theta_0, \ldots, \theta_{s-1}]$ finite sets of polynomials. Let $D_t \in k[\theta_0, \ldots, \theta_{s-1}][t]$ be a monic, separable polynomial of degree $\deg_t(D_t) \in \{2\mathrm{g}+1, 2\mathrm{g}+2\}$.

We denote $d_x := \deg_x(D_x)$.

Output: This algorithm reports, whether there exist

$$t, u \in k(x,y) \quad \text{and} \quad \theta_0, \ldots, \theta_{s-1} \in k$$

such that

- $x \in k[t]$,
- $u^2 = D_t$,
- $k(x,y) = k(t,u)$,
- $f(\theta_0, \ldots, \theta_{s-1}) = 0$ for each $f \in C_0$ and
- $h(\theta_0, \ldots \theta_{s-1}) \neq 0$ for each $h \in C_{\neq 0}$.

If this is the case, the algorithm returns $\theta_0, \ldots, \theta_{s-1}, \alpha_0, \alpha_1, \varphi \in k$ such that setting $t := \frac{x-\alpha_1}{\alpha_0}$ and $u := \varphi^{-1}y$ implies the above conditions.

Steps:

(1) We substitute $x = \alpha_0 t + \alpha_1$ into D_x, symbolically. We expand the resulting polynomial and denote it by $D_{x,t} \in k[\alpha_0, \alpha_1][t]$.

(2) We simplify the polynomial equation $D_{x,t} = \alpha_0^{d_x} D_t$ and compare coefficients of t. The resulting set of polynomials which need to be $= 0$ is denoted by

$$E_0' \subseteq k[\alpha_0, \alpha_1, \theta_0, \ldots, \theta_{s-1}].$$

(3) Let $E_0 := E_0' \cup C_0$. This is the set of polynomials, which need to be $= 0$.

(4) Let $E_{\neq 0} := \{\alpha_0\} \cup C_{\neq 0}$. This is the set of polynomials, which need to be $\neq 0$ simultaneously.

(5) We transform $E_{\neq 0}$ into a polynomial which needs to be $= 0$. To do so, we choose a variable symbol $z \notin \{t, u, \alpha_0, \alpha_1, \theta_0, \ldots, \theta_{s-1}\}$. We set

$$e_{\neq 0} := 1 - z \cdot \left(\prod_{h \in E_{\neq 0}} h \right).$$

(6) We set $E := E_0 \cup \{e_{\neq 0}\}$ and try to solve $E = 0$ using Gröbner basis methods. If there exists a solution $(\alpha_0, \alpha_1, \theta_0, \ldots, \theta_{s-1}, z) \in k^{s+3}$, we try to compute $\varphi \in k$ such that $\varphi^2 = \alpha_0^{d_x}$. If φ exists, we return $\alpha_0, \alpha_1, \varphi$ which determine t and u, as well as $\theta_0, \ldots, \theta_{s-1}$ which define $D_t \in k[t]$.

(7) If step (6) does not yield a solution, we report that there are no $\theta_0, \ldots, \theta_{s-1} \in k$ such that there exists a basis $k(x, y) = k(t, u)$ with $x \in k[t]$ and $u^2 = D_t$.

We prove the correctness of algorithm IV.3 in proposition IV.3. To do so, we start showing that the transformation in step (5) is correct.

Lemma IV.2. *Let k be a field, $X_0, \ldots, X_{n-1}$ transcendental over k (variable symbols), $E_{\neq 0} \subseteq k[X_0, \ldots, X_{n-1}]$ finite and $Z \notin \{X_0, \ldots, X_{n-1}\}$ a new variable symbol. We define*

$$e(X_0, \ldots, X_{n-1}, Z) := 1 - Z \cdot \left(\prod_{h \in E_{\neq 0}} h \right).$$

Then the following assertions are equivalent

(1) *There exist $x_0, \ldots, x_{n-1} \in k$ such that $h(x_0, \ldots, x_{n-1}) \neq 0$ for each $h \in E_{\neq 0}$.*

(2) *There exist $x_0, \ldots, x_{n-1}, z \in k$ such that $e(x_0, \ldots, x_{n-1}, z) = 0$.*

If this is the case, each solution $(x_0, \ldots, x_{n-1}, z) \in k^{n+1}$ of $e = 0$ immediately yields a solution $(x_0, \ldots, x_{n-1})$ of $E_{\neq 0} \neq 0$.

Proof. Let $h(x_0, \ldots, x_{n-1}) \neq 0$ for each $h \in E_{\neq 0}$. Then

$$\prod_{h \in E_{\neq 0}} h(x_0, \ldots, x_{n-1}) \neq 0.$$

Since k is a field, we can define $z := \left(\prod_{h \in E_{\neq 0}} h(x_0, \ldots, x_{n-1}) \right)^{-1}$. We obtain

$$z \cdot \prod_{h \in E_{\neq 0}} h(x_0, \ldots, x_{n-1}) = 1,$$

i.e. $e(x_0, \ldots, x_{n-1}, z) = 0$.

On the other hand, let $e(x_0, \ldots, x_{n-1}, z) = 0$. Then $z \prod_{h \in E_{\neq 0}} h(x_0, \ldots, x_{n-1}) = 1$, i.e.

$$\prod_{h \in E_{\neq 0}} h(x_0, \ldots, x_{n-1}) \neq 0.$$

Thus, each $h(x_0, \ldots, x_{n-1}) \neq 0$. □

Using this lemma, we can prove the correctness of algorithm IV.3.

Proposition IV.3. *We use the notations of algorithm IV.3. The algorithm yields a solution iff there exist $t, u \in k(x,y)$ and $\theta_0, \dots, \theta_{s-1} \in k$ such that*

- $x \in k[t]$,
- $u^2 = D_t$,
- $k(x,y) = k(t,u)$,
- $f(\theta_0, \dots, \theta_{s-1}) = 0$ *for each* $f \in C_0$ *and*
- $h(\theta_0, \dots \theta_{s-1}) \neq 0$ *for each* $h \in C_{\neq 0}$.

Proof. Let the algorithm yield a solution. Then, there are

$$\alpha_0, \alpha_1, \varphi, \theta_0, \dots, \theta_{s-1}, z \in k$$

solving E and $\varphi^2 = \alpha_0^{d_x}$. Because of

$$E = E_0 \cup \{e_{\neq 0}\} = E_0' \cup C_0 \cup \{e_{\neq 0}\},$$

we obtain the following facts.

(1) $f(\alpha_0, \alpha_1, \theta_0, \dots, \theta_{s-1}) = 0$ for each $f \in E_0'$. Thus $\alpha_0^{d_x} D_t = D_{x,t} \in k[t]$.
(2) $f(\theta_0, \dots, \theta_{s-1}) = 0$ for each $f \in C_0$.
(3) $e_{\neq 0}(\alpha_0, \alpha_1, \theta_0, \dots, \theta_{s-1}, z) = 0$. Thus lemma IV.2 implies $\alpha_0 \neq 0$ and

$$h(\theta_0, \dots, \theta_{s-1}) \neq 0 \quad \text{for all} \quad h \in C_{\neq 0}.$$

Setting $t := \frac{1}{\alpha_0}(x - \alpha_1) \in k(x,y)$ we obtain $x = \alpha_0 t + \alpha_1 \in k[t]$ and $D_{x,t} = D_x$. Because of $\varphi \in k$, we also have $u := \varphi^{-1} y \in k(x,y)$. Thus,

$$u^2 = \varphi^{-2} y^2 = \alpha_0^{-d_x} D_x = \alpha_0^{-d_x} D_{x,t} = \alpha_0^{d_x - d_x} D_t = D_t.$$

By theorem III.18, this implies $k(x,y) = k(t,u)$, as claimed.

Let $\theta_0, \dots, \theta_{s-1} \in k$ be a solution of $C_0 = 0$ and $C_{\neq 0} \neq 0$ and $t, u \in k(x,y)$ a basis such that $u^2 = D_t(\theta_0, \dots, \theta_{s-1}, t)$ and $x \in k[t]$. By theorem III.16, there are $\alpha_0, \alpha_1 \in k$, such that $x = \alpha_0 t + \alpha_1$ and $\alpha_0 \neq 0$. Furthermore, there exists $\varphi \in k$ such that $\varphi^2 = \alpha_0^{d_x}$ and $y = \varphi u$. Thus, $\alpha_0^{d_x} D_t = \varphi^2 u^2 = y^2 = D_x$. Hence, $\alpha_0, \alpha_1, \theta_0, \dots, \theta_{s-1}$ are a solution to $E_0' = 0$. Since the θ_i solve $C_0 = 0$ and $C_{\neq 0} \neq 0$, we know that $\alpha_0, \alpha_1, \theta_0, \dots, \theta_{s-1}$ solve $E_0 = 0$ and $E_{\neq 0} \neq 0$. By lemma IV.2, there exists a $z \in k$, such that $\alpha_0, \alpha_1, \theta_0, \dots, \theta_{s-1}, z$ solve $e_{\neq 0} = 0$. Hence, these elements solve $E = 0$. Because $\varphi \in k$, step (6) returns a solution. □

In the following example, we demonstrate, how algorithm IV.3 works.

Example IV.2. Let $F = \mathbb{F}_{11}(x,y)$, $y^2 = D_x := x^5 + x^4 + 4x^3 + 5x^2 + 10x + 7$. We would like to know, if there is a basis $F = \mathbb{F}_{11}(t,u)$ such that $u^2 = D_t := t^5 + 7t^3 + 9t^2 + 9t + 6$ and $x \in \mathbb{F}_{11}[t]$. Thus, we choose $s := 0$, $C_0 := C_{\neq 0} := \emptyset$.

(1) Substituting $x = \alpha_0 t + \alpha_1$ into D_x, we get

$$\begin{aligned} D_{x,t} = D_x(\alpha_0 t + \alpha_1) = & \alpha_0^5 t^5 \\ & + (5\alpha_0^4 \alpha_1 + \alpha_0^4) t^4 \\ & + (10\alpha_0^3 \alpha_1^2 + 4\alpha_0^3 \alpha_1 + 4\alpha_0^3) t^3 \\ & + (10\alpha_0^2 \alpha_1^3 + 6\alpha_0^2 \alpha_1^2 + \alpha_0^2 \alpha_1 + 5\alpha_0^2) t^2 \\ & + (5\alpha_0 \alpha_1^4 + 4\alpha_0 \alpha_1^3 + \alpha_0 \alpha_1^2 + 10\alpha_0 \alpha_1 + 10\alpha_0) t \\ & + \alpha_1^5 + \alpha_1^4 + 4\alpha_1^3 + 5\alpha_1^2 + 10\alpha_1 + 7 \end{aligned}$$

where α_0, α_1 are to be found.

(2) Comparing coefficients in $D_{x,t} = \alpha_0^5 D_t$ yields the equations E_0':

$$\begin{aligned}0 =&5\alpha_0^4\alpha_1 + \alpha_0^4,\\ 0 =&10\alpha_0^3\alpha_1^2 + 4\alpha_0^3\alpha_1 + 4\alpha_0^3 - 7\alpha_0^5,\\ 0 =&10\alpha_0^2\alpha_1^3 + 6\alpha_0^2\alpha_1^2 + \alpha_0^2\alpha_1 + 5\alpha_0^2 - 9\alpha_0^5,\\ 0 =&5\alpha_0\alpha_1^4 + 4\alpha_0\alpha_1^3 + \alpha_0\alpha_1^2 + 10\alpha_0\alpha_1 + 10\alpha_0 - 9\alpha_0^5,\\ 0 =&\alpha_1^5 + \alpha_1^4 + 4\alpha_1^3 + 5\alpha_1^2 + 10\alpha_1 + 7 - 6\alpha_0^5.\end{aligned}$$

(3) Let $E_0 := E_0'$.

(4) Let $E_{\neq 0} := \{\alpha_0\}$.

(5) Let $e_{\neq 0} := 1 - \alpha_0 z$.

(6) Let $E := E_0 \cup \{e_{\neq 0}\}$. We interpret E as an ideal $Ek[\alpha_0, \alpha_1, z]$. Singular ([**GPS$^+$02**]) computes the following Gröbner basis of E with respect to the lexicographical ordering:

$$\begin{aligned}z - 4 =&0\\ \alpha_0 - 3 =&0\\ \alpha_1 - 2\alpha_0^5 z^2 - 3\alpha_0^2 z^2 =&0\end{aligned}$$

This implies $z = 4$, $\alpha_0 = 3$. Substituting these values into the remaining equation, we obtain $\alpha_1 = 2$. Setting $t := 4x - 3$, $u := y$, i.e. $x = 3t + 2$, $\varphi = 3^5 = 1$, we get a basis $F = \mathbb{F}_{11}(t, u)$, with $u^2 = D_t$.

We continue presenting algorithm IV.4, which corresponds to the second case of theorem III.16, i.e. the case $x = \frac{\alpha_0 t + \alpha_1}{t + \alpha_3} \in k(t)$, where $D_x(\alpha_0) \neq 0$.

Algorithm IV.4. Check a hyperelliptic function field $k(x, y)$ for having a defining equation $u^2 = D_t$ with $x = \frac{\alpha_0 t + \alpha_1}{t + \alpha_3}$ and $D_x(\alpha_0) \neq 0$.

Input: Let $k(x, y)$ be a hyperelliptic function field and $y^2 = D_x$, $D_x \in k[x]$ the corresponding defining equation. Let $s \in \mathbb{N}$, $\theta_0, \ldots, \theta_{s-1}$ be variable symbols and C_0, $C_{\neq 0} \subseteq k[\theta_0, \ldots, \theta_{s-1}]$ finite sets of polynomials. Let $D_t \in k[\theta_0, \ldots, \theta_{s-1}][t]$ be a monic, separable polynomial of degree $\deg_t(D_t) \in \{2\mathrm{g} + 1, 2\mathrm{g} + 2\}$.

We denote $d_x := \deg_x(D_x)$.

Output: This algorithm reports, whether there exist

$$t, u \in k(x, y) \quad \text{and} \quad \theta_0, \ldots, \theta_{s-1} \in k$$

such that

- $x = \frac{\alpha_0 t + \alpha_1}{t + \alpha_3} \in k(t)$ with $\alpha_0, \alpha_1, \alpha_3 \in k$ and $D_x(\alpha_0) \neq 0$,
- $u^2 = D_t$,
- $k(x, y) = k(t, u)$,
- $f(\theta_0, \ldots, \theta_{s-1}) = 0$ for each $f \in C_0$ and
- $h(\theta_0, \ldots \theta_{s-1}) \neq 0$ for each $h \in C_{\neq 0}$.

If this is the case, the algorithm returns $\theta_0, \ldots, \theta_{s-1}, \alpha_0, \alpha_1, \alpha_3 \in k$ and $\varphi \in k(t)$ such that setting $t := \frac{\alpha_3 x - \alpha_1}{\alpha_0 - x}$ and $u := \varphi^{-1} y$ implies the above conditions.

Steps:

(1) We substitute $x = \frac{\alpha_0 t + \alpha_1}{t + \alpha_3}$ into D_x, symbolically. We expand the result, factor out the denominator $(t + \alpha_3)^{-d_x}$ and denote this product by

$$D_x(\frac{\alpha_0 t + \alpha_1}{t + \alpha_3}) =: (t + \alpha_3)^{-d_x} \cdot D_{x,t},$$

i.e. $D_{x,t} \in k[\alpha_0, \alpha_1, \alpha_3][t]$.

(2) We simplify the polynomial equation $D_x(\alpha_0) \cdot D_t = (t+\alpha_3)^{2g+2-d_x} \cdot D_{x,t}$ and compare coefficients of t. The resulting set of polynomials which need to be $= 0$ is denoted by $E_0' \subseteq k[\alpha_0, \alpha_1, \alpha_3, \theta_0, \dots, \theta_{s-1}]$.
(3) Let $E_0 := E_0' \cup C_0$. This is the set of polynomials, which need to be $= 0$.
(4) Let $E_{\neq 0} := \{\alpha_0\alpha_3 - \alpha_1, D_x(\alpha_0)\} \cup C_{\neq 0}$. This is the set of polynomials, which need to be $\neq 0$ simultaneously.
(5) We transform $E_{\neq 0}$ into a polynomial which needs to be $= 0$. To do so, we choose a variable symbol $z \notin \{t, u, \alpha_0, \alpha_1, \alpha_3, \theta_0, \dots, \theta_{s-1}\}$. We set

$$e_{\neq 0} := 1 - z \cdot \left(\prod_{h \in E_{\neq 0}} h \right).$$

(6) We set $E := E_0 \cup \{e_{\neq 0}\}$ and try to solve $E = 0$ using Gröbner basis methods. If there exists a solution $(\alpha_0, \alpha_1, \alpha_3, \theta_0, \dots, \theta_{s-1}, z)$, we try to compute $\beta \in k$ such that $\beta^2 = D_x(\alpha_0)$. If β exists, we return $\alpha_0, \alpha_1, \alpha_3$ and $\varphi := \frac{\beta}{(t+\alpha_3)^{g+1}} \in k(t)$ which determine t and u, as well as $\theta_0, \dots, \theta_{s-1}$ which define a possible $D_t \in k[t]$.
(7) If step (6) does not yield a solution, we report that there are no $\theta_0, \dots, \theta_{s-1} \in k$ such that there exists a basis $k(x, y) = k(t, u)$ with $x = \frac{\alpha_0 t + \alpha_1}{t + \alpha_3} \in k(t)$, $D_x(\alpha_0) \neq 0$ and $u^2 = D_t$.

The correctness of algorithm IV.4 is shown analogously to proposition IV.3:

Proposition IV.4. *We use the notations from algorithm IV.4. The algorithm yields a solution iff there exist $t, u \in k(x, y)$ and $\theta_0, \dots, \theta_{s-1} \in k$ such that*

- $x = \frac{\alpha_0 t + \alpha_1}{t + \alpha_3} \in k(t)$ *with* $\alpha_0, \alpha_1, \alpha_3 \in k$ *and* $D_x(\alpha_0) \neq 0$,
- $u^2 = D_t$,
- $k(x, y) = k(t, u)$,
- $f(\theta_0, \dots, \theta_{s-1}) = 0$ *for each* $f \in C_0$ *and*
- $h(\theta_0, \dots \theta_{s-1}) \neq 0$ *for each* $h \in C_{\neq 0}$.

Proof. Let the algorithm yield a solution. Then, there are

$$\alpha_0, \alpha_1, \alpha_3, \beta, \theta_0, \dots, \theta_{s-1}, z \in k$$

solving E and $\beta^2 = D_x(\alpha_0)$. Because of

$$E = E_0' \cup C_0 \cup \{e_{\neq 0}\},$$

we obtain the following facts.

(1) $f(\alpha_0, \alpha_1, \alpha_3, \theta_0, \dots, \theta_{s-1}) = 0$ for each $f \in E_0'$. Thus $D_x(\alpha_0) \cdot D_t = (t + \alpha_3)^{2g+2-d_x} \cdot D_{x,t}$, i.e.

$$D_{x,t} = \frac{D_x(\alpha_0)}{(t+\alpha_3)^{2g+2-d_x}} \cdot D_t.$$

(2) $f(\theta_0, \dots, \theta_{s-1}) = 0$ for each $f \in C_0$.
(3) $e_{\neq 0}(\alpha_0, \alpha_1, \alpha_3, \theta_0, \dots, \theta_{s-1}, z) = 0$. Thus lemma IV.2 implies $\alpha_0\alpha_3 - \alpha_1 \neq 0$ as well as $D_x(\alpha_0) \neq 0$ and

$$h(\theta_0, \dots, \theta_{s-1}) \neq 0 \quad \text{for all} \quad h \in C_{\neq 0}.$$

Setting $t := \frac{\alpha_1 - \alpha_3 x}{x - \alpha_0} \in k(x, y)$ we obtain $x = \frac{\alpha_0 t + \alpha_1}{t + \alpha_3}$ and $(t + \alpha_3)^{-d_x} \cdot D_{x,t} = D_x$. Because of $\varphi := \frac{\beta}{(t+\alpha_3)^{g+1}} \in k(t)^* \subseteq k(x, y)^*$, we also have $u := \varphi^{-1} y \in k(x, y)$.

Thus,

$$\begin{aligned}
u^2 =&\varphi^{-2}y^2 \\
=&\frac{(t+\alpha_3)^{2g+2}}{\beta^2}\cdot D_x \\
=&\frac{(t+\alpha_3)^{2g+2}}{D_x(\alpha_0)}\cdot(t+\alpha_3)^{-d_x}\cdot D_{x,t} \\
=&\frac{(t+\alpha_3)^{2g+2-d_x}}{D_x(\alpha_0)}\cdot D_{x,t} \\
=&\frac{(t+\alpha_3)^{2g+2-d_x}}{D_x(\alpha_0)}\cdot\frac{D_x(\alpha_0)}{(t+\alpha_3)^{2g+2-d_x}}\cdot D_t \\
=&D_t.
\end{aligned}$$

By theorem III.18, this implies $k(x,y) = k(t,u)$, as claimed.

Let $\theta_0,\dots,\theta_{s-1}\in k$ be a solution of $C_0 = 0$ and $C_{\neq 0}\neq 0$ and $t,u\in k(x,y)$ a basis such that $u^2 = D_t(\theta_0,\dots,\theta_{s-1},t)$ and $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3}$ with $\alpha_0,\alpha_1,\alpha_3\in k$ and $D_x(\alpha_0)\neq 0$. Proposition III.8 implies $\alpha_0\alpha_3-\alpha_1\neq 0$. By theorem III.16 there exists $\beta\in k$ such that $\beta^2 = D_x(\alpha_0)$ and $y=\varphi u$ with $\varphi := \frac{\beta}{(t+\alpha_3)^{g+1}}$. Thus,

$$\begin{aligned}
D_x(\alpha_0)\cdot D_t =&\frac{D_x(\alpha_0)}{(t+\alpha_3)^{2g+2}}(t+\alpha_3)^{2g+2}\cdot u^2 \\
=&\varphi^2(t+\alpha_3)^{2g+2}u^2 \\
=&(t+\alpha_3)^{2g+2}y^2 \\
=&(t+\alpha_3)^{2g+2}D_x \\
=&(t+\alpha_3)^{2g+2-d_x}D_{x,t}.
\end{aligned}$$

Hence, $\alpha_0,\alpha_1,\alpha_3,\theta_0,\dots,\theta_{s-1}$ are a solution to $E_0' = 0$. Since the θ_i solve $C_0 = 0$ and $C_{\neq 0}\neq 0$, we know that $\alpha_0,\alpha_1,\alpha_3,\theta_0,\dots,\theta_{s-1}$ solve $E_0 = 0$ and $E_{\neq 0}\neq 0$. By lemma IV.2, there exists a $z\in k$, such that $\alpha_0,\alpha_1,\alpha_3,\theta_0,\dots,\theta_{s-1},z$ solve $e_{\neq 0} = 0$. Hence, these elements solve $E = 0$. Because $\beta\in k$, step (6) returns a solution. □

The next example shows how algorithm IV.4 works.

EXAMPLE IV.3. Let $F = \mathbb{F}_{79}(x,y)$, $y^2 = D_x := x^5+49x^4+21x^2+13$. We would like to know, if there is a basis $F = \mathbb{F}_{79}(t,u)$ such that $u^2 = D_t := t^6+28t^5+71t^4+39t^3+18t+3$ and $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3}\in\mathbb{F}_{79}(t)$ with $D_x(\alpha_0)\neq 0$. Thus, we choose $s := 0$, $C_0 := C_{\neq 0} := \emptyset$.

(1) Substituting $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3}$ into D_t, we get

$$\begin{aligned}
D_{x,t} =&(t+\alpha_3)^5\cdot D_x \\
=&(\alpha_0^5+49\alpha_0^4+21\alpha_0^2+13)t^5 \\
&+(49\alpha_0^4\alpha_3+5\alpha_0^4\alpha_1+38\alpha_0^3\alpha_1+63\alpha_0^2\alpha_3+42\alpha_0\alpha_1+65\alpha_3)t^4 \\
&+(38\alpha_0^3\alpha_3\alpha_1+10\alpha_0^3\alpha_1^2+63\alpha_0^2\alpha_3^2+57\alpha_0^2\alpha_1^2 \\
&\quad+47\alpha_0\alpha_3\alpha_1+51\alpha_3^2+21\alpha_1^2)t^3 \\
&+(21\alpha_0^2\alpha_3^3+57\alpha_0^2\alpha_3\alpha_1^2+10\alpha_0^2\alpha_1^3+47\alpha_0\alpha_3^2\alpha_1 \\
&\quad+38\alpha_0\alpha_1^3+51\alpha_3^3+63\alpha_3\alpha_1^2)t^2 \\
&+(42\alpha_0\alpha_3^3\alpha_1+38\alpha_0\alpha_3\alpha_1^3+5\alpha_0\alpha_1^4+65\alpha_3^4+63\alpha_3^2\alpha_1^2+49\alpha_1^4)t \\
&+13\alpha_3^5+21\alpha_3^3\alpha_1^2+49\alpha_3\alpha_1^4+\alpha_1^5
\end{aligned}$$

where $\alpha_0, \alpha_1, \alpha_3$ are to be found.

(2) Comparing coefficients in $D_x(\alpha_0)D_t = (t+\alpha_3)D_{x,t}$, i.e. in

$$(\alpha_0^5 + 49\alpha_0^4 + 21\alpha_0^2 + 13) \cdot (t^6 + 28t^5 + 71t^4 + 39t^3 + 18t + 3) = (t + \alpha_3)D_{x,t}$$

yields the equations E_0', which we omit for the sake of readability.

(3) Let $E_0 := E_0'$.

(4) Let $E_{\neq 0} := \{\alpha_0\alpha_3 - \alpha_1, \alpha_0^5 + 49\alpha_0^4 + 21\alpha_0^2 + 13\}$.

(5) Let $e_{\neq 0} := 1 - (\alpha_0\alpha_3 - \alpha_1) \cdot (\alpha_0^5 + 49\alpha_0^4 + 21\alpha_0^2 + 13) \cdot z$.

(6) Let $E := E_0 \cup \{e_{\neq 0}\}$. We interpret E as an ideal $E\mathbb{F}_{79}[\alpha_0, \alpha_1, \alpha_3, z]$. Using Singular ([**GPS$^+$02**]) we compute a Gröbner basis of E with respect to the lexicographical ordering, which implies $z = 27$ and $\alpha_0 = 3$. Substituting this, we obtain $\alpha_1 = 28$, which finally yields $\alpha_3 = 58$.
Unfortunately, $D_x(\alpha_0) = 68$ is no square in $\mathbb{F}_{79}$. Thus, there is no β such that $\beta^2 = D_x(\alpha_0)$.

(7) There is no basis $t, u \in \mathbb{F}_{79}(x, y)$, such that $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3}$, $D_x(\alpha_0) \neq 0$.

If we consider $F\mathbb{F}_{79^2}$ instead, there exists a square root $\beta \in \mathbb{F}_{79^2}$ of $D_x(\alpha_0) = 68$, because $68^{(79^2-1)/2} = 1 \in \mathbb{F}_{79^2}$ (Euler's criterion). Hence, given this field, our algorithm successfully computes the requested basis.

In order to describe algorithm IV.1, it remains to give algorithm IV.5, which corresponds to the third case of theorem III.16: $k(x, y) = k(t, u)$, $u^2 = D_t$, where $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3}$ and $D_x(\alpha_0) = 0$.

In this case, we have only very few possibilities to choose α_0: The zeroes of D_x. On the other hand, we need to consider these zeroes separately, since we need to know α_0 in order to compute φ.

Algorithm IV.5. Check a hyperelliptic function field $k(x, y)$ for having a defining equation $u^2 = D_t$ with $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3}$ and $D_x(\alpha_0) = 0$.

Input: Let $k(x, y)$ be a hyperelliptic function field and $y^2 = D_x$, $D_x \in k[x]$ the corresponding defining equation. Let $s \in \mathbb{N}$, $\theta_0, \ldots, \theta_{s-1}$ be variable symbols and C_0, $C_{\neq 0} \subseteq k[\theta_0, \ldots, \theta_{s-1}]$ finite sets of polynomials. Let $D_t \in k[\theta_0, \ldots, \theta_{s-1}][t]$ be a monic, separable polynomial of degree $\deg_t(D_t) \in \{2g + 1, 2g + 2\}$.

We denote $d_x := \deg_x(D_x)$.

Output: This algorithm reports, whether there exist

$$t, u \in k(x, y) \quad \text{and} \quad \theta_0, \ldots, \theta_{s-1} \in k$$

such that

- $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3} \in k(t)$ with $\alpha_0, \alpha_1, \alpha_3 \in k$ and $D_x(\alpha_0) = 0$,
- $u^2 = D_t$,
- $k(x, y) = k(t, u)$,
- $f(\theta_0, \ldots, \theta_{s-1}) = 0$ for each $f \in C_0$ and
- $h(\theta_0, \ldots \theta_{s-1}) \neq 0$ for each $h \in C_{\neq 0}$.

If this is the case, the algorithm returns $\theta_0, \ldots, \theta_{s-1}, \alpha_0, \alpha_1, \alpha_3 \in k$ and $\varphi \in k(t)$ such that setting $t := \frac{\alpha_3 x-\alpha_1}{\alpha_0 - x}$ and $u := \varphi^{-1}y$ implies the above conditions.

Steps:

(1) We factor D_x over k in order to obtain its zeroes. For each $\alpha_0 \in k$ such that $D_x(\alpha_0) = 0$ we do the following:

(1.1) We substitute $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3}$ into D_x, symbolically. We expand the result, factor out the denominator $(t+\alpha_3)^{-d_x}$ and denote this product by

$$D_x(\frac{\alpha_0 t+\alpha_1}{t+\alpha_3}) =: (t+\alpha_3)^{-d_x} \cdot D_{x,t},$$

i.e. $D_{x,t} \in k[\alpha_1, \alpha_3][t]$.

(1.2) We compute the polynomial $\tilde{D}_x(x) := \frac{D_x(x)}{x-\alpha_0} \in k[x]$.

(1.3) We simplify the polynomial equation

$$(\alpha_1 - \alpha_0\alpha_3) \cdot \tilde{D}_x(\alpha_0) \cdot D_t = (t+\alpha_3)^{2\mathrm{g}+2-d_x} \cdot D_{x,t}$$

and compare coefficients of t. The resulting set of polynomials which need to be $= 0$ is denoted by $E_0' \subseteq k[\alpha_1, \alpha_3, \theta_0, \ldots, \theta_{s-1}]$.

(1.4) Let $E_0 := E_0' \cup C_0$. This is the set of polynomials, which need to be $= 0$.

(1.5) Let $E_{\neq 0} := \{\alpha_0\alpha_3 - \alpha_1\} \cup C_{\neq 0}$. This is the set of polynomials, which need to be $\neq 0$ simultaneously.

(1.6) We transform $E_{\neq 0}$ into a polynomial which needs to be $= 0$. To do so, we choose a variable symbol $z \notin \{t, u, \alpha_1, \alpha_3, \theta_0, \ldots, \theta_{s-1}\}$. We set

$$e_{\neq 0} := 1 - z \cdot \left(\prod_{h \in E_{\neq 0}} h \right).$$

(1.7) We set $E := E_0 \cup \{e_{\neq 0}\}$ and try to solve $E = 0$ using Gröbner basis methods. If there exists a solution $(\alpha_1, \alpha_3, \theta_0, \ldots, \theta_{s-1}, z)$, we try to compute $\beta \in k$ such that $\beta^2 = (\alpha_1 - \alpha_0\alpha_3)\tilde{D}_x(\alpha_0)$. If β exists, we return $\alpha_0, \alpha_1, \alpha_3$ and $\varphi := \frac{\beta}{(t+\alpha_3)^{\mathrm{g}+1}} \in k(t)$ which determine t and u, as well as $\theta_0, \ldots, \theta_{s-1}$ which define a possible $D_t \in k[t]$.

(2) If step (1.7) does not yield a solution for any $\alpha_0 \in k$ with $D_x(\alpha_0) = 0$, we report that there are no $\theta_0, \ldots, \theta_{s-1} \in k$ such that there exists a basis $k(x, y) = k(t, u)$ satisfying the above conditions.

Let us consider the correctness of this algorithm:

Proposition IV.5. *We use the notations from algorithm IV.5. The algorithm yields a solution iff there exist $t, u \in k(x, y)$ and $\theta_0, \ldots, \theta_{s-1} \in k$ such that*

- $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3} \in k(t)$ *with* $\alpha_0, \alpha_1, \alpha_3 \in k$ *and* $D_x(\alpha_0) = 0$,
- $u^2 = D_t$,
- $k(x, y) = k(t, u)$,
- $f(\theta_0, \ldots, \theta_{s-1}) = 0$ *for each* $f \in C_0$ *and*
- $h(\theta_0, \ldots \theta_{s-1}) \neq 0$ *for each* $h \in C_{\neq 0}$.

Proof. Analogously to proposition IV.4. □

We finish this section by giving an example for algorithm IV.5.

Example IV.4. Let $F = \mathbb{F}_{59^2}(x, y)$, $y^2 = D_x := x^6 + 37x^5 + 13x^4 + 18x^3 + 42x^2 + 55x + 32$. We would like to know, if there is a basis $F = \mathbb{F}_{59^2}(t, u)$ such that $u^2 = D_t := t^5 + 27t^4 + 7t^3 + 14t^2 + 50t + 11$ and $x = \frac{\alpha_0 t+\alpha_1}{t+\alpha_3} \in \mathbb{F}_{59^2}(t)$ with $D_x(\alpha_0) = 0$. Thus, we choose $s := 0$, $C_0 := C_{\neq 0} := \emptyset$.

(1) Factoring D_x yields

$$D_x = (x + 19)(x + 10)(x^2 + 14x + 54)(x^2 + 53x + 34).$$

Hence, we either have $\alpha_0 \in \{-19, -10\} = \{40, 49\}$ or there is no solution at all. We start trying $\alpha_0 = 40$.

(1.1) Substituting $x = \frac{40t+\alpha_1}{t+\alpha_3}$ into D_t, we get

$$\begin{aligned} D_{x,t} =&(t+\alpha_3)^6 \cdot D_x \\ =&(2\alpha_1 + 38\alpha_3)t^5 \\ &+ (57\alpha_1^2 + 52\alpha_1\alpha_3 + 58\alpha_3^2)t^4 \\ &+ (22\alpha_1^3 + 7\alpha_1^2\alpha_3 + \alpha_1\alpha_3^2 + 5\alpha_3^3)t^3 \\ &+ (25\alpha_1^4 + 19\alpha_1^3\alpha_3 + 21\alpha_1^2\alpha_3^2 + 31\alpha_1\alpha_3^3 + 33\alpha_3^4)t^2 \\ &+ (41\alpha_1^5 + 51\alpha_1^4\alpha_3 + 10\alpha_1^3\alpha_3^2 + 27\alpha_1^2\alpha_3^3 + 36\alpha_1\alpha_3^4 + 32\alpha_3^5)t \\ &+ \alpha_1^6 + 37\alpha_1^5\alpha_3 + 13\alpha_1^4\alpha_3^2 + 18\alpha_1^3\alpha_3^3 + 42\alpha_1^2\alpha_3^4 + 55\alpha_1\alpha_3^5 + 32\alpha_3^6 \end{aligned}$$

where α_1 and α_3 are to be found.

(1.2) $\tilde{D}_x(x) = x^5 + 18x^4 + 25x^3 + 15x^2 + 52x + 11$.

(1.3) Comparing coefficients in $(\alpha_1 - 40\alpha_3)\tilde{D}_x(40)D_t = D_{x,t}$, i.e. in

$$2(\alpha_1 - 40\alpha_3)D_t = D_{x,t}$$

yields the equations E_0':

$$\begin{aligned} 0 =&57\alpha_1^2 + 52\alpha_1\alpha_3 + 58\alpha_3^2 - 54\alpha_1 - 23\alpha_3 \\ 0 =&22\alpha_1^3 + 7\alpha_1^2\alpha_3 + \alpha_1\alpha_3^2 + 5\alpha_3^3 - 14\alpha_1 - 30\alpha_3 \\ 0 =&25\alpha_1^4 + 19\alpha_1^3\alpha_3 + 21\alpha_1^2\alpha_3^2 + 31\alpha_1\alpha_3^3 + 33\alpha_3^4 - 28\alpha_1 - \alpha_3 \\ 0 =&41\alpha_1^5 + 51\alpha_1^4\alpha_3 + 10\alpha_1^3\alpha_3^2 + 27\alpha_1^2\alpha_3^3 + 36\alpha_1\alpha_3^4 + 32\alpha_3^5 \\ &- 41\alpha_1 - 12\alpha_3 \\ 0 =&\alpha_1^6 + 37\alpha_1^5\alpha_3 + 13\alpha_1^4\alpha_3^2 + 18\alpha_1^3\alpha_3^3 + 42\alpha_1^2\alpha_3^4 + 55\alpha_1\alpha_3^5 + 32\alpha_3^6 \\ &- 22\alpha_1 - 5\alpha_3 \end{aligned}$$

(1.4) Let $E_0 := E_0'$.

(1.5) Let $E_{\neq 0} := \{40\alpha_3 - \alpha_1\}$.

(1.6) Let $e_{\neq 0} := 1 - (40\alpha_3 - \alpha_1) \cdot z$.

(1.7) Let $E := E_0 \cup \{e_{\neq 0}\}$. We interpret E as an ideal $E\mathbb{F}_{59^2}[\alpha_1, \alpha_3, z]$. Singular ([**GPS⁺02**]) computes the Gröbner basis $\{1\}$ of E. Thus, $E = k[\alpha_1, \alpha_3, z]$, which implies that E has no solutions in $\mathbb{F}_{59^2}$ (or any of its extension fields).

(2) Next we try $\alpha_0 = 49$. Like above, we construct the ideal $E\mathbb{F}_{59^2}[\alpha_1, \alpha_3, z]$ and compute its Gröbner basis with respect to the lexicographical ordering. We obtain the following Gröbner basis.

$$\begin{aligned} 0 =&z + 2 \\ 0 =&\alpha_1 - 18 \\ 0 =&\alpha_3 - 9 \end{aligned}$$

Thus, $\alpha_0 = 49$, $\alpha_1 = 18$, $\alpha_3 = 9$ is a solution of E. We have to find $\beta \in \mathbb{F}_{59^2}$ such that $\beta^2 = (\alpha_1 - \alpha_0\alpha_3)\tilde{D}_x(\alpha_0) = 56$, next. From $56^{(59^2-1)/2} = 1 \in \mathbb{F}_{59^2}$, we know that 56 is a square root. In order to compute it explicitly, we need a basis for $\mathbb{F}_{59^2}/\mathbb{F}_{59}$. If the basis has been chosen in advance, we compute $\beta := 56^{(59^2+1)/4} \in \mathbb{F}_{59}$. Otherwise, we simply choose $\mathbb{F}_{59^2} := \mathbb{F}_{59}(\beta)$, $\beta^2 - 56 = 0$, since 56 is no square modulo 59.

1.2. Constructing Necessary Constant Field Extensions. In section 1.1, we have presented algorithm IV.1, which checks whether a hyperelliptic function field $F = k(x, y)$ has a given defining equation $u^2 = D_t$. Furthermore, this algorithm constructs a basis satisfying $u^2 = D_t$, explicitly. In example IV.3, we have seen that even if F does not have the defining equation $u^2 = D_t$, F may have a constant field extension having this equation. Thus, it is sensible to ask whether a hyperelliptic function field F/k has a constant field extension Fk' having the defining equation $u^2 = D_t$. With slight modifications, algorithm IV.1 can be used to decide this question. Furthermore, the smallest such field extension Fk'/F and a basis $Fk' = k'(x, y) = k'(t, u)$ satisfying $u^2 = D_t$ can be constructed as well. The case, where an explicit construction of k', t and u is not necessary, is discussed in section 1.3.

Algorithm IV.1 is modified in the following way to solve our problem: First of all, solving the set E of polynomials in the sub-algorithms IV.3, IV.4 and IV.5 is done over $\overline{k}$ (instead of over k itself) and the smallest k'/k containing all solutions is constructed. Furthermore, because we allow constant field extensions, factoring D_x and D_t decomposes them into linear factors. Thus, step (1) of algorithm IV.1, which checks the degrees of the factors of D_x and D_t for compatibility, becomes useless and is omitted.

Algorithm IV.6. Check a hyperelliptic function field for a defining equation in a constant field extension, construct extension and basis.

Input: Let $k(x, y)$ be a hyperelliptic function field and $y^2 = D_x$, $D_x \in k[x]$ the corresponding defining equation. Let $s \in \mathbb{N}$, $\theta_0, \ldots, \theta_{s-1}$ be variable symbols and C_0, $C_{\neq 0} \subseteq k[\theta_0, \ldots, \theta_{s-1}]$ finite sets of polynomials. Let $D_t \in k[\theta_0, \ldots, \theta_{s-1}][t]$ be a monic, separable polynomial of degree $\deg_t(D_t) \in \{2\mathrm{g} + 1, 2\mathrm{g} + 2\}$.

Output: This algorithm reports, whether there exist a finite extension k'/k,

$$t, u \in k'(x, y) \quad \text{and} \quad \theta_0, \ldots, \theta_{s-1} \in k'$$

such that

- $u^2 = D_t$,
- $k'(x, y) = k'(t, u)$,
- $f(\theta_0, \ldots, \theta_{s-1}) = 0$ for each $f \in C_0$ and
- $h(\theta_0, \ldots \theta_{s-1}) \neq 0$ for each $h \in C_{\neq 0}$.

If this is the case, the algorithm returns the smallest possible extension field k'/k as well as $\theta_0, \ldots, \theta_{s-1}, \alpha_0, \ldots, \alpha_3 \in k'$ and $\varphi \in k'(t)$ such that setting $x =: \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}$ and $y =: \varphi u$ implies the above conditions.

Steps:

(1) We try to construct k', t, u such that $x \in k'[t]$ using a modified version of algorithm IV.3, where we solve E over $\overline{k}$ and construct the smallest extension field k' containing $\alpha_0, \alpha_1, \theta_0, \ldots, \theta_{s-1}$, as well as φ. If this is possible, we quit returning the constructed parameters.

(2) We try to construct k', t, u such that $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3} \in k'(t)$ and $D_x(\alpha_0) \neq 0$ using a modified version of algorithm IV.4. As in step (1), we solve E over $\overline{k}$ constructing the smallest extension field k'/k containing our solution as well as satisfying $\varphi \in k(t)$. If this is possible, we quit returning the constructed parameters.

(3) We try to construct k', t, u such that $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3} \notin k'(t)$ and $D_x(\alpha_0) = 0$ using a modified version of algorithm IV.5 as in steps (1) and (2). Note that we need to factor D_x over $\overline{k}$, here. If we can find a solution, we quit returning the constructed parameters.

(4) Since we did not quit till now, it is impossible to construct k', t, u. Thus, we report that there exist no k'/k, $t, u \in k'(x, y)$, $\theta_0, \dots, \theta_{s-1} \in k'$ such that the above conditions hold.

The correctness of algorithm IV.6 is obvious from that of algorithm IV.1.

1.3. Checking for Solutions Over the Algebraic Closure. In many cases, it suffices to decide whether a hyperelliptic function field F/k has a constant field extension Fk'/F with a given defining equation $u^2 = D_t$, while explicit formulas for k', t and u are not needed at all. For example if we wish to compute the automorphism group of a hyperelliptic function field over the algebraic closure of its constant field, we are in this situation (cf. chapter V).

The most time consuming part of algorithm IV.1 is finding solutions of the sets E of polynomials in the different cases. On the other hand, knowing whether E is solvable over $\overline{k}$ is all we need, here. This can be checked efficiently for most examples using standard techniques (see remark IV.6). As in algorithm IV.6, the first step of algorithm IV.1 can be omitted because every polynomial decomposes into linear factors over $\overline{k}$. These modifications transform algorithm IV.1 into

Algorithm IV.7. Check a hyperelliptic function field for a defining equation over the algebraic closure of its constant field.

Input: Let $k(x, y)$ be a hyperelliptic function field and $y^2 = D_x$, $D_x \in k[x]$ the corresponding defining equation. Let $s \in \mathbb{N}$, $\theta_0, \dots, \theta_{s-1}$ be variable symbols and C_0, $C_{\neq 0} \subseteq k[\theta_0, \dots, \theta_{s-1}]$ finite sets of polynomials. Let $D_t \in k[\theta_0, \dots, \theta_{s-1}][t]$ be a monic, separable polynomial of degree $\deg_t(D_t) \in \{2\mathrm{g} + 1, 2\mathrm{g} + 2\}$.

Output: This algorithm reports, whether there exist

$$t, u \in \overline{k}(x, y) \quad \text{and} \quad \theta_0, \dots, \theta_{s-1} \in \overline{k}$$

such that

- $u^2 = D_t$,
- $\overline{k}(x, y) = \overline{k}(t, u)$,
- $f(\theta_0, \dots, \theta_{s-1}) = 0$ for each $f \in C_0$ and
- $h(\theta_0, \dots \theta_{s-1}) \neq 0$ for each $h \in C_{\neq 0}$.

Steps:

(1) We check the existence of t, u such that $x \in \overline{k}[t]$ using a modified version of algorithm IV.3: Instead of solving E, we check it for solvability[1] over $\overline{k}$. Checking for $\varphi \in \overline{k}$ can obviously be omitted. If a solution exist, we quit reporting this fact.

(2) We check the existence of t, u such that $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3} \in \overline{k}(t)$ and $D_x(\alpha_0) \neq 0$ using a modification of algorithm IV.4: Instead of solving E, we check it for solvability over $\overline{k}$. Checking for $\varphi \in \overline{k}(t)$ can obviously be omitted. If a solution exist, we quit reporting this fact.

(3) We check the existence of t, u such that $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3} \in \overline{k}(t)$ and $D_x(\alpha_0) = 0$ using a modification of algorithm IV.5: Instead of solving E, we check it for solvability over $\overline{k}$. Note that we need to factor D_x over $\overline{k}$ in step (1) of algorithm IV.5 obtaining d_x candidates for α_0. Checking for $\varphi \in \overline{k}(t)$ can obviously be omitted. If a solution exist, we quit reporting this fact.

(4) Since we did not quit till now, it is impossible to construct t, u. Thus, we report that there exist no $t, u \in \overline{k}(x, y)$, $\theta_0, \dots, \theta_{s-1} \in \overline{k}$ such that the above conditions hold.

[1] see remark IV.6

The correctness of algorithm IV.1 implies that of algorithm IV.7. The following remark explains how to check E for solvability:

Remark IV.6. In algorithm IV.7 we need to find out, if a finite set E of polynomials in $\overline{k}[X_0, \dots, X_{n-1}]$ has a solution over $\overline{k}$. To obtain this information, we interpret E as the ideal $E\overline{k}[X_0, \dots, X_{n-1}] \subseteq \overline{k}[X_0, \dots, X_{n-1}]$ and compute its Gröbner basis with respect to an ordering which promises an efficient Gröbner basis construction. In many cases, the degree reverse lexicographical ordering is a good choice, here. E has a solution iff the resulting basis is different from $\{1\}$.

We apply algorithm IV.7 to the following example.

Example IV.5. Let $F = \mathbb{F}_{809}(x, y)$ with

$$y^2 = D_x := x^6 + 388x^5 + 240x^4 + 708x^3 + 138x^2 + 549x + 501.$$

We would like to know whether $F\overline{\mathbb{F}_{809}}$ has a degree 2 elliptic subfield. Fields of this type are discussed in [**Sha00**]. As explained in the introduction of section II.4, such fields have a defining equation $u^2 = D_t =: t^6 - s_1t^4 + s_2t^2 - 1$ with $27 - 18s_1s_2 - s_1^2s_2^2 + 4s_1^3 + 4s_2^3 \neq 0$. Hence our task is to decide whether $u^2 = D_t$ is a defining equation of $F\overline{\mathbb{F}_{809}}$. Algorithm IV.7 yields the following:

(1) $F\overline{\mathbb{F}_{809}}$ has no basis $F\overline{\mathbb{F}_{809}} = \overline{\mathbb{F}_{809}}(t, u)$ with $u^2 = D_t$ such that $x \in \mathbb{F}_{809}[t]$.

(2) $F\overline{\mathbb{F}_{809}}$ has a basis $F\overline{\mathbb{F}_{809}} = \overline{\mathbb{F}_{809}}(t, u)$ with $u^2 = D_t$ such that
$$x = \frac{\alpha_0 t + \alpha_1}{t + \alpha_3} \in \mathbb{F}_{809}(t), \quad D_x(\alpha_0) \neq 0.$$

(3) $F\overline{\mathbb{F}_{809}}$ has no basis $F\overline{\mathbb{F}_{809}} = \overline{\mathbb{F}_{809}}(t, u)$ with $u^2 = D_t$ such that
$$x = \frac{\alpha_0 t + \alpha_1}{t + \alpha_3} \in \mathbb{F}_{809}(t), \quad D_x(\alpha_0) = 0.$$

Thus, $F\overline{\mathbb{F}_{809}}$ has a degree 2 elliptic subfield.

2. Explicit Determination of Isomorphisms

Let $F = k(x, y)$, $y^2 = D_x$ and $G = k(t, u)$, $u^2 = D_t$ be two hyperelliptic function fields. We wish to determine, whether $F \cong G$ are isomorphic over k. According to propositions III.19 and III.20, we have $F \cong G$ iff $u^2 = D_t$ is a defining equation for F. Thus, we can decide $F \cong G$ using algorithm IV.1:

Algorithm IV.8. Construct an isomorphism between two hyperelliptic function fields.

Input: Let $F = k(x, y)$ and $G = k(T, U)$ be hyperelliptic function fields and $y^2 = D_x$, $D_x \in k[x]$, $U^2 = D_t(T)$, $D_t(T) \in k[T]$ the corresponding defining equations.

Output: This algorithm reports whether $F \cong G$ are k-isomorphic function fields over k. If this is the case, we return an isomorphism, explicitly.

Steps:

(1) Check if $u^2 = D_t(t)$ is a defining equation of F using algorithm IV.1. If this is the case, let $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}$, $y = \varphi(t)u$ be the basis transformation returned by algorithm IV.1.
Otherwise, quit reporting $F \ncong G$.

(2) We report that $F \cong G$ and that a k-isomorphism is given by
$$\Phi : F \to G, \quad x \mapsto \frac{\alpha_0 T + \alpha_1}{\alpha_2 T + \alpha_3}, \quad y \mapsto \varphi(T)U.$$

The inverse isomorphism is given by

$$\Psi : G \to F, \quad T \mapsto t = \frac{\alpha_3 x - \alpha_1}{\alpha_0 - \alpha_2 x}, \quad U \mapsto u = \frac{y}{\varphi(t)} = \frac{y}{\varphi(\frac{\alpha_3 x - \alpha_1}{\alpha_0 - \alpha_2 x})}.$$

Remark IV.7. Algorithm IV.8 can be generalized such that it can also be applied if G is not known completely, i.e. if D_t contains parameters $\theta_0, \ldots, \theta_{s-1}$. Since we will not use this algorithm in the remainder of this work and because the generalization is obvious from algorithm IV.1, the author chose to omit it from algorithm IV.8 for the sake of readability.

Remark IV.8. We can easily generalize algorithm IV.8 to check hyperelliptic function fields over $\overline{k}$ or to construct a minimal constant field extension yielding an isomorphism. To do so, we mainly need to substitute algorithm IV.1 by algorithm IV.6 or IV.7 in step (1).

In order to show the correctness of algorithm IV.8, we need to prove that $\Phi : t \mapsto T$, $u \mapsto U$ and that $\Psi = \Phi^{-1}$.

Proposition IV.9. *We use the notation of algorithm IV.8. If F and G are not k-isomorphic, the algorithm reports this fact. Otherwise, the algorithm constructs k-isomorphisms $\Phi : F \to G$ and $\Psi : G \to F$ such that $\Psi = \Phi^{-1}$.*

Proof. Let $F \ncong G$. By proposition III.19, $u^2 = D_t(t)$ is no defining equation for F. Because algorithm IV.1 is correct, algorithm IV.8 quits reporting that $F \ncong G$.

Let $F \cong G$. By proposition III.20, $u^2 = D_t(t)$ is a defining equation for F. Let $F = k(t, u)$ be the corresponding basis. Because algorithm IV.1 is correct, it returns $\alpha_0, \ldots, \alpha_3 \in k$ and $\varphi(t) \in k(t)$ such that $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}$ and $y = \varphi(t)u$. By proposition III.19, the mapping $t \mapsto T$, $u \mapsto U$ induces a k-isomorphism $\Phi' : F \to G$. We obtain

$$\Phi'(x) = \Phi'(\frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}) = \frac{\alpha_0 \Phi'(t) + \alpha_1}{\alpha_2 \Phi'(t) + \alpha_3} = \frac{\alpha_0 T + \alpha_1}{\alpha_2 T + \alpha_3} = \Phi(x)$$

and

$$\Phi'(y) = \Phi'(\varphi(t) \cdot u) = \varphi(\Phi'(t)) \cdot \Phi'(u) = \varphi(T) \cdot U = \Phi(y).$$

Thus $\Phi = \Phi'$, i.e. $\Phi : F \to G$ is a k-isomorphism as claimed. Hence,

$$\Psi(\Phi(t)) = t, \quad \Psi(\Phi(u)) = u, \quad \Phi(\Psi(T)) = T \quad \text{and} \quad \Phi(\Psi(U)) = U.$$

Thus $\Psi = \Phi^{-1}$ and we only need to verify the equations $t = \frac{\alpha_3 x - \alpha_1}{\alpha_0 - \alpha_2 x}$, $u = \frac{y}{\varphi(\frac{\alpha_3 x - \alpha_1}{\alpha_0 - \alpha_2 x})}$. This, in turn, is proved easily by solving $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}$ and $y = \varphi(t)u$ for t and u. □

Let us study algorithm IV.8 using an example:

Example IV.6. Let $F = \mathbb{F}_{83}(x, y)$ and $G := \mathbb{F}_{83}(T, U)$ with

$$\begin{aligned} y^2 = D_x :=& x^8 + 29x^7 + 73x^6 + 64x^5 + 28x^3 + 5x^2 + 54x + 27, \\ U^2 = D_t(T) :=& T^8 + 54T^7 + 70T^6 + 34T^5 + 48T^4 + 14T^3 + 58T^2 + 40T + 81. \end{aligned}$$

(1) Algorithm IV.1 yields exactly one[2] solution $F = \mathbb{F}_{83}(t, u)$ such that $u^2 = D_t(t)$, namely $x = \frac{14t}{t+48}$, $y = \pm \frac{65}{(t+48)^8} \cdot u$.

[2] i.e. up to the sign of u, which obviously cannot be determined from the quadratic equation $u^2 = D_t(t)$.

(2) A k-isomorphism $F \cong G$ is given by

$$\Phi : F \to G, \quad x \mapsto \frac{14T}{T+48}, \quad y \mapsto \frac{65}{(T+48)^8} \cdot U.$$

The inverse isomorphism is given by

$$\Psi : G \to F, \quad T \mapsto \frac{48x}{14-x}, \quad U \mapsto \frac{y(t+48)^8}{65} = \frac{11y}{65(14-x)^8}.$$

3. Normal Forms

In this section, we give a normal form for hyperelliptic function fields as well as explicit formulas which transform a hyperelliptic function field to normal form. Our notion of a normal form is not be uniquely determined by the field, alone. But if we also choose three ramified places and fix their representation, the resulting normal form becomes unique. Thus, any hyperelliptic function field has at most $8\mathrm{g}^3 + 12\mathrm{g}^2 + 4\mathrm{g}$ normal forms, which is at most 720 for fields of practical relevance.[3] Thus, using normal forms, we can easily check hyperelliptic function fields for isomorphy (see algorithm IV.9): Two hyperelliptic function fields are isomorphic, iff there exists a choice of places such that the resulting normal forms are equal. This check is much more efficient than algorithm IV.8, because we only need to perform substitutions in the defining equations as well as some elementary arithmetics, while algorithm IV.8 needs Gröbner basis methods. On the other hand, this method cannot be generalized in the same way as noted in remark IV.7, i.e. if D_t contains parameters outside of known linear factors, we cannot apply algorithm IV.9.

To define our normal forms, we need to discuss briefly, how many restrictions we can pose on a defining equation. From theorem III.18 we know that defining equations of a hyperelliptic function field can be changed substituting the variable symbol by a fraction of linear polynomials. Thus, the set of defining equations of a hyperelliptic function field over k is—at least, if k is algebraically closed—generated by $\mathrm{PGL}_2(k)$. This gives us the possibility to choose three (linear) conditions for the defining equation. We decide to fix the representation of three places.

Definition IV.1. Let $F = k(x, y)$ be a hyperelliptic function field and $y^2 = D_x$ its defining equation. F is called to be *in normal form*, if $\deg_x(D_x) = 2\mathrm{g} + 1$, $D_x(0) = 0$ and $D_x(-1) = 0$.

In other words, a defining equation in normal form has the property

$$D_x = x \cdot (x+1) \cdot f(x),$$

where $f \in k[x]$ is a polynomial of odd degree.

Let us start showing that each hyperelliptic function field has a normal form if its defining equation can be factored into linear terms and if the constant field contains a specific square root. In particular, each hyperelliptic function field over an algebraically closed function field has a normal form.

Proposition IV.10. *Let $F = k(x, y)$, $y^2 = D_x$ be a hyperelliptic function field such that D_x completely decomposes into linear factors and $D_x = (x+a)(x+b)(x+c) \cdot f(x)$ be a partial factorization of D_x, $a, b, c \in k$. Let*

$$t := \frac{(c-a)x + b(c-a)}{(b-c)x + a(b-c)}, \quad u := \frac{(a-c)^{\mathrm{g}}(b-a)^{\mathrm{g}}}{(c-b)^{\mathrm{g}+1}(x+a)^{\mathrm{g}+1}} \cdot \frac{y}{\gamma},$$

where $\gamma \in k$ such that $\gamma^2 = \frac{f(-a)}{b-c}$. Then $F = k(t, u)$ is in normal form.

[3] As explained in chapter II, only fields of genus ≤ 4 are suitable for cryptographic purposes.

Proof. Solving the definition of t for x, we obtain

$$x = \frac{-a(b-c)t - b(a-c)}{(b-c)t + (a-c)}. \tag{4}$$

The denominator of this fraction can be expressed by x:

$$\begin{aligned}(b-c)t+(a-c) =&(b-c)\frac{(c-a)x+b(c-a)}{(b-c)x+a(b-c)}+(a-c)\\ =&(b-c)\left(\frac{(c-a)x+b(c-a)}{(b-c)(x+a)}+\frac{a-c}{b-c}\right)\\ =&(b-c)\frac{(c-a)x+b(c-a)+(a-c)(x+a)}{(b-c)(x+a)}\\ =&\frac{(c-a)x+b(c-a)+(a-c)x+(a-c)a}{(x+a)}\\ =&\frac{b(c-a)+(a-c)a}{(x+a)}.\end{aligned}$$

Thus, we have

$$(b-c)t+(a-c) = \frac{(a-c)(a-b)}{(x+a)}. \tag{5}$$

In order to show that $k(t,u)$ is in normal form, we compute the relation between t and u:

$$\begin{aligned}u^2 =&\frac{(a-c)^{2\mathrm{g}}(b-a)^{2\mathrm{g}}}{(c-b)^{2\mathrm{g}+2}(x+a)^{2\mathrm{g}+2}}\cdot\frac{y^2}{\gamma^2},\\ =&\frac{(b-c)(a-c)^{2\mathrm{g}}(a-b)^{2\mathrm{g}}}{f(-a)(b-c)^{2\mathrm{g}+2}(x+a)^{2\mathrm{g}+2}}\cdot D_x\\ =&\frac{(b-c)(a-c)^{2\mathrm{g}+1}(a-b)^{2\mathrm{g}+1}}{f(-a)(a-c)(a-b)(b-c)^{2\mathrm{g}+2}(x+a)^{2\mathrm{g}+2}}\cdot D_x\\ \overset{(5)}{=}&\frac{(b-c)\left((b-c)t+a-c\right)^{2\mathrm{g}+1}}{f(-a)(a-c)(a-b)(b-c)^{2\mathrm{g}+2}(x+a)}\cdot(x+a)(x+b)(x+c)\cdot f(x)\\ =&\frac{(b-c)\left((b-c)t+a-c\right)^{2\mathrm{g}+1}}{f(-a)(a-c)(a-b)(b-c)^{2\mathrm{g}+2}}\cdot(x+b)\cdot(x+c)\cdot f(x)\\ =&\frac{-\left((b-c)t+a-c\right)(x+b)}{(a-b)(b-c)}\cdot\frac{-\left((b-c)t+a-c\right)(x+c)}{(a-c)(b-c)}\\ &\cdot\frac{\left((b-c)t+a-c\right)^{2\mathrm{g}-1}f(x)}{f(-a)(b-c)^{2\mathrm{g}-1}}.\end{aligned}$$

We consider these factors separately.

(1) To simplify the first factor, we substitute equation (4) into $x+b$.

$$\begin{aligned}x+b =&\frac{-a(b-c)t-b(a-c)}{(b-c)t+(a-c)}+b\\ =&\frac{-a(b-c)t-b(a-c)+b(b-c)t+b(a-c)}{(b-c)t+(a-c)}\\ =&\frac{-(a-b)(b-c)t}{(b-c)t+(a-c)}.\end{aligned}$$

Hence, the first factor of u^2 is equal to t.

(2) To simplify the second factor, we substitute equation (4) into $x + c$.

$$\begin{aligned}x + c =&\frac{-a(b-c)t - b(a-c)}{(b-c)t + (a-c)} + c\\ =&\frac{-a(b-c)t - b(a-c) + c(b-c)t + c(a-c)}{(b-c)t + (a-c)}\\ =&\frac{-(a-c)(b-c)t - (b-c)(a-c)}{(b-c)t + (a-c)}\\ =&-(a-c)(b-c)\cdot\frac{t+1}{(b-c)t + (a-c)}.\end{aligned}$$

Hence, the second factor of u^2 is equal to $t + 1$.

(3) Finally, we consider the third factor of u^2 above. Let $d := \deg_x(f(x))$ and $\eta_1, \ldots, \eta_d \in k$ the zeroes of f, i.e.

$$f(x) = \prod_{i=1}^{d}(x - \eta_i).$$

Substituting equation (4), we get

$$\begin{aligned}f(x) =&\prod_{i=1}^{d}(\frac{-a(b-c)t - b(a-c)}{(b-c)t + (a-c)} - \eta_i)\\ =&\prod_{i=1}^{d}(\frac{-a(b-c)t - b(a-c) - \eta_i(b-c)t - \eta_i(a-c)}{(b-c)t + (a-c)})\\ =&\prod_{i=1}^{d}(\frac{-(a+\eta_i)(b-c)t - (b+\eta_i)(a-c)}{(b-c)t + (a-c)}).\end{aligned}$$

Thus, the third factor of u^2 equals

$$\begin{aligned}h :=&\frac{((b-c)t + a - c)^{2\mathrm{g}-1} f(x)}{f(-a)(b-c)^{2\mathrm{g}-1}}\\ =&\frac{((b-c)t + a - c)^{2\mathrm{g}-1-d}\cdot\prod_{i=1}^{d}\left(-(a+\eta_i)(b-c)t - (b+\eta_i)(a-c)\right)}{(b-c)^{2\mathrm{g}-1}\cdot\prod_{i=1}^{d}(-a-\eta_i)}\\ =&\frac{((b-c)t + a - c)^{2\mathrm{g}-1-d}\cdot\prod_{i=1}^{d}\left(t - \frac{(b+\eta_i)(a-c)}{-(a+\eta_i)(b-c)}\right)}{(b-c)^{2\mathrm{g}-1-d}}.\end{aligned}$$

We immediately see $h \in k[t]$, $\mathrm{lc}_t(h) = 1$ and $\deg_t(h) = 2\mathrm{g} - 1$.

Summing up, we obtain

$$u^2 = t(t+1)\cdot h(t) =: D_t$$

with $\deg_t(D_t) = 2 + \deg_t(h) = 2\mathrm{g} + 1$. Hence, $k(t, u)$ is in normal form. Note that all the above fractions are defined, since D_x is separable. □

Let us apply proposition IV.10 to an example field.

Example IV.7. Let $F := \mathbb{F}_{139}(x, y)$ be defined by

$$\begin{aligned}y^2 = D_x :=&(x+60)(x+61)(x+75)(x+84)(x+94)(x+95)(x+132)\\ =&x^7 + 45x^6 + 57x^5 + 44x^4 + 5x^3 + 122x^2 + 105x + 95\end{aligned}$$

We choose $a := 60$, $b := 75$, $c := 84$ and define

$$\begin{aligned} t :=& \frac{(c-a)x + b(c-a)}{(b-c)x + a(b-c)} = \frac{24x+132}{130x+16} = \frac{90x+78}{x+60}, \\ u :=& \frac{(a-c)^{\mathrm{g}}(b-a)^{\mathrm{g}}}{(c-b)^{\mathrm{g}+1}(x+a)^{\mathrm{g}+1}} \cdot \frac{y}{\gamma} = \frac{76 \cdot 39}{28(x+60)^4} \cdot \frac{y}{99} = \frac{116}{(x+60)^4} \cdot y. \end{aligned}$$

Solving these for x, y yields

$$\begin{aligned} x =& \frac{8t-66}{-65t+12} = \frac{79t+78}{t+49}, \\ y =& \frac{(x+60)^4}{116} u = \frac{(\frac{79t+78}{t+49}+60)^4}{116} u = \frac{99^4}{116(t+49)^4} u = \frac{83}{(t+49)^4} u \end{aligned}$$

The resulting defining equation is the desired normal form

$$u^2 = \frac{(t+49)^8}{83^2} y^2 = \frac{(t+49)^8}{78} D_x = t^7 + 37t^6 + 66t^5 + 85t^4 + 107t^3 + 82t^2 + 30t.$$

In the previous example the choice of a, b, c was quite arbitrary. Let us choose these parameters differently. We will see that normal forms of hyperelliptic function fields are not uniquely determined. Even permuting a, b, c yields a different normal form in many cases.

Example IV.8. As in example IV.7 we consider $F := \mathbb{F}_{139}(x, y)$, defined by

$$\begin{aligned} y^2 = D_x :=& (x+60)(x+61)(x+75)(x+84)(x+94)(x+95)(x+132) \\ =& x^7 + 45x^6 + 57x^5 + 44x^4 + 5x^3 + 122x^2 + 105x + 95 \end{aligned}$$

This time, we choose $a := 84$, $b := 60$, $c := 75$. According to proposition IV.10, we define

$$\begin{aligned} t :=& \frac{(c-a)x + b(c-a)}{(b-c)x + a(b-c)} = \frac{130x+16}{124x+130} = \frac{84x+36}{x+84} \\ u :=& \frac{(a-c)^{\mathrm{g}}(b-a)^{\mathrm{g}}}{(c-b)^{\mathrm{g}+1}(x+a)^{\mathrm{g}+1}} \cdot \frac{y}{\gamma} = \frac{97}{(x+84)^4} \cdot y. \end{aligned}$$

Solving for x yields

$$x = \frac{9t+16}{124t+9} = \frac{55t+36}{t+55}.$$

The resulting defining equation for $F = \mathbb{F}_{139}(t, u)$ is

$$u^2 = t^7 + 66t^6 + 106t^4 + 95t^3 + 52t^2 + 128t.$$

If we check all possible choices for a, b, c, we obtain 105 pairwise different normal forms. The remaining 105 possibilities imply $\gamma \notin \mathbb{F}_{139}$, i.e. we get no normal form, there.

For a fixed defining equation $y^2 = D_x$, choosing a, b, c is the same as choosing a triplet of ramified places[4] and asserting that these points lie over ∞_t, t and $t+1$, respectively. Although we have seen that normal forms of hyperelliptic function fields are not unique, this choice of places makes them unique. We show this fact in proposition IV.12. The main part of its proof is to establish that three ramified places uniquely determine t, which is the gist of the following proposition.

[4] Or a triplet of Weierstraß points, if the constant field is algebraically closed.

PROPOSITION IV.11. *Let F/k be a hyperelliptic function field and $P_0, P_1, P_2 \in \mathbb{P}_F$. Let $t, x \in F$, such that $k(t) = k(x)$ is rational*[5] *and $[F : k(t)] = 2$. If $P_0 \mid \infty_t$, $P_0 \mid \infty_x$, $P_1 \mid t$, $P_1 \mid x$, $P_2 \mid t + 1$ and $P_2 \mid x + 1$, then $t = x$.*

PROOF. Since each place of $k(t)$ is uniquely determined by a place lying above it, we obtain $\infty_t = \infty_x$, $(t)_0^{k(t)} = (x)_0^{k(t)}$ and $(t + 1)_0^{k(t)} = (x + 1)_0^{k(t)}$.

From $\infty_t = \infty_x$ and $(t)_0^{k(t)} = (x)_0^{k(t)}$, we obtain $(t)^{k(t)} = (x)^{k(t)}$. This implies $(\frac{x}{t})^{k(t)} = 0$, i.e. $\frac{x}{t} \in k$. Let $a := \frac{x}{t} \in k$, i.e. $x = at$.

We denote $p_2 := P_2 \cap k(t) = (t + 1)_0^{k(t)}$. Then, we have $\mathrm{v}_{p_2}(x + 1) = 1$, i.e. $t + 1 \bigm| x + 1$. Because of the degrees we obtain $b(t + 1) = x + 1 = at + 1$ for some $b \in k$. Solving this equation yields $(b - a)t + (b - 1) = 0$. Since t is transcendental over k, we get $b - a = 0$, $b - 1 = 0$. Thus, $b = a = 1$, which yields our claim $x = t$. □

Now, the uniqueness of a normal form—given a triplet of places—is easy to see:

PROPOSITION IV.12. *Let $F = k(t, u)$, $u^2 = D_t$ be a hyperelliptic function field in normal form and $P_0, P_1, P_2 \in \mathbb{P}_F$ the places lying over ∞_t, t and $t + 1$, i.e. $P_0 \mid \infty_t$, $P_1 \mid t$ and $P_2 \mid t + 1$. If $F = k(x, y)$, $y^2 = D_x$ is another basis of F such that $P_0 \mid \infty_x$, $P_1 \mid x$ and $P_2 \mid x + 1$, then $D_x = D_t$.*

PROOF. By proposition IV.11, we have $t = x$. Theorem III.16 implies $u = y$. Thus, $D_x(t) = D_x(x) = y^2 = u^2 = D_t(t)$. □

From proposition I.39, we know that the places lying over divisors of D_t and the infinite place (if D_t has odd degree) are exactly the ramified places of F. Counting the number of possible triplets of ramified places, we obtain the maximal number of normal forms of a hyperelliptic function field.

COROLLARY IV.13. *A hyperelliptic function field has at most $8\mathrm{g}^3 + 12\mathrm{g}^2 + 4\mathrm{g}$ normal forms, if g is its genus.*

PROOF. Let F/k be a hyperelliptic function field. If F has no normal form, our claim trivially holds for F. Let $u^2 = D_t$ be a normal form of F. By propositions I.39 and I.40, each place lying over ∞_t, t or $t + 1$ is ramified and of degree 1. Obviously, these places are pairwise distinct. Thus, proposition IV.12 tells us that each normal form of F is uniquely determined by a triplet of distinct, ramified places of $F/k(t)$. Since $F/k(t)$ has at most $2\mathrm{g} + 2$ ramified places, there are at most $(2\mathrm{g} + 2)(2\mathrm{g} + 1)(2\mathrm{g}) = 8\mathrm{g}^3 + 12\mathrm{g}^2 + 4\mathrm{g}$ triplets of distinct, ramified places, i.e. at most this much normal forms. □

Using normal forms, it is easily possible to check two hyperelliptic function fields over an algebraically closed constant field for isomorphy: We compute a normal form of the first field and check, whether it is equal to any normal form of the second field.

ALGORITHM IV.9. Construct an isomorphism between two hyperelliptic function fields over an algebraically closed constant field.

Input: Let k be algebraically closed and F, G be hyperelliptic function fields over k.

Output: This algorithm reports whether $F \cong G$ are k-isomorphic.

Steps:

[5] Note that $[F : k(x)] = 2 = [F : k(t)]$ and $k(x)$, $k(t)$ rational implies $k(t) = k(x)$ by proposition III.1.

(1) We compute a normal form $u_G^2 = D_{t,G}(t_G)$ of G using proposition IV.10.
(2) If F is in imaginary quadratic representation, we transform F into real quadratic representation according to lemma I.31.
Let $y_F^2 = D_x(x_F)$ be a real quadratic defining equation of F.
(3) Factor D_x into linear factors.
(4) For each possible triplet of linear factors $D_x = (x+a)(x+b)(x+c) \cdot f(x)$, we compute the corresponding normal form $u_F^2 = D_{t,F}(t_F)$ according to proposition IV.10.
If $D_{t,F}(t) = D_{t,G}(t)$, we quit reporting $F \cong G$.
(5) If none of the above triplets yields $D_{t,F} = D_{t,G}$, we quit reporting $F \ncong G$.

Remark IV.14. It is easily possible to extend algorithm IV.9 to return explicit formulas for the constructed isomorphism, too. This can be done analogously to algorithm IV.8.

In contrast to algorithm IV.8, it is not obvious how to generalize algorithm IV.9 such that it allows G to be given by a defining equation containing parameters.

When computing automorphism groups, we need to check hyperelliptic function fields for having defining equations which contain parameters (see chapter V). Thus, algorithm IV.9 cannot be used in our application. Instead, we will use algorithms IV.1, IV.6 or IV.7. Because the computation of automorphism groups is the main issue of this thesis, we will not discuss normal forms in the remaining chapters.

CHAPTER V

Computing the Automorphism Group

In this chapter we propose an efficient method to compute the automorphism group of an arbitrary hyperelliptic function field over an algebraically closed constant field of prime characteristic > 2. The computation over finite constant fields also is possible if efficiency is no issue (cf. remark V.10). Beside theoretical applications, knowing the automorphism group of a hyperelliptic function field also is useful in cryptography, as we have seen in chapter II.

Let us outline our algorithm briefly. It is well known that the automorphism group of a hyperelliptic function field is finite (cf. remark I.52 and proposition V.1). For each finite group, which can occur as subgroup of such an automorphism group, Brandt has given a normal form for the corresponding hyperelliptic function fields and explicit formulas for these automorphisms (theorem V.6, [**Bra88**]). Brandt's theorem reduces the computation of the automorphism group to the question whether a given hyperelliptic function field has a specific defining equation. This can be checked using the algorithms discussed in chapter IV. Brandt's results only apply to function fields over algebraically closed constant fields, but this is no problem for our intended application: As mentioned before, we would like to check hyperelliptic function fields for their subfields because (hyper-)elliptic subfields of hyperelliptic function fields may yield insecure Jacobians[1]. Many order counting methods for—as well as some attacks against—Jacobians use constant field extensions. The automorphism group over the algebraic closure of the constant field can be used to avoid Jacobians which become insecure over extension fields. Hence, considering automorphisms over the algebraic closure is even more sensible than working over the given constant field.

If the constant field k is algebraically closed and $\mathrm{char}(k) > 2$, algorithm V.4 is the only efficient possibility known to compute the automorphism group of an arbitrary hyperelliptic function field. For finite k of odd characteristic, Michael Stoll implemented an algorithm to compute the automorphism group ([**Sto00**]). We will discuss his approach in section 5. If $\mathrm{Aut}(F/k) = \mathrm{Aut}(F\overline{k}/\overline{k})$, algorithm V.4 is an alternative to Stoll's algorithm.

Our algorithm is not intended for the case $\mathrm{char}(k) = 0$. Here, the automorphism group can be computed using a technique invented by Tony Shaska ([**Sha03**]), who transforms the curve into a normal form yielding so called dihedral invariants. These invariants give information on the reduced automorphisms.

This chapter is structured as follows: In section 1, we discuss some basic issues concerning automorphism groups. The major part of section 2 is the statement of Brandt's theorem, which we use in section 3 to check for subgroups of the automorphism group. The resulting algorithms are combined to compute the automorphism group itself (section 4). We conclude this chapter by a brief description of Stoll's algorithm in section 5.

[1] Cf. theorem II.1.

1. Elementary Facts on Automorphism Groups

In section I.5 we defined the automorphism group $\mathrm{Aut}(F/k)$ of a general algebraic function field F/k to be the set of field automorphisms of F fixing k. We have seen that all finite separable subfields of hyperelliptic function fields are generated by subgroups of automorphism groups (theorem I.25). In section II.4 we recognized that such subfields may cause insecure Jacobians. Because of these facts it is sensible to have algorithms at hand which compute the automorphism group of a hyperelliptic function field.

We would like to compute the automorphism group by identifying its finite subgroups. This strategy yields the whole automorphism group, because the latter is finite, as we have seen in section I.7. To get a feeling for the orders of automorphism groups of hyperelliptic function fields, we give an upper bound, which was proved by Peter Roquette.

Proposition V.1. *Let k be an algebraically closed field and F/k a hyperelliptic function field such that $\mathrm{char}(k) = 0$ or $p := \mathrm{char}(k) > \mathrm{g} + 1$ and the defining equation of F is distinct from $u^2 = t^p - t$. Then*

$$|\mathrm{Aut}(F/k)| \leq 84(\mathrm{g} - 1)$$

In the excluded case $F = k(t, u)$, $u^2 = t^p - t$, we have $|\mathrm{Aut}(F/k)| = 2p(p^2 - 1)$.

Proof. [**Roq70**, Satz 1]. □

It is easy to see that this proposition also holds if k is not algebraically closed.

Corollary V.2. *Let F/k be a hyperelliptic function field such that $\mathrm{char}(k) = 0$ or $p := \mathrm{char}(k) > \mathrm{g} + 1$ and the defining equation of F is distinct from $u^2 = t^p - t$. Then*

$$|\mathrm{Aut}(F/k)| \leq 84(\mathrm{g} - 1)$$

In the excluded case $F = k(t, u)$, $u^2 = t^p - t$, we have $|\mathrm{Aut}(F/k)| \leq 2p(p^2 - 1)$.

Proof. Let $u^2 = D_t$ be a defining equation of F/k. Then each automorphism φ of F/k is uniquely determined by the mapping $t \mapsto \varphi(t)$, $u \mapsto \varphi(u)$. Since the same holds for $F\overline{k}/\overline{k}$, each automorphism of F/k can be extended to an automorphism of $F\overline{k}/\overline{k}$. Thus, extending automorphisms is an embedding, i.e. $\mathrm{Aut}(F/k) \leq \mathrm{Aut}(F\overline{k}/\overline{k})$. Proposition V.1 yields our claim. □

A natural question is how automorphisms of a hyperelliptic function field look like. Fortunately, this can be answered quite easily using theorem III.16.

Proposition V.3. *Let $F = k(t, u)$, $u^2 = D(t)$ be a hyperelliptic function field. Then $\mathrm{Aut}(F/k)$ is the set of field homomorphisms $\psi : F \to F$ fixing k, which are given by mappings*

$$\psi : t \mapsto \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3},\ u \mapsto \varphi u \ \text{ such that } \psi(u)^2 = D(\psi(t)),$$

where $\alpha_i \in k$, $\alpha_0\alpha_3 - \alpha_1\alpha_2 \neq 0$ and φ is given as in theorem III.16.

Proof. Let $\psi \in \mathrm{Aut}(F/k)$. Proposition III.20 implies that $\psi(u)^2 = D(\psi(t))$ and $F = k(\psi(t), \psi(u))$. Thus, we can apply theorem III.16, which yields the existence of the $\alpha_i \in k$ and $\varphi \in k(t)$ such that $\psi(t) = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$, $\psi(u) = \varphi u$ and $\alpha_0\alpha_3 - \alpha_1\alpha_2 \neq 0$.

Let $\psi : F \to F$ be the field homomorphism given by $t \mapsto \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$, $u \mapsto \varphi u$ with $\psi(u)^2 = D(\psi(t))$. Let $G := k(\psi(t), \psi(u)) \subseteq F$. From proposition III.19 we obtain that $\psi : F \to G$ is a k-isomorphism, which obviously implies $\psi \in \mathrm{Aut}(F/k)$. □

Let us consider the structure of the automorphism group, next. Each hyperelliptic function field $F = k(t, u)$, $u^2 = D_t$ has at least one automorphism Φ, which is defined by $t \mapsto t$, $u \mapsto -u$. We call this automorphism the *hyperelliptic involution* of F. The next proposition shows that this definition makes sense, i.e. that the hyperelliptic involution of F is a uniquely determined involution. As it is obvious that the hyperelliptic involution is an automorphism, we do not prove this fact.

PROPOSITION V.4. *Let $F = k(t, u) = k(x, y)$, $u^2 = D_t$, $y^2 = D_x$ be a hyperelliptic function field. Let $\phi, \psi \in \mathrm{Aut}(F/k)$ be defined by*

$$\phi : t \mapsto t,\ u \mapsto -u,$$
$$\psi : x \mapsto x,\ y \mapsto -y.$$

Then $\phi = \psi$ is an involution, i.e. $\phi^2 = \mathrm{id}_F$.

PROOF. By theorem III.16, we know $x = \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$ and $y = \varphi(t)u$ with $\alpha_i \in k$, $\varphi(t) \in k(t)$. This implies

$$\begin{aligned}\phi(x) =&\phi\left(\frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}\right) = \frac{\alpha_0\phi(t) + \alpha_1}{\alpha_2\phi(t) + \alpha_3} = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3} = x \quad \text{and}\\ \phi(y) =&\phi(\varphi(t)u) = \phi(\varphi(t))\phi(u) = -\varphi(\phi(t))u = -\varphi(t)u = -y.\end{aligned}$$

Thus $\phi = \psi$. From $\phi^2(t) = \phi(t) = t$ and $\phi^2(u) = \phi(-u) = u$, we get $\phi^2 = \mathrm{id}_F$. □

The fixed field F^Φ of the hyperelliptic involution is the rational subfield of F of degree 2, which is uniquely determined according to proposition III.1. By Galois theory, we know that $\mathrm{Aut}(F/k)$ is a central extension[2] of $\langle\Phi\rangle \cong \mathcal{C}_2$ by $\mathrm{Aut}(F^\Phi/k)$. Thus, if we know all (finite) subgroups of $\mathrm{Aut}(F^\Phi/k)$ together with their generators, we also know $\mathrm{Aut}(F/k)$. A hyperelliptic function field F/k is called of type $\mathrm{F}[G, k]$, if $\mathrm{Aut}(F^\Phi/k)$ contains G as a subgroup, as we see in the following definition.

DEFINITION V.1. Let F/k be a hyperelliptic function field, Φ its hyperelliptic involution and G a finite group. F is called a function field *of type* $\mathrm{F}[G, k]$, if there is a finite group U, such that $U \le \mathrm{Aut}(F/k)$, $\langle\Phi\rangle \trianglelefteq U$ and $U/\langle\Phi\rangle \cong G$. The elements of $U/\langle\Phi\rangle$ are called *reduced automorphisms*.

We denote such a group U by $\mathrm{U}(G)$ or $\mathrm{U}_F(G)$, although U needs not to be uniquely determined by F, G and k. We will only use this notation to state that a specific group can be used as U in this definition.

For field extensions $k' \supseteq k$, we call F to be of type $\mathrm{F}[G, k']$ iff the constant field extension Fk'/k' is of type $\mathrm{F}[G, k']$.

For the reader's convenience, we recall the notation of the groups G which can occur in field types or as subgroups $\mathrm{U}(G)$ of automorphism groups (the stated definitions and results are taken from [**Bra88**], [**Hum96**] and [**Kun94**]):

REMARK V.5. Let $m, n, p \in \mathbb{N}_+$, $n > 1$, p an odd prime, $q := p^m$ and G, H finite groups. We will consider the following finite groups:

$\mathcal{C}_n$:	The *cyclic group* of n elements.
$\mathcal{D}_n$:	The *dihedral group* of order $2n$.
$\mathcal{A}_n$:	The *alternating group*, i.e. the group of even permutations of n elements. Its order is $\frac{1}{2}n!$.
$\mathcal{S}_n$:	The *symmetric group*, i.e. the group of permutations of n elements. Its order is $n!$.

[2] I.e. we have $\langle\Phi\rangle \trianglelefteq \mathrm{Aut}(F/k)$, $\mathrm{Aut}(F/k)/\langle\Phi\rangle \cong \mathrm{Aut}(F^\Phi/k)$ and $\langle\Phi\rangle$ is a subgroup of the centralizer $\{\sigma \in \mathrm{Aut}(F/k) \mid \sigma\tau = \tau\sigma\ \forall\tau \in \mathrm{Aut}(F/k)\}$ of F's automorphism group.

$G \rtimes H$: A *semidirect product* of G with H. Thus, $G \rtimes H$ is the set $G \times H$ with a group law given by $(g_1, h_1) \cdot (g_2, h_2) := (g_1 \cdot \varphi(h_1)(g_2), h_1 \cdot h_2)$, where $\varphi : H \to \mathrm{Aut}(G)$ is a fixed group homomorphism. The order of $G \rtimes H$ is $|G| \cdot |H|$.

$\mathrm{PSL}_n(q)$: The *projective special linear group*, i.e.

$$\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/\{\lambda \cdot I_n \mid \lambda \in \mathbb{F}_q\},$$

where $\mathrm{SL}_n(q)$ is the *special linear group* consisting of invertible $n \times n$-matrices of determinant 1 over $\mathbb{F}_q$ and I_n is the identity matrix. The order of $\mathrm{PSL}_n(q)$ is

$$\frac{1}{(q-1) \cdot (n, q-1)} \cdot \prod_{\nu=0,\ldots,n-1} (q^n - q^\nu),$$

in particular, $|\mathrm{PSL}_2(q)| = \frac{1}{2} \cdot (q^3 - q)$.

$\mathrm{PGL}_n(q)$: The *projective general linear group*, i.e.

$$\mathrm{PGL}_n(q) = \mathrm{GL}_n(q)/\{\lambda \cdot I_n \mid \lambda \in \mathbb{F}_q\},$$

where $\mathrm{GL}_n(q)$ is the *general linear group* consisting of invertible $n \times n$-matrices over $\mathbb{F}_q$ and I_n is the identity matrix. The order of $\mathrm{PGL}_n(q)$ is

$$\frac{1}{q-1} \cdot \prod_{\nu=0,\ldots,n-1} (q^n - q^\nu),$$

in particular, $|\mathrm{PGL}_2(q)| = q^3 - q$.

2. Automorphism Groups and Associated Normal Forms

Our aim is to compute the automorphism group of any given hyperelliptic function field $k(x, y)$, $y^2 = D$. As mentioned above, Brandt gives normal forms for each type of hyperelliptic function fields:

THEOREM V.6 (Brandt). *Let F be a hyperelliptic function field over an algebraically closed constant field k of prime characteristic $p \geq 3$. Then the types of F are characterized as follows*

(1) *F is of type $\mathrm{F}[\mathcal{C}_n, k]$ for $n \in \mathbb{N}_+$ with $(n, p) = 1$ iff there are $t, u \in F$, such that $F = k(t, u)$,*

$$u^2 = t^\nu \prod_{j=0}^{s-1} (t^n - a_j),$$

where $\nu \in \{0, 1\}$, $s \in \mathbb{N}_+$ and the $a_j \in k^*$ are pairwise distinct.
In this case, $\mathrm{U}_F(\mathcal{C}_n)$ is generated by Φ and $\psi : t \mapsto \eta^2 t$, $u \mapsto \eta^\nu u$, where η is a primitive $2n$-th root of unity.

(2) *F is of type $\mathrm{F}[\mathcal{C}_p^m, k]$ with $m \in \mathbb{N}_+$ iff there are $t, u \in F$ and a subgroup A of the additive group of k with order $|A| = p^m$, such that $F = k(t, u)$,*

$$u^2 = \prod_{j=0}^{s-1} \left(\prod_{a \in A} (t + a) - a_j \right),$$

where $s \in \mathbb{N}_+$ and the $a_j \in k$ are pairwise distinct.
In this case, $\mathrm{U}_F(\mathcal{C}_p^m)$ is generated by Φ and all $\psi_a : t \mapsto t + a$, $u \mapsto u$ with $a \in A$.

(3) *F is of type* $\mathrm{F}[\mathcal{D}_n, k]$, *where* $n \in \mathbb{N}_+$, $(n, p) = 1$ *iff there are* $t, u \in F$, *such that* $F = k(t, u)$,

$$u^2 = t^{\nu_0}(t^n - 1)^{\nu_1}(t^n + 1)^{\nu_2} \prod_{j=0}^{s-1}(t^{2n} - a_j t^n + 1),$$

where $\nu_j \in \{0, 1\}$, $s \in \mathbb{N}$ *and the* $a_j \in k \setminus \{\pm 2\}$ *are pairwise distinct. If* $n = 2$ *or* $n \equiv 1 \mod 2$, *we need to have* $\nu_1 = \nu_2$.
In this case, $\mathrm{U}_F(\mathcal{D}_n)$ *is generated by* Φ, $\psi : t \mapsto \eta^2 t$, $u \mapsto \eta^{\nu_0} u$ *and* $\sigma : t \mapsto \frac{1}{t}$, $u \mapsto \frac{i^{\nu_1} u}{t^m}$, *where* η *is a primitive* $2n$*-th root of unity,* $i^2 = -1$ *and* $m = \frac{1}{2} \cdot n(\nu_1 + \nu_2) + 2\nu_0 + 2ns$.

(4) *F is of type* $\mathrm{F}[\mathcal{D}_p, k]$ *iff there are* $t, u \in F$, *such that* $F = k(t, u)$,

$$u^2 = (t^p - t)^{\nu} \prod_{j=0}^{s-1}((t^p - t)^2 - a_j),$$

where $\nu \in \{0, 1\}$, $s \in \mathbb{N}$ *and the* $a_j \in k^*$ *are pairwise distinct.*
In this case, $\mathrm{U}_F(\mathcal{D}_p)$ *is generated by* $\psi : t \mapsto t + 1$, $u \mapsto -u$, $\sigma : t \mapsto -t$, $u \mapsto i^{\nu} u$, *where* $i^2 = -1$.
It is easy to see that the hyperelliptic involution Φ *also is an element of* $\mathrm{U}_F(\mathcal{D}_p)$.

(5) *Let* $p = 3$. *Then F is of type* $\mathrm{F}[\mathcal{A}_4, k]$ *iff there are* $t, u \in F$, *such that* $F = k(t, u)$,

$$u^2 = (t^3 - t)^{\nu_0}(t^6 + t^4 + t^2 + 1)^{\nu_1} \prod_{j=0}^{s-1} \left((t^6 + t^4 + t^2 + 1)^2 - a_j (t^3 - t)^3\right),$$

where $\nu_j \in \{0, 1\}$, $s \in \mathbb{N}$ *and the* $a_j \in k^*$ *are pairwise distinct.*
In this case, $\mathrm{U}_F(\mathcal{A}_4)$ *is generated by* Φ, $\psi : t \mapsto t + 1$, $u \mapsto u$ *and* $\sigma : t \mapsto \frac{1}{t}$, $u \mapsto \frac{u}{t^m}$, *where* $m = 2\nu_0 + 3\nu_1 + 6s$.

(6) *Let* $p > 3$. *Then F is of type* $\mathrm{F}[\mathcal{A}_4, k]$ *iff there are* $t, u \in F$, *such that* $F = k(t, u)$,

$$u^2 = (t^5 - t)^{\nu_0}(t^4 - 2i\sqrt{3} \cdot t^2 + 1)^{\nu_1}$$
$$(t^4 + 2i\sqrt{3} \cdot t^2 + 1)^{\nu_2} \prod_{j=0}^{s-1} \left(\prod_{l=0}^{2} (t^4 - a_{j,l} t^2 + 1) \right),$$

where $\nu_j \in \{0, 1\}$, $i^2 = -1$, $s \in \mathbb{N}$, $a_{j,l} \in k \setminus \{\pm 2, \pm 2i\sqrt{3}\}$ *are pairwise distinct,* $a_{j,1} = \frac{2a_{j,0} + 12}{2 - a_{j,0}}$ *and* $a_{j,2} = \frac{2a_{j,0} - 12}{2 + a_{j,0}}$.
In this case, $\mathrm{U}_F(\mathcal{A}_4)$ *is generated by* Φ, $\psi : t \mapsto -t$, $u \mapsto i^{\nu_0} u$ *and* $\sigma : t \mapsto i \cdot \frac{t+1}{t-1}$, $u \mapsto \frac{\xi u}{(t-1)^m}$, *where*

$$\xi^2 = (8i)^{\nu_0}(2 + 2i\sqrt{3})^{\nu_1}(2 - 2i\sqrt{3})^{\nu_2} \prod_{j=0}^{s-1} \left(\prod_{l=0}^{2} (2 + a_{j,l}) \right)$$

and $m = 3\nu_0 + 2(\nu_1 + \nu_2) + 6s$.
If $\nu_0 = 1$, *we can omit* Φ *from our set of generators, because* $\psi^2 = \Phi$.

(7) *Let* $p = 3$. *F is of type* $\mathrm{F}[\mathcal{S}_4, k]$ *iff there are* $t, u \in F$, *such that* $F = k(t, u)$,

$$u^2 = (t^3 - t)^{\nu_0}(t^6 + t^4 + t^2 + 1)^{\nu_1} \prod_{j=0}^{s-1} \left((t^6 + t^4 + t^2 + 1)^4 - a_j (t^3 - t)^6\right),$$

where $\nu_j \in \{0, 1\}$, $s \in \mathbb{N}$ *and the* $a_j \in k^*$ *are pairwise distinct.*

In this case, $\mathrm{U}_F(\mathcal{S}_4)$ *is generated by* Φ, $\psi : t \mapsto -t$, $u \mapsto i^{\nu_0}u$, $\sigma : t \mapsto t+1$, $u \mapsto u$ *and* $\tau : t \mapsto \frac{1}{t}$, $u \mapsto \frac{i^{\nu_0}u}{t^m}$, *where* $i^2 = -1$ *and* $m = 2\nu_0 + 3\nu_1 + 12s$.

(8) *Let* $p > 3$. *Then* F *is of type* $\mathrm{F}[\mathcal{S}_4, k]$ *iff there are* $t, u \in F$, *such that* $F = k(t,u)$,

$$u^2 = (t^5-t)^{\nu_0}(t^8+14t^4+1)^{\nu_1} \left((t^4+1)(t^8-34t^4+1)\right)^{\nu_2} \prod_{j=0}^{s-1}\left((t^8+14t^4+1)^3 - a_j(t^5-t)^4\right),$$

where $\nu_j \in \{0,1\}$, $s \in \mathbb{N}$ *and the* $a_j \in k \setminus \{0, 108\}$ *are pairwise distinct.*

In this case, $\mathrm{U}_F(\mathcal{S}_4)$ *is generated by* Φ, $\psi : t \mapsto it$, $u \mapsto \eta^{\nu_0}u$ *and* $\sigma : t \mapsto i \cdot \frac{t+1}{t-1}$, $u \mapsto \frac{\xi u}{(t-1)^m}$, *where* $i^2 = -1$, η *is a primitive* 8*-th root of unity with* $\eta^2 = i$,

$$\xi^2 = (8i)^{\nu_0}(16)^{\nu_1}(-64)^{\nu_2}(64)^{2s}$$

and $m = 3\nu_0 + 4\nu_1 + 6\nu_2 + 12s$.

(9) *Let* $p = 3$. *Then* F *is of type* $\mathrm{F}[\mathcal{A}_5, k]$ *iff there are* $t, u \in F$, *such that* $F = k(t,u)$,

$$u^2 = \left(t(t^{10}+2it^5+1)\right)^{\nu_0}\left(t^{10}-1\right)^{\nu_1} \prod_{j=0}^{s-1}\left((t^{10}-1)^6 - a_j\left(t(t^{10}+2it^5+1)\right)^5\right),$$

where $i^2 = -1$, $\nu_j \in \{0,1\}$, $s \in \mathbb{N}$ *and the* $a_j \in k^*$ *are pairwise distinct.*

In this case, $\mathrm{U}_F(\mathcal{A}_5)$ *is generated by* Φ, $\psi : t \mapsto \eta^2 t$, $u \mapsto \eta^{\nu_0}u$ *and* $\sigma : t \mapsto \frac{-t-\lambda}{\lambda t+1}$, $u \mapsto \frac{\xi u}{(\lambda t+1)^m}$, *where* η *is a primitive* 10*-th root of unity,* $\lambda = -i(\eta^2+\eta^8)$, $\xi^2 = (-\lambda^2)^{\nu_0}(1-\lambda^2)^{\nu_1}(-\lambda^2)^s$ *and* $m = 6\nu_0 + 5\nu_1 + 30s$.

(10) *Let* $p = 5$. *Then* F *is of type* $\mathrm{F}[\mathcal{A}_5, k]$ *iff there are* $t, u \in F$, *such that* $F = k(t,u)$,

$$u^2 = (t^5-t)^{\nu_0}\left((t^5-t)^4+1\right)^{\nu_1}\prod_{j=0}^{s-1}\left(\left((t^5-t)^4+1\right)^3 - a_j(t^5-t)^{10}\right),$$

where $\nu_j \in \{0,1\}$, $s \in \mathbb{N}$ *and the* $a_j \in k^*$ *are pairwise distinct.*

In this case, $\mathrm{U}_F(\mathcal{A}_5)$ *is generated by* Φ, $\psi : t \mapsto -t$, $u \mapsto i^{\nu_0}u$, $\sigma : t \mapsto -\frac{1}{t}$, $u \mapsto \frac{u}{t^m}$ *and* $\tau : t \mapsto t+1$, $u \mapsto u$, *where* $i^2 = -1$ *and* $m = 3\nu_0 + 10\nu_1 + 30s$.

(11) *Let* $p > 5$. *Then* F *is of type* $\mathrm{F}[\mathcal{A}_5, k]$ *iff there are* $t, u \in F$, *such that* $F = k(t,u)$,

$$u^2 = \left(t^{30} + 522i(t^{25}-t^5) + 10005i(t^{20}-t^{10}) - 1\right)^{\nu_0} \left(t^{20} - 228i(t^{15}+t^5) - 494t^{10} + 1\right)^{\nu_1}\left(t^{11}+11it^6+t\right)^{\nu_2} \prod_{j=0}^{s-1}\left(\left(t^{20} - 228i(t^{15}+t^5) - 494t^{10}+1\right)^3 - a_j\left(t^{11}+11it^6+t\right)^5\right),$$

where $i^2 = -1$, $\nu_j \in \{0,1\}$, $s \in \mathbb{N}$ *and the* $a_j \in k \setminus \{0, -1728i\}$ *are pairwise distinct.*

In this case, there exists[3] *some* $\xi \in k^*$ *such that* $\mathrm{U}_F(\mathcal{A}_5)$ *is generated by* Φ, $\psi : t \mapsto \eta t$, $u \mapsto u$ *and* $\sigma : t \mapsto -\frac{t+\lambda}{\lambda t+1}$, $u \mapsto \frac{\xi u}{(\lambda t+1)^m}$, *where* η *is a primitive* 5*-th root of unity,* $\lambda = -i(\eta+\eta^4)$ *and* $m = 15\nu_0 + 10\nu_1 + 6\nu_2 + 30s$.

[3] Using proposition V.3, it is possible to compute ξ explicitly. We omit a general formula for ξ because of its complexity.

(12) *Let $m, n \in \mathbb{N}_+$, $n > 1$ and $n \mid p^m - 1$. Then F is of type $\mathrm{F}[\mathcal{C}_p^m \rtimes \mathcal{C}_n, k]$, iff there are $t, u \in F$, such that $F = k(t,u)$,*

$$u^2 = \left(t \prod_{l=0}^{r-1} (t^n - b_l) \right)^{\nu} \cdot \prod_{j=0}^{s-1} \left(\left(t \prod_{l=0}^{r-1} (t^n - b_l) \right)^{n} - a_j \right),$$

where $\nu \in \{0,1\}$, $r = \frac{p^m - 1}{n}$, the $a_j \in k^*$ are pairwise distinct and $b_l \in k^*$ such that $\mathcal{U} := \{a \in k \mid a \prod_{l=0}^{r-1} (a^n - b_l) = 0\} \leq (k,+)$.
In this case, $\mathrm{U}_F(\mathcal{C}_p^m \rtimes \mathcal{C}_n)$ is generated by Φ, $\psi : t \mapsto \eta^2 t$, $u \mapsto \eta^{\nu} u$ and $\sigma_a : t \mapsto t + a$, $u \mapsto u$ for each $a \in \mathcal{U}$, where η is a primitive $2n$-th root of unity.

(13) *F is of type $\mathrm{F}[\mathrm{PSL}_2(p^m), k]$, where $m \in \mathbb{N}_+$ iff there are $t, u \in F$, such that $F = k(t,u)$,*

$$u^2 = (t^r - t)^{\nu_0} \left((t^r - t)^{r-1} + 1 \right)^{\nu_1} \prod_{j=0}^{s-1} \left(\left((t^r - t)^{r-1} + 1 \right)^{\frac{r+1}{2}} - a_j (t^r - t)^{\frac{r^2 - r}{2}} \right),$$

where $\nu_j \in \{0,1\}$, $s \in \mathbb{N}$, $r = p^m$ and the $a_j \in k^*$ are pairwise distinct.
In this case, $\mathrm{U}_F(\mathrm{PSL}_2(p^m))$ is generated by Φ, $\psi : t \mapsto \eta^2 t$, $u \mapsto \eta^{\nu_0} u$, $\sigma : t \mapsto t + 1$, $u \mapsto u$ and $\tau : t \mapsto -\frac{1}{t}$, $u \mapsto \frac{u}{t^n}$, where η is a primitive $(p^m - 1)$-th root of unity and

$$n = \frac{1}{2} \left(\nu_0 (p^m + 1) + \nu_1 p^m (p^m - 1) + \frac{1}{2} p^m (p^{2m} - 1) s \right).$$

(14) *F is of type $\mathrm{F}[\mathrm{PGL}_2(p^m), k]$ iff there are $t, u \in F$, such that $F = k(t,u)$,*

$$u^2 = (t^r - t)^{\nu_0} \left((t^r - t)^{r-1} + 1 \right)^{\nu_1} \prod_{j=0}^{s-1} \left(\left((t^r - t)^{r-1} + 1 \right)^{r+1} - a_j (t^r - t)^{r^2 - r} \right),$$

where $\nu_j \in \{0,1\}$, $s \in \mathbb{N}$, $r = p^m$ and the $a_j \in k^*$ are pairwise distinct.
In this case, $\mathrm{U}_F(\mathrm{PGL}_2(p^m))$ is generated by Φ, $\psi : t \mapsto \eta^2 t$, $u \mapsto \eta^{\nu_0} u$, $\sigma : t \mapsto t + 1$, $u \mapsto u$ and $\tau : t \mapsto \frac{1}{t}$, $u \mapsto \frac{i^{\nu_0} u}{t^n}$, where $i^2 = -1$, η is a primitive $2(p^m - 1)$-th root of unity and

$$n = \frac{1}{2} \left((p^m + 1)\nu_0 + p^m (p^m - 1) \nu_1 + p^m (p^{2m} - 1) s \right).$$

Proof. A slightly more general theorem was proved by Rolf Brandt in his PhD. thesis: The types of cyclic extensions of rational function fields over algebraically closed constant fields are characterized in [**Bra88**]. We list the references for each of the stated facts, citing the proof that a function field of the given type has the given normal form, first. Then, the proof of the inverse implication and the generators are given.

(1) [**Bra88**, Satz 5.1], [**Bra88**, Satz 5.6] and [**Bra88**, Lemma 5.5].
(2) [**Bra88**, Satz 6.3] and its proof.
(3) If n is even: [**Bra88**, Satz 7.3], [**Bra88**, Satz 7.5] and [**Bra88**, Lemma 7.4]. If n is odd, we apply [**Bra88**, Satz 7.9], as $p \geq 3$ and $(n,p) = 1$ obviously imply $(2n, p) = 1$. The generators and the inverse implication are proved analogously to [**Bra88**, Satz 7.5] and [**Bra88**, Lemma 7.4].
(4) [**Bra88**, Satz 7.14], [**Bra88**, Satz 7.16] and [**Bra88**, Satz 7.15]. Let us consider Φ: As $\mathrm{char}(k) = p$, we have $\psi^p(t) = t + p = t$. Furthermore, $\psi^p(u) = (-1)^p u = -u$ since p is odd. Thus $\Phi = \psi^p \in \langle \psi, \sigma \rangle = \mathrm{U}_F(\mathcal{D}_p)$.

(5) [**Bra88**, Satz 8.1], [**Bra88**, Satz 8.5] and [**Bra88**, Lemma 8.3].
(6) [**Bra88**, Satz 8.6], [**Bra88**, Satz 8.10] and [**Bra88**, Lemma 8.9].
(7) [**Bra88**, Satz 9.2], [**Bra88**, Satz 9.5] and [**Bra88**, Lemma 9.4].
(8) [**Bra88**, Satz 9.8], [**Bra88**, Satz 9.10] and [**Bra88**, Lemma 9.9].
(9) [**Bra88**, Satz 10.3], [**Bra88**, Satz 10.5] and [**Bra88**, Lemma 10.4].
(10) [**Bra88**, Satz 10.8], [**Bra88**, Satz 10.10] and [**Bra88**, Lemma 10.9].
(11) [**Bra88**, Satz 10.13], [**Bra88**, Satz 10.15] and [**Bra88**, Lemma 10.14].
(12) [**Bra88**, Satz 11.2 and Satz 11.6], [**Bra88**, Satz 11.5 and Bemerkung 11.9] and [**Bra88**, Lemma 11.4].
(13) [**Bra88**, Satz 12.1], [**Bra88**, remark below Satz 12.5], [**Bra88**, Lemma 12.2].
(14) [**Bra88**, Satz 13.1], [**Bra88**, Satz 13.6]. The automorphisms are given in [**Bra88**, Lemma 13.2]. Unfortunately, this lemma contains a typo: τ needs to map u to $\frac{i^{\nu_0}u}{t^n}$ instead of $\frac{u}{t^n}$. This is an easy consequence of $\tau(t) = \frac{1}{t}$ (which is also given in [**Bra88**, Satz 2.3, case 9] and its proof), the defining equation and proposition V.3.

□

In order to be able to check a given hyperelliptic function field for its types using the algorithms described in chapter IV, we need to translate all conditions on parameters, which are given in theorem V.6, into polynomial equations and inequalities for these parameters.

This task is easy for most of the given cases. Nevertheless, the types $\mathcal{C}_p^m$ and $\mathcal{C}_p^m \rtimes \mathcal{C}_n$ pose problems, because of the subgroups of $(k,+)$ we need to have. We start describing the finite subgroups of $(k,+)$. To do so, we note that such groups are elementary abelian p-groups:

Lemma V.7. *Let k be a field of prime characteristic p, $m \in \mathbb{N}_+$ and $A \subseteq k$ such that $|A| = p^m$. Then A is a subgroup of the additive group of k iff $(A,+) \cong \mathcal{C}_p^m$ is the product of m cyclic groups of order p.*

Proof. Let $A \leq (k,+)$. Because $\mathrm{char}(k) = p$, the order of each element $0 \neq a \in A$ is p. [**Hum96**, proposition 14.9] yields $A \cong \mathcal{C}_p \times \cdots \times \mathcal{C}_p$.

The inverse implication is trivial. □

The fact that A is an elementary abelian p-group of order p^m can be expressed using only polynomial conditions. To simplify the notation we use the following scalar product:

Definition V.2. Let k be a field of prime characteristic p, $m \in \mathbb{N}_+$ and $l \in \mathbb{N}$ a non-negative integer with p-adic representation $l = \sum_{\nu \in \mathbb{N}} l_\nu p^\nu$. Furthermore let $c_0, \ldots, c_{m-1} \in k$ and $c := (c_0, \ldots, c_{m-1}) \in k^m$. Then we define

$$(l \cdot c) := l_0 c_0 + l_1 c_1 + \cdots + l_{m-1} c_{m-1} \in k.$$

This definition obviously yields an element of k for each l and c. If the c_μ are linearly independent over $\mathbb{F}_p \subseteq k$, it is a bijection $\{0, \ldots, p^m - 1\} \to \langle c_0, \ldots, c_{m-1} \rangle$.

Let us state our conditions for a finite subgroup of $(k,+)$:

Proposition V.8. *Let k be a field of prime characteristic p, $m \in \mathbb{N}_+$ and $r := p^m$. Let $A := \{a_0, \ldots, a_{r-1}\} \subseteq k$. A is a subgroup of $(k,+)$ with $|A| = r$ iff the following holds:*

(1) *$a_j - a_l \neq 0$ for all $j \neq l$, i.e. the a_j are pairwise distinct.*
(2) *There is a $c \in k^m$ such that an appropriate numbering of the a_j yields $a_j = (j \cdot c)$ for each $j \in \{0, \ldots, r-1\}$.*

Proof. Obviously $|A| = r$ is equivalent to condition (1). Thus, we may assume both of these conditions to be true.

Let $A \leq (k, +)$. By lemma V.7, we have $A \cong \mathcal{C}_p^m$. Thus, A has m generators $c_0, \ldots, c_{m-1}$ over $\mathbb{F}_p$. In other words, each a_j can be represented as a linear combination of the c_μ.

The reverse implication can be shown analogously. □

Using proposition V.8, we can specify a finite subgroup $A \leq (k, +)$ of cardinality p^m where both p and m are known, using only polynomial conditions: We use variable symbols for the generators $c_0, \ldots, c_{m-1}$ as well as for the elements a_j of A and assume the conditions of our proposition. We will use this in algorithm V.2.

Next, we discuss how to specify the condition

$$\left\{ a \in k \mid a \prod_{l=0}^{r-1} (a^n - b_l) = 0 \right\} \leq (k, +)$$

on the choice of the b_l in case (12) of theorem V.6. The assertion is translated to an equivalent set of polynomial conditions. To do so, we mainly use proposition V.8:

Proposition V.9. *Let k be an algebraically closed field of prime characteristic p, $m, n \in \mathbb{N}_+$, $n \mid p^m - 1$ and $r := \frac{p^m-1}{n}$. Then the following conditions are equivalent:*

(1) *There are $b_0, \ldots, b_{r-1} \in k$, such that*

$$\mathcal{U} := \left\{ a \in k \mid a \prod_{\nu=0}^{r-1} (a^n - b_\nu) = 0 \right\}$$

is a subgroup of $(k, +)$.

(2) *There are $b_0, \ldots, b_{r-1} \in k$ and $c \in k^m$ such that*
   (a) *For each $j, l \in \{0, \ldots, p^m - 1\}$, $j \neq l$ we have*

$$(j \cdot c) - (l \cdot c) \neq 0.$$

   (b) *For each $j \in \{0, \ldots, p^m - 1\}$ we have*

$$(j \cdot c) \cdot \prod_{\nu=0}^{r-1} ((j \cdot c)^n - b_\nu) = 0.$$

Proof. Let us assume condition (1). Obviously, $|\mathcal{U}| = 1 + nr = p^m$. By proposition V.8, there need to be $c \in k^m$ such that setting $a_j := (j \cdot g)$ implies $\mathcal{U} = \{a_j \mid j = 0, \ldots, p^m - 1\}$ and $a_j \neq a_l$ whenever $j \neq l$. From $a_j \neq a_l$, we immediately deduce condition (2a). Because $\mathcal{U} = \{a_j \mid j = 0, \ldots, p^m - 1\}$, we obtain

$$a_j \prod_{\nu=0}^{r-1} (a_j^n - b_\nu) = 0$$

for each j. Thus, condition (2b) holds.

To prove the inverse implication, we assume condition (2). Let $a_j := (j \cdot c)$ for each $j \in \{0, \ldots, p^m - 1\}$ and $\mathcal{V} := \{a_j \mid j = 0, \ldots, p^m - 1\}$. Because $a_j \neq a_l$ whenever $j \neq l$, we obtain $|\mathcal{V}| = p^m$. Proposition V.8 implies $\mathcal{V} \leq (k, +)$. From condition (2b), we infer $\mathcal{U} = \mathcal{V}$. □

We will use this characterization in algorithm V.3.

3. Subgroup Checking

In this section, we will see how to find out of which types a given hyperelliptic function field is. To do so, we give algorithms to check for each of the possible types. In order to avoid annoying the reader, we will restrict ourselves to giving explicit algorithms in the cases $\mathrm{F}[\mathcal{C}_n, \overline{k}]$, $(n,p) = 1$, $\mathrm{F}[\mathcal{C}_p^m, \overline{k}]$ and $\mathrm{F}[\mathcal{C}_p^m \rtimes \mathcal{C}_n, \overline{k}]$. The remaining cases are omitted, because they are similar to the first one. The cases $\mathrm{F}[\mathcal{C}_p^m, \overline{k}]$ and $\mathrm{F}[\mathcal{C}_p^m \rtimes \mathcal{C}_n, \overline{k}]$ will be discussed, since we need to check for certain subgroups of $(k, +)$, here.

Because the automorphism group is finite, the largest of its finite subgroups is the automorphism group itself. Thus, checking for all possible subgroups of the automorphism group solves our initial problem.

3.1. Checking for Cyclic Subgroups Whose Order is Prime to $\mathrm{char}(k)$**.** In this section we give an algorithm which checks, whether a hyperelliptic function field F/k is of type $\mathrm{F}[\mathcal{C}_n, \overline{k}]$ where $(n, \mathrm{char}(k)) = 1$. This algorithm can be viewed as a template algorithm for checking for all types of fields except those discussed in sections 3.2 and 3.3.

Algorithm V.1. Check, whether F/k is of type $\mathrm{F}[\mathcal{C}_n, \overline{k}]$, $(n,p) = 1$ for any n.

Input: Let $F = k(x,y)$, $y^2 = D_t$ be a hyperelliptic function field of prime characteristic $p > 2$.

Output: This algorithm reports, whether there exists some $n \in \mathbb{N}_+$ such that $(n,p) = 1$ and F is of type $\mathrm{F}[\mathcal{C}_n, \overline{k}]$.

Steps:

```
(1) For each $n \in \{2, 3, \dots, 2\mathrm{g}+2\}$, $s \in \mathbb{N}_+$ and $\nu \in \{0,1\}$ such that $(n,p) = 1$
    and $ns + \nu \in \{2\mathrm{g}+1, 2\mathrm{g}+2\}$, we perform the following steps:

    (1.1) Let $a_0, \dots, a_{s-1}$ be variable symbols representing elements of $\overline{k}$. We
          define
              $C_{\neq 0} := \{a_j \mid 0 \le j < s\} \cup \{a_j - a_l \mid 0 \le j < l < s\}.$
    (1.2) We check, whether there are $a_0, \dots, a_{s-1} \in \overline{k}$ such that we have $h \neq 0$
          for each $h \in C_{\neq 0}$ and $u^2 = t^\nu \prod_{\nu=0}^{s-1}(t^n - a_\nu)$ is a defining equation for
          $F\overline{k}$. To do so, we use algorithm IV.7.
          If this is the case, we report that $F$ is of type $\mathrm{F}[\mathcal{C}_n, \overline{k}]$.

(2) If step (1.2) does not report $F$ being of type $\mathrm{F}[\mathcal{C}_n, \overline{k}]$ for any $n$, we quit stating
    this fact.
```

The correctness of algorithm V.1 is obvious from that of algorithm IV.7 and from theorem V.6.

Remark V.10. If we use algorithm IV.6 instead of algorithm IV.7 in step (1.2) of algorithm V.1, we can construct the corresponding automorphisms, explicitly. Furthermore, we can find the smallest extension $k' \supseteq k$ such that F is of type $\mathrm{F}[\mathcal{C}_n, k']$ whenever F is of type $\mathrm{F}[\mathcal{C}_n, \overline{k}]$. To do so, we construct k' large enough to fulfill the following conditions:

(1) Fk' needs to have a basis $k'(t,u)$ with a defining equation of the form $u^2 = t^\nu \prod (t^n - a_j)$ as required for $F\overline{k}$ in theorem V.6. This is achieved by using algorithm IV.6.

(2) Each of the generators of $\mathrm{U}_{F\overline{k}}(\mathcal{C}_n)$ needs to be defined over k'. To achieve this, we need to enlarge k' such that it contains a primitive n-th root of unity, if $\nu = 0$ and a primitive $2n$-th root of unity, if $\nu = 1$.

Example V.1. We consider the field $F := \mathbb{F}_{10301}(x, y)$, given by

$$y^2 = D_x := x^5 - 3657x^4 - 2940x^3 - 2593x^2 - 463x - 1322.$$

We get the following possibilities to choose n, s and ν:

- $n = 2$, $s = 2$, $\nu = 1$, which implies $ns + \nu = 5$.
- $n = 2$, $s = 3$, $\nu = 0$, which implies $ns + \nu = 6$.
- $n = 3$, $s = 2$, $\nu = 0$, which implies $ns + \nu = 6$.
- $n = 4$, $s = 1$, $\nu = 1$, which implies $ns + \nu = 5$.
- $n = 5$, $s = 1$, $\nu = 0$, which implies $ns + \nu = 5$.
- $n = 5$, $s = 1$, $\nu = 1$, which implies $ns + \nu = 6$.
- $n = 6$, $s = 1$, $\nu = 0$, which implies $ns + \nu = 6$.

Applying algorithm IV.7 yields that F is of the following types

- $\mathrm{F}[\mathcal{C}_2, \overline{\mathbb{F}_{10301}}]$ with $s = 3$, $\nu = 0$,
- $\mathrm{F}[\mathcal{C}_2, \overline{\mathbb{F}_{10301}}]$ with $s = 2$, $\nu = 1$,
- $\mathrm{F}[\mathcal{C}_3, \overline{\mathbb{F}_{10301}}]$ with $s = 2$, $\nu = 0$ and
- $\mathrm{F}[\mathcal{C}_4, \overline{\mathbb{F}_{10301}}]$ with $s = 1$, $\nu = 1$.

To motivate the usability of the modification discussed in remark V.10, we apply it to the fourth of the above cases, where $n = 4$, $s = 1$ and $\nu = 1$. Here, step (1) of algorithm IV.6 yields a variety[4] which contains an infinite number of solutions. One of these solutions is given by $a_0 = 1$, $x = t - 3389$, $y = u$, i.e. we have $F = \mathbb{F}_{10301}(t, u)$, $u^2 = t(t^4 - 1)$. The corresponding automorphism ψ of $F\overline{k}/\overline{k}$ such that $\mathrm{U}(\mathcal{C}_4) = \langle \Phi, \psi \rangle$ is given by $\psi : t \mapsto 1020t$, $u \mapsto \sqrt{1020}u$. Thus, F is of type $\mathrm{F}[\mathcal{C}_4, \mathbb{F}_{10301^2}]$. The field $\mathbb{F}_{10301}$ does not contain an 8-th primitive root η of unity as required for the definition of ψ in case (1) of theorem V.6. Hence, $k' = \mathbb{F}_{10301^2}$ is the smallest possible extension of $\mathbb{F}_{10301}$ such that F is of type $\mathrm{F}[\mathcal{C}_4, k']$.

3.2. Checking for Elementary Abelian $\mathrm{char}(k)$**-Groups.** From case (2) of theorem V.6 we know that a hyperelliptic function field F/k is of type $\mathrm{F}[\mathcal{C}_p^m, \overline{k}]$ iff there exists a finite subgroup $A \leq (\overline{k}, +)$ of order $\mathrm{char}(k)^m$ such that F has a specific normal form. The subgroup condition can be specified using proposition V.8 as we see in the following algorithm:

Algorithm V.2. Check, whether F/k is of type $\mathrm{F}[\mathcal{C}_p^m, \overline{k}]$ for any m.

Input: Let $F = k(x, y)$, $y^2 = D_t$ be a hyperelliptic function field of prime characteristic $p > 2$.

Output: This algorithm reports, whether there exists some $m \in \mathbb{N}_+$ such that F is of type $\mathrm{F}[\mathcal{C}_p^m, \overline{k}]$.

Steps:

(1) For each $m, s \in \mathbb{N}_+$ such that $s \cdot p^m \in \{2\mathrm{g} + 1, 2\mathrm{g} + 2\}$, we perform the following steps:

(1.1) Let $a_0, \ldots, a_{s-1}, c_0, \ldots, c_{m-1}$ be variable symbols representing elements of $\overline{k}$ and $c := (c_0, \ldots, c_{m-1})$. We define

$$C_{\neq 0} := \{a_j - a_l \mid 0 \leq j < l < s\} \cup \{(j \cdot c) - (l \cdot c) \mid 0 \leq j < l < p^m\}$$

[4] the variety of the ideal E

(1.2) We check, whether there are $a_0, \dots, a_{s-1}, c_0, \dots, c_{m-1} \in \overline{k}$ such that we have

- $h \neq 0$ for each $h \in C_{\neq 0}$ and
- $u^2 = \prod_{j=0}^{s-1} \left(\prod_{l=0}^{p^m-1} (t + (l \cdot c)) - a_j \right)$ is a defining equation for $F\overline{k}$.

To do so, we use algorithm IV.7.
If this is the case, we report that F is of type $\mathrm{F}[\mathcal{C}_p^m, \overline{k}]$.

(2) If step (1.2) does not report F being of type $\mathrm{F}[\mathcal{C}_p^m, \overline{k}]$ for any n, we quit stating this fact.

Let us discuss the correctness of algorithm V.2 briefly. Proposition V.8 yields that the condition $C_{\neq 0} \neq 0$ is equivalent to $A := \{(0 \cdot c), \dots, ((p^m - 1) \cdot c)\}$ being a subgroup of $(k, +)$ of order p^m and the a_j being pairwise distinct. Thus, we obtain from case (2) of theorem V.6 and the correctness of algorithm IV.7 that algorithm V.2 also is correct.

Remark V.11. If we use algorithm IV.6 instead of algorithm IV.7 in step (1.2) of algorithm V.2, we can construct the corresponding automorphisms, explicitly. Furthermore we can find the smallest extension $k' \supseteq k$ such that F is of type $\mathrm{F}[\mathcal{C}_p^m, k']$ whenever F is of type $\mathrm{F}[\mathcal{C}_p^m, \overline{k}]$. This can be done analogously to remark V.10.

Example V.2. Let us consider the field $F := \mathbb{F}_3(x, y)$, given by

$$y^2 = D_x := x^9 - x^3 + x - 1.$$

The only possible choices of m and s are $m = 1$, $s = 3$ and $m = 2$, $s = 1$, because $3^m > 10$ for each $m > 2$. In both cases we have $s \cdot 3^m = 9 = 2\mathrm{g} + 1$. Applying algorithm IV.7 yields that F is of the types $\mathrm{F}[\mathcal{C}_3, \overline{\mathbb{F}_3}]$ and $\mathrm{F}[\mathcal{C}_3^2, \overline{\mathbb{F}_3}]$.

3.3. Checking for Semidirect Product Groups. From theorem V.6, case (12) we know that a hyperelliptic function field F/k is of type $\mathrm{F}[\mathcal{C}_p^m \rtimes \mathcal{C}_n, \overline{k}]$ iff there exist $b_0, \dots, b_{r-1} \in \overline{k}$ such that the set of zeroes of $t \cdot \prod_{j=0}^{r-1} (t^n - b_j)$ forms a subgroup of $(\overline{k}, +)$ and F has a specific normal form. The subgroup condition can be specified using proposition V.9 as we see in the following algorithm:

Algorithm V.3. Check, whether F/k is of type $\mathrm{F}[\mathcal{C}_p^m \rtimes \mathcal{C}_n, \overline{k}]$ for any m, n.

Input: Let $F = k(x, y)$, $y^2 = D_t$ be a hyperelliptic function field of prime characteristic $p > 2$.

Output: This algorithm reports, whether there exist $m, n \in \mathbb{N}_+$ such that F is of type $\mathrm{F}[\mathcal{C}_p^m \rtimes \mathcal{C}_n, \overline{k}]$.

Steps:

(1) For each $m, n \in \mathbb{N}_+$, $s \in \mathbb{N}$ and $\nu \in \{0, 1\}$ such that $\nu \cdot p^m + s \cdot n \cdot p^m \in \{2\mathrm{g} + 1, 2\mathrm{g} + 2\}$ and $n \mid p^m - 1$, we perform the following steps:

(1.1) Let $r := \frac{p^m - 1}{n}$, $a_0, \dots, a_{s-1}, b_0, \dots b_{r-1}, c_0, \dots, c_{m-1}$ be variable symbols representing elements of $\overline{k}$ and $c := (c_0, \dots, c_{m-1})$. We define

$$\begin{aligned} C_{\neq 0} :=& \{a_j \mid 0 \leq j < s\} \cup \{a_j - a_l \mid 0 \leq j < l < s\} \\ & \cup \{b_l \mid 0 \leq l < r\} \cup \{(j \cdot c) - (l \cdot c) \mid 0 \leq j < l < p^m\}, \\ C_0 :=& \left\{ (j \cdot c) \cdot \prod_{\nu=0}^{r-1} ((j \cdot c)^n - b_\nu) \mid 0 \leq j < p^m \right\}. \end{aligned}$$

(1.2) We check, whether there are $a_0, \dots, a_{s-1}, b_0, \dots, b_{r-1}, c_0, \dots, c_{m-1} \in \overline{k}$ such that we have

- $f = 0$ for each $f \in C_0$,
- $h \neq 0$ for each $h \in C_{\neq 0}$ and
- $F\overline{k}$ has the defining equation

$$u^2 = \left(t \prod_{l=0}^{r-1} (t^n - b_l) \right)^{\nu} \cdot \prod_{j=0}^{s-1} \left(\left(t \prod_{l=0}^{r-1} (t^n - b_l) \right)^n - a_j \right).$$

To do so, we use algorithm IV.7. If $F\overline{k}$ has this defining equation, we report that F is of type $\mathrm{F}[\mathcal{C}_p^m \rtimes \mathcal{C}_n, \overline{k}]$.

(2) If step (1.2) does not report F being of type $\mathrm{F}[\mathcal{C}_p^m \rtimes \mathcal{C}_n, \overline{k}]$ for any n, we quit stating this fact.

The correctness of algorithm V.3 follows from proposition V.9, theorem V.6 and the correctness of algorithm IV.7.

Remark V.12. If we use algorithm IV.6 instead of algorithm IV.7 in step (1.2) of algorithm V.3, we can construct the corresponding automorphisms, explicitly. Furthermore we can find the smallest extension $k' \supseteq k$ such that F is of type $\mathrm{F}[\mathcal{C}_p^m \rtimes \mathcal{C}_n, k']$ whenever F is of type $\mathrm{F}[\mathcal{C}_p^m \rtimes \mathcal{C}_n, \overline{k}]$. This can be done analogously to remark V.10.

Example V.3. We consider the field $F = \mathbb{F}_7(x, y)$, given by

$$y^2 = x^{14} + 5x^8 + x^2 + 6.$$

The only possible choice for m, n, s, ν is $m = 1$, $n = 2$, $s = 1$ $\nu = 0$ and it turns out that F actually is of the corresponding type $\mathrm{F}[\mathcal{C}_7 \rtimes \mathcal{C}_2, \overline{k}]$.

4. Computing the Automorphism Group

In this section we present a method to compute the reduced automorphism group of any hyperelliptic function field as well as the generators of its automorphism group. Knowing the above facts and algorithms, the idea of our algorithm is straightforward: We check our field for each possible type. The largest such type defines the reduced automorphism group.

Algorithm V.4. Compute $\mathrm{Aut}(F\overline{k}/\overline{k})/\langle\Phi\rangle$ and generators of $\mathrm{Aut}(F\overline{k}/\overline{k})$.

Input: Let $F = k(x, y)$, $y^2 = D_x$ be a hyperelliptic function field of characteristic $p > 2$.

Output: This algorithm computes $\mathrm{Aut}(F\overline{k}/\overline{k})/\langle\Phi\rangle$ as well as the generators of $\mathrm{Aut}(F\overline{k}/\overline{k})$.

Steps:

(1) For each possible type of field $\mathrm{F}[G, \overline{k}]$ as specified in theorem V.6, we check, whether F is of type $\mathrm{F}[G, \overline{k}]$. In the cases $G = \mathcal{C}_p^m$ and $G = \mathcal{C}_p^m \rtimes \mathcal{C}_n$, we use algorithms V.2 and V.3, respectively. In the case $G = \mathcal{C}_n$, we use algorithm V.1. The remaining cases are checked similarly to algorithm V.1.

(2) Let G be the largest[5] group such that F is of type $\mathrm{F}[G, \overline{k}]$. If F is of no type at all, let $G := \{1\}$.
We return $\mathrm{Aut}(F\overline{k}/\overline{k})/\langle\Phi\rangle \cong G$. From theorem V.6, we obtain the generators of $\mathrm{Aut}(F\overline{k}/\overline{k})$, which are defined with respect to the basis (t, u) whose existence has been shown in step (1). If F is of no type (i.e. if we defined

[5] Here, the term "larger" can be interpreted both with respect to the subgroup relation or with respect to group orders, because each $G \leq \mathrm{Aut}(F\overline{k}/\overline{k})$ and equality can be achieved.

$G = \{1\}$ above), $\mathrm{Aut}(F\overline{k}/\overline{k})$ is generated by the hyperelliptic involution Φ, only.
If the generators are needed explicitly, we apply algorithm IV.6 instead of algorithm IV.7 when checking for the field types as indicated in remark V.10. In other words, we solve the occurring systems of polynomials obtaining explicit formulas for the basis (t, u). These immediately give formulas for the generators of $\mathrm{Aut}(F\overline{k}/\overline{k})$ with respect to our given basis (x, y). Furthermore, we obtain the smallest k'/k such that $\mathrm{Aut}(Fk'/k') = \mathrm{Aut}(F\overline{k}/\overline{k})$ using this modification.

Example V.4. Let $F = \mathbb{F}_{9871}(x, y)$ be defined by

$$y^2 = x^5 - 3741x^4 - 2773x^3 - 4074x^2 - 2955.$$

In step (1) of algorithm V.4, we find out, that F is of the types $\mathrm{F}[\mathcal{C}_2, \overline{\mathbb{F}_{9871}}]$, $\mathrm{F}[\mathcal{C}_3, \overline{\mathbb{F}_{9871}}]$, $\mathrm{F}[\mathcal{C}_4, \overline{\mathbb{F}_{9871}}]$, $\mathrm{F}[\mathcal{D}_2, \overline{\mathbb{F}_{9871}}]$, $\mathrm{F}[\mathcal{D}_3, \overline{\mathbb{F}_{9871}}]$, $\mathrm{F}[\mathcal{D}_4, \overline{\mathbb{F}_{9871}}]$, $\mathrm{F}[\mathcal{A}_4, \overline{\mathbb{F}_{9871}}]$ and $\mathrm{F}[\mathcal{S}_4, \overline{\mathbb{F}_{9871}}]$. The largest of these groups is $\mathcal{S}_4$, its order is 24. Thus, we obtain the reduced automorphism group

$$\mathrm{Aut}(F\overline{\mathbb{F}_{9871}}/\overline{\mathbb{F}_{9871}})/\langle\Phi\rangle \cong \mathcal{S}_4.$$

The defining equation of $F\overline{\mathbb{F}_{9871}}$ which proves that F is of type $\mathrm{F}[\mathcal{S}_4, \overline{\mathbb{F}_{9871}}]$ is $u^2 = t^5 - t$, i.e. we have $\nu_0 = 1$, $\nu_1 = 0$, $\nu_2 = 0$ and $s = 0$. Theorem V.6, gives the generators of $\mathrm{Aut}(F\overline{\mathbb{F}_{9871}}/\overline{\mathbb{F}_{9871}})$. We start computing their parameters: Let i be a square root of -1 over $\mathbb{F}_{9871}$. Then, an 8-th primitive root of unity is given by $\eta := 4091(i + 1)$. The condition $\xi^2 = 8i$ implies $\xi = \pm 2(i + 1)$. We choose $\xi = 2(i + 1)$. Finally, we compute $m = 3$. Thus, we obtain the following generators of the automorphism group:

$$\begin{array}{lllllll}
\Phi: & t & \mapsto & t, & u & \mapsto & -u, \\
\psi: & t & \mapsto & it, & u & \mapsto & 4091(i+1)u, \\
\sigma: & t & \mapsto & i \cdot \frac{t+1}{t-1}, & u & \mapsto & \frac{2(i+1)u}{(t-1)^3}.
\end{array}$$

In order to express these automorphism with respect to our given basis (x, y), we need to solve for the corresponding basis transformation, explicitly. We obtain the solutions $x = t - 1226$, $y = u$ and $x = -t - 1226$, $y = iu$, from which we choose the former one. Substituting this transformation into the definitions of our generators yields their representations with respect to (x, y):

$$\begin{array}{lllllll}
\Phi: & x & \mapsto & x, & y & \mapsto & -y, \\
\psi: & x & \mapsto & ix + 1226(i-1), & y & \mapsto & 4091(i+1)y, \\
\sigma: & x & \mapsto & \frac{(i-1226)x+(1227i-1458)}{x+1225}, & y & \mapsto & \frac{2(i+1)y}{(x+1225)^3}.
\end{array}$$

Remark V.13. Based on the reduced automorphism group G and the ramification behaviour of F/F^G, Aristides Kontogeorgis ([**Kon99**]) gives explicit formulas for the structure of the automorphism group $\mathrm{Aut}(F\overline{k}/\overline{k})$.

Because we have not discussed how to compute ramification indices in these function field extensions, we will not go into further details of how to compute the group structure of $\mathrm{Aut}(F\overline{k}/\overline{k})$ itself, algorithmically.

5. Stoll's Algorithm

Even though algorithm V.4 can be used to compute automorphism groups over k if k is not algebraically closed, it is much more efficient when considering $\overline{k}$. This is due to the fact that solving a system of polynomial equations is much harder than checking its solvability. On the other hand, for finite k, Michael Stoll implemented[6] an algorithm to compute $\mathrm{Aut}(F/k)$ in [**Sto00**]. Stoll's algorithm (algorithm V.5) uses a totally different approach from algorithm V.4. Instead of trying to compute the structure and generators of the automorphism group, Stoll constructs each automorphism, separately. To characterize the automorphisms, Stoll uses proposition V.3. Let us outline Stoll's algorithm:

Algorithm V.5 (Stoll).

Input: Let $F = k(t, u)$ be a hyperelliptic function field over a finite constant field of characteristic > 2, given by the defining equation $u^2 = D(t)$.

Output: This algorithms lists the elements of $\mathrm{Aut}(F/k)$.

Steps:

(1) We construct all fractions $\frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3} \in k(t)$ such that $\alpha_0\alpha_3 - \alpha_1\alpha_2 \neq 0$ and there exists $\gamma \in k$ with

$$D(t) = \begin{cases} \gamma^2 \cdot (\alpha_2 t + \alpha_3)^{2\mathrm{g}+2} \cdot D\left(\frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}\right) & \text{if } \alpha_2 \neq 0 \\ \gamma^2 \cdot D\left(\frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}\right) & \text{if } \alpha_2 = 0. \end{cases}$$

(2) For each of the above fractions, we return the automorphisms $t \mapsto \frac{\alpha_0 t+\alpha_1}{\alpha_2 t+\alpha_3}$, $u \mapsto \pm\varphi u$, where

$$\varphi = \begin{cases} \frac{1}{\gamma\cdot(\alpha_2 t+\alpha_3)^{\mathrm{g}+1}} & \text{if } \alpha_2 \neq 0 \\ \frac{1}{\gamma} & \text{if } \alpha_2 = 0. \end{cases}$$

The correctness of algorithm V.5 is an immediate consequence of proposition V.3. We will compare the efficiencies of algorithms V.5 and V.4 in chapter VI. It will turn out that algorithm V.5 is fast if the automorphism group is small but that its running time seems to grow linearly with the order of the automorphism group. Because the algorithm has to consider every reduced automorphism separately, this observation is plausible.

[6] A theoretical discussion of Stoll's algorithm does not seem to exist, yet. The following is based on the `Magma` source code, only.

CHAPTER VI

Computational Aspects

One of our motivations for considering automorphism groups of hyperelliptic function fields was to sort out fields yielding insecure Jacobians, quickly. Because of its generality, the Pohlig-Hellman attack[1] poses a major threat to a Jacobian's security. Hence, we need to avoid Jacobians whose order have relevant divisors. As we saw in section II.3, the problem of computing the order of a general Jacobian is still unsolved. In most of the cases where order counting is possible, it takes a lot of time. Thus, a fast test which allows us to abandon Jacobians whose order has relevant divisors, would be of great value for the construction of secure Jacobians.

From Madan's theorem (theorem II.1), we know that $|\mathbb{J}_F|$ divides $|\mathbb{J}_{F'}|$ whenever F'/F is a finite Galois extension of function fields. Because finite Galois subfields are given by subgroups of the automorphism group[2], we conjecture that function fields with secure Jacobians need to have trivial[3] automorphism groups. In section 1 we consider such a secure Jacobian. We will see that the automorphism group of the corresponding hyperelliptic function field is indeed trivial.

In order to get an idea of how often our test will report an insecure field, we investigate the number of hyperelliptic function fields with non-trivial automorphism group in section 2. If a function field has non-trivial automorphisms, we would like to know how much influence this fact has on the actual security of the corresponding Jacobian—which we suspect to be insecure because of Madan's theorem. This influence can be measured by the fraction of the group orders of the Jacobians of the given and fixed fields. Because Madan's theorem does not contain any statement on this fraction, we investigate it computationally in section 3.

The authors implementation of algorithm V.4 and its running time are discussed in section 4, where we also compare it to the efficiency of Stoll's algorithm (algorithm V.5).

1. A Secure Jacobian

The first question which arises when thinking about the usage of automorphism groups to identify hyperelliptic function fields with insecure Jacobians is, whether secure hyperelliptic function fields have trivial automorphism groups.

Using zeta function methods[4], the author was able to construct a hyperelliptic function field which resists most known attacks[5]:

Example VI.1. Let $F = \mathbb{F}_{3^{61}}(t, u)$ with $u^2 = t^5 + t^4 + t$. The usual zeta function algorithm yields

$$|\mathbb{J}_F| = 8 \cdot 2021636587403726826456314444374236419919242578545012376397,$$

[1] cf. section II.2.

[2] cf. theorem I.25.

[3] i.e. it only contains the hyperelliptic involution

[4] cf. section II.3

[5] cf. section II.2

where the latter factor p_0 is a prime of 191 bits. Because of the size of p_0, the discrete logarithm problem on $\mathbb{J}_F$ cannot be solved using the Pohlig-Hellman method. It is easy to prove that p_0 does not divide $\left(3^{61}\right)^l - 1$ for any l in the range

$$1 \leq l \leq (\log_2(3^{61}))^2 \approx (96.68)^2 \approx 9347.5.$$

Hence, the Frey-Rück attack is inapplicable to $\mathbb{J}_F$. That the Adleman-DeMarrais-Huang attack is no threat to $\mathbb{J}_F$ is obvious, because $\mathrm{g}_F = 2 \leq 4$. Finally, $|\mathbb{J}_F|$ is no power of 3, which avoids the Rück attack.

Applying algorithm V.4, we obtain that F has the trivial automorphism group

$$\mathrm{Aut}(F/\mathbb{F}_{3^{61}}) = \mathrm{Aut}(F\overline{\mathbb{F}_{3^{61}}}/\overline{\mathbb{F}_{3^{61}}}) = \langle \Phi \rangle,$$

which is generated by the hyperelliptic involution.

This example leads us to assume that secure fields have trivial automorphism groups. Furthermore, this example proves that Madan's theorem (theorem II.1) cannot be reversed: Even though $|\mathbb{J}_F|$ has non-trivial divisors, there are no automorphisms whose fixed field has a divisor class number dividing any of them.

2. The Number of Non-Trivial Automorphism Groups

In this section we investigate the probability for a hyperelliptic function field to have a non-trivial automorphism group over the algebraic closure of its constant field, experimentally. This probability gives an idea of the usefulness of algorithm V.4 for checking hyperelliptic function fields for the security of their Jacobians: The more fields have non-trivial automorphism group, the more insecure fields can be avoided from being checked for security by more expensive methods. The question of how insecure a field with non-trivial automorphism group is, is discussed in section 3.

To estimate the probability for non-trivial automorphisms, the author computed the reduced automorphism groups $\mathrm{Aut}(F\overline{k}/\overline{k})/\langle\Phi\rangle$ of the following hyperelliptic function fields F/k using algorithm V.4:

1. All hyperelliptic function fields $F/\mathbb{F}_3$ of genera 2 and 3 in imaginary quadratic representation. See sections 1 and 2 of appendix A for a list of those such fields with non-trivial automorphism group $\mathrm{Aut}(F\overline{\mathbb{F}_3}/\overline{\mathbb{F}_3})$.
2. All hyperelliptic function fields $F/\mathbb{F}_5$ of genus 2 in imaginary quadratic representation. See section 3 of appendix A for a list of those such fields with non-trivial automorphism group $\mathrm{Aut}(F\overline{\mathbb{F}_5}/\overline{\mathbb{F}_5})$.
3. 10000 random hyperelliptic function fields $F/\mathbb{F}_p$ of genus 3 over prime fields of small characteristic $3 \leq p \leq 257$. See section 4 of appendix A for a list of those such fields with non-trivial automorphism group $\mathrm{Aut}(F\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p})$.
4. 10000 random hyperelliptic function fields $F/\mathbb{F}_p$ of genus 3 over prime fields of large[6] characteristic $16411 \leq p \leq 32003$. All of these fields had trivial automorphism group.
5. 6900 random hyperelliptic function fields $F/\mathbb{F}_p$ of genus 4 over prime fields of small characteristic $3 \leq p \leq 257$. See section 5 of appendix A for a list of those such fields with non-trivial automorphism group $\mathrm{Aut}(F\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p})$.
6. 6685 random hyperelliptic function fields $F/\mathbb{F}_p$ of genus 3 over prime fields of large characteristic $16411 \leq p \leq 32003$. All of these fields had trivial automorphism group.

[6] Our implementation of algorithm V.4 uses Singular ([**GPS$^+$02**]) for Gröbner basis computations. Because field characteristics are restricted to be ≤ 32003 in Singular, examples with larger characteristic cannot be computed using the author's implementation.

	Genus	Characteristic p	Number of Examples	Non-Trivial
(1)	2	3	162	29.6%
(1)	2	5	2500	16.0%
(2)	3	3	1458	10.2%
(3)	3	3–257	10000	0.15%
(4)	3	16411–32003	10000	0%
(5)	4	3–257	6900	0.12%
(6)	4	16411–32003	6685	0%

Table 1. Relative frequencies of hyperelliptic function fields over $\mathbb{F}_p$ with non-trivial automorphism group over $\overline{\mathbb{F}_p}$ in examples computed by the author. The number in the first column specifies the kind of example as discussed in section 2.

A collection of all of these examples can be found in [**Göb03b**].

The resulting relative frequencies of non-trivial automorphism groups are listed in table 1. From this data, we conjecture that it is very unlikely to find hyperelliptic function fields of large characteristic, which have non-trivial automorphism groups. In contrast, the genus of the considered fields does not seem to have much influence on the probability for finding non-trivial automorphisms.

We conclude that the computation of automorphism groups can only be useful for identifying insecure fields, if the characteristic is very small. On the other hand, it is quite easy to compute the divisor class number, if the characteristic is small (cf. section II.3). Hence, our initial goal to develop a fast criterion for insecure curves does not seem to be achievable by computing automorphism groups.

3. Fixed Fields and Their Class Numbers

Madan's theorem tells us that the order of the Jacobian of a Galois subfield divides the order of the Jacobian of a given function field F. From this fact, we conjectured that hyperelliptic function fields with non-trivial automorphism groups yield insecure Jacobians, because each non-trivial automorphism defines a subfield: Its fixed field. The aim of this section is to investigate experimentally, whether this conjecture is true. We compute fixed fields and compare their class numbers to that of F. If the class number of the fixed fields is about as large as the remaining factor of $|\mathbb{J}_F|$, the corresponding automorphism subgroup has the biggest possible impact on the security of $\mathbb{J}_F$.

Of course the largest Jacobians can be expected if we take small automorphism subgroups. This is due to the facts that the Jacobian order is[7] approximately $|k|^{\mathrm{g}}$ and that the genus of the subfield is[8] at most $1 + \frac{\mathrm{g}_F - 1}{m}$ for each nontrivial automorphism subgroup G of order m. This is, why we restrict our discussion to cyclic subgroups of $\mathrm{Aut}(F\overline{k}/\overline{k})$.

First, we have to find defining equations for fixed fields of cyclic automorphism subgroups. We start with a simple fact on the elements of F.

Lemma VI.1. *Let $F = k(t, u)$, $u^2 = D_t$ be a hyperelliptic function field. The elements of F can be written in the form*

$$\frac{\sum_{j=0}^{m} a_j t^j + u \sum_{j=0}^{m} b_j t^j}{\sum_{j=0}^{m} c_j t^j},$$

[7] Hasse-Weil interval, see page 40.

[8] This inequality is an easy consequence of corollary I.23 and $|G| = [F : F^G] =\geq 2$.

where $m \in \mathbb{N}$, $a_j, b_j, c_j \in k$ *and* $(a_m, b_m, c_m) \neq 0$.

Proof. Because $u^2 \in k(t)$, each element can be written in the form

$$\frac{\sum_{j=0}^m a_j t^j}{\sum_{j=0}^m c'_j t^j} + u \frac{\sum_{j=0}^m b_j t^j}{\sum_{j=0}^m d_j t^j},$$

with $m \in \mathbb{N}_+$, $a_j, b_j, c'_j, d_j \in k$ and $(a_m, b_m, c_m, d_m) \neq 0$. Computing the common denominator of both of these fractions yields our claim. □

Using this fact, it is very easy to characterize the elements of a fixed field:

Corollary VI.2. *Let* $F = k(t, u)$ *be a hyperelliptic function field and* U *a subgroup of* $\mathrm{Aut}(F/k)$*. Then*

$$F^U = \left\{ \frac{\sum_{j=0}^m a_j t^j + u \sum_{j=0}^m b_j t^j}{\sum_{j=0}^m c_j t^j} \in F \;\middle|\; \frac{\sum_{j=0}^m a_j t^j}{\sum_{j=0}^m c_j t^j} = \frac{\sum_{j=0}^m a_j \psi(t)^j}{\sum_{j=0}^m c_j \psi(t)^j} \text{ and } \frac{u \sum_{j=0}^m b_j t^j}{\sum_{j=0}^m c_j t^j} = \frac{\psi(u) \sum_{j=0}^m b_j \psi(t)^j}{\sum_{j=0}^m c_j \psi(t)^j} \text{ for all } \psi \in U \right\}$$

Proof. This easily follows from lemma VI.1, the linear independency of 1 and u and the fact that each automorphism maps u to a $k(t)$-multiple of u (proposition V.3). □

If we are able to give an upper bound[9] for the degree m of the elements of F^U, we can compute explicit formulas for these elements algorithmically. Unfortunately, such formulas do not give us a defining equation for the fixed field. Hence, these formulas are useless if we wish to compute data of the fixed field's Jabobian. Therefore, we will not discuss this algorithm in more detail. Let us prove some facts on defining equations of fixed fields of cyclic automorphism groups, instead.

From theorem V.6, we know that each cyclic subgroup[10] of the automorphism group is given by $\psi : t \mapsto \eta^2 t$, $u \mapsto \eta^\nu u$, where η is a root of unity and $\nu \in \{0, 1\}$ is the exponent of the factor t in the normal form. We consider the cases $\nu = 0$ and $\nu = 1$ separately, starting with the easier case $\nu = 0$.

3.1. Fixed Fields of $\mathcal{C}_n$, where $(n, \mathrm{char}(k)) = 1$ and $\nu = 0$. Let us consider the case, where F has a defining $u^2 = \prod_{j=0}^s (t^n - a_j)$. According to theorem V.6, we have $\mathrm{U}(\mathcal{C}_n) = \langle \Phi, \psi \rangle$ with $\psi : t \mapsto \eta^2 t$, $u \mapsto u$, where η is a $2n$-th primitive root of unity. In other words, ψ multiplies t by an n-th primitive root of unity and leaves u unchanged. Obviously, ψ generates both a cyclic subgroup of order n of $\mathrm{U}(\mathcal{C}_n)$ and the quotient group $\mathcal{C}_n \cong \mathrm{U}(\mathcal{C}_n)/\langle \Phi \rangle$. Thus, the fixed field we are interested in, is $F^{\mathcal{C}_n} = F^\psi$. This field can be computed very easily from our normal form:

Proposition VI.3. *Let* $F = k(x, y)$ *be a hyperelliptic function field of type* $\mathrm{F}[\mathcal{C}_n, k]$ *over an algebraically closed constant field* k *of characteristic* p *such that* $(n, p) = 1$*. Furthermore, let* $u^2 = \prod_{j=0}^s (t^n - a_j)$ *be the corresponding normal form and* $\mathrm{U}(\mathcal{C}_n) = \langle \Phi, \psi \rangle$*. Then* $F^\psi = k(t^n, u)$*.*

[9] The author conjectures $m \leq |U|$. An attempt to prove this supposition has not been made.

[10] whose order is relatively prime to the characteristic; the case of elementary abelian groups is discussed in section 3.3 below.

PROOF. From $\psi(t^n) = \psi(t)^n = (\eta^2)^n t^n = t^n$, $\psi(u) = u$ we get $k(t^n, u) \subseteq F^\psi$. To show equality, we consider extension degrees.

Obviously, $X^n - t^n \in k(t^n, u)[X]$ is a polynomial with root t, i.e. $[F : k(t^n, u)] \leq n$. From Galois theory, we know that $[F : F^\psi] = |\langle\psi\rangle| = n$. We infer

$$n = [F : F^\psi] \leq [F : F^\psi] \cdot [F^\psi : k(t^n, u)] = [F : k(t^n, u)] \leq n.$$

Hence $[F^\psi : k(t^n, u)] = 1$, i.e. $F^\psi = k(t^n, u)$ as claimed. □

REMARK VI.4. If the basis transformation $x = \frac{\alpha_0 t + \alpha_1}{\alpha_2 t + \alpha_3}$, $y = \varphi(t)u$ is known explicitly in proposition VI.3, we can also express the fixed field in terms of x and y:

$$F = k\left(\left(\frac{\alpha_3 x - \alpha_1}{\alpha_0 - \alpha_2 x}\right)^n, \varphi\left(\frac{\alpha_3 x - \alpha_1}{\alpha_0 - \alpha_2 x}\right) \cdot y\right).$$

This formula is obvious from $t = \frac{\alpha_3 x - \alpha_1}{\alpha_0 - \alpha_2 x}$.

EXAMPLE VI.2. Let $F = \mathbb{F}_{61}(x, y)$ be given by

$$y^2 = x^{10} + 19x^9 + 23x^8 + 14x^7 + 19x^6 + 51x^5 + 20x^4 + 48x^3 + 14x^2 + 30x + 3.$$

Using algorithm V.4 we obtain $\mathrm{Aut}(F\overline{\mathbb{F}_{61}}/\overline{\mathbb{F}_{61}})/\langle\Phi\rangle \cong \mathcal{C}_3$. For type $\mathrm{F}[\mathcal{C}_3, \overline{\mathbb{F}_{61}}]$, we obtain the normal form

$$u^2 = (t^3 - 32)(t^3 - 39)(t^3 - 55)$$

and the basis transformation

$$t = \frac{11x + 46}{x + 42}, u = \frac{13y}{(x + 42)^5}.$$

The corresponding automorphism (apart from Φ) is given by $\psi : t \mapsto 13t$, $u \mapsto u$. From proposition VI.3 and remark VI.4 we obtain the fixed field

$$\left(F\overline{\mathbb{F}_{61}}\right)^\psi = \overline{\mathbb{F}_{61}}(t^3, u) = \overline{\mathbb{F}_{61}}\left(\left(\frac{11x + 46}{x + 42}\right)^3, u\right).$$

Furthermore, our transformation as well as our automorphism are defined over $\mathbb{F}_{61}$. Thus, $\mathbb{F}_{61}(x, y) = \mathbb{F}_{61}(t, u)$ and $\langle\psi\rangle \leq \mathrm{Aut}(F/\mathbb{F}_{61})$. We obtain

$$F^\psi = F \cap \left(F\overline{\mathbb{F}_{61}}\right)^\psi = F \cap \overline{\mathbb{F}_{61}}(t^3, u) = \mathbb{F}_{61}(t^3, u).$$

Using KASH ([**DFK+97**]), we obtain the following orders of Jacobians:

$$|\mathbb{J}_{F^\psi}| = 636, \quad |\mathbb{J}_F| = 177476649696 = 636 \cdot 279051336.$$

In table 2, we list some hyperelliptic function fields of type $\mathrm{F}[\mathcal{C}_n, k]$, where $\nu = 0$, i.e. where the defining polynomial D_t is not divisible by t, and where the automorphisms in $\mathrm{U}(\mathcal{C}_n)$ are defined over k. The divisor class numbers have been computed using KASH ([**DFK+97**]). Note that the given defining equations are the normal forms of general hyperelliptic fields of this type. We observe that $|\mathbb{J}_{F^{\mathcal{C}_n}}|$ can be larger, smaller or even equal to the remaining factor of $|\mathbb{J}_F|$. To get an idea of this relation, we computed 140 examples of fixed fields of $\mathcal{C}_2$. On the average, $|\mathbb{J}_{F^{\mathcal{C}_2}}|$ is about 67% of the remaining factor $|\mathbb{J}_F|/|\mathbb{J}_{F^{\mathcal{C}_2}}|$. For different cyclic group orders n, this percentage changes to 0,7% ($n = 3$, 10 examples) or 0,1% ($n = 4$, 14 examples). These examples can be found in section 1 of appendix B. They suggest, that fields of type $\mathrm{F}[\mathcal{C}_2, k]$, where $\nu = 0$ are insecure, while cyclic subgroups of higher order do not seem to pose serious security problems.

k	n	s	a_j	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_n}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_n}}\rvert}$
$\mathbb{F}_{97}$	2	4	$10, 14, 17, 91$	976768	104	9392
$\mathbb{F}_{83}$	2	6	$1, 5, 12, 16, 46, 69$	4198547456	6976	601856
$\mathbb{F}_{83}$	2	6	$1, 8, 26, 27, 59, 78$	4009239552	7376	543552
$\mathbb{F}_{17}$	2	5	$3, 8, 13, 14, 16$	147456	384	384
$\mathbb{F}_{31}$	2	5	$4, 8, 16, 17, 22$	952576	976	976
$\mathbb{F}_{29}$	2	3	$7, 20, 23$	960	40	24
$\mathbb{F}_{79}$	2	5	$6, 23, 40, 44, 49$	37355520	7296	5120
$\mathbb{F}_{97}$	3	3	$15, 65, 77$	81870336	96	852816
$\mathbb{F}_{31}$	3	3	$13, 14, 16$	1288656	36	35796
$\mathbb{F}_{101}$	4	3	$5, 84, 100$	9599975424	96	99999744
$\mathbb{F}_{97}$	4	3	$1, 8, 64$	13530240000	100	135302400

Table 2. Jacobian orders of hyperelliptic function fields $F = k(t, u)$ of the form $u^2 = \prod_{j=0}^{s-1}(t^n - a_j)$ and of their fixed fields $F^{\mathcal{C}_n} = k(t^n, u)$

3.2. Fixed Fields of $\mathcal{C}_n$, where $(n, \mathrm{char}(k)) = 1$ and $\nu = 1$. We consider the case, where F has a defining $u^2 = t\prod_{j=0}^{s}(t^n - a_j)$. According to theorem V.6, we have $\mathrm{U}(\mathcal{C}_n) = \langle \Phi, \psi \rangle$ with $\psi : t \mapsto \eta^2 t$, $u \mapsto \eta u$, where η is a $2n$-th primitive root of unity. In contrast to the above case, we have $F^{\psi} \neq F^{\mathcal{C}_n}$. This follows from

$$\psi^n(t) = \eta^2 t = t, \quad \psi^n(u) = \eta^n u = -u,$$

i.e. $\Phi = \psi^n \in \langle \psi \rangle \cong \mathcal{C}_{2n}$. Therefore, we need to find a generator σ for $\mathcal{C}_n \leq \mathrm{Aut}(F/k)$, if we want to compute $F^{\mathcal{C}_n}$. To do so, we discuss some simple, group-theoretic facts.

Lemma VI.5. *Let $n > 1$ be an integer and G a cyclic group of order $2n$, generated by ψ. Then*

1. *G contains exactly one cyclic subgroup S of order n.*
2. *ψ^2 generates S.*
3. *G contains exactly one element of order 2. It is given by ψ^n.*

Proof. Let $S, S' \leq G$, $S, S' \cong \mathcal{C}_n$. If $S \neq S'$ we obtain $S \cap S' = \{1\}$. Hence $|S \cup S'| = 2n - 1$. The remaining element of G needs to be ψ because each element of $S \cup S'$ has order $\leq n$. From $\mathrm{ord}(\psi) = 2n \geq 4$, we obtain $\psi^3 \neq \psi$, i.e. $\psi^3 \in S \cup S'$. Thus, $\psi^{3n} = 1$, which implies $\psi^n = 1$. Contradiction. Thus, S is uniquely determined.

Because $\psi^{2n} = 1$, the order of ψ^2 is a divisor of n. As ψ is a generator of G, the order of ψ^2 needs to be n itself. Thus, $\langle \psi^2 \rangle \cong \mathcal{C}_n$, which implies $\langle \psi^2 \rangle = S$ since S is unique.

Let $\theta \in G$ have order 2. There exists some integer $\tau \in \{1, \ldots, 2n-1\}$ s.th. $\theta = \psi^{\tau}$. From $\theta^2 = 1$ we obtain $2n \mid 2\tau$, i.e. $n \mid \tau$. Thus, $\tau = n$ and θ is the only element of order 2. □

So, the generator σ of $\mathcal{C}_n \leq \mathrm{Aut}(F/k)$ we are looking for is just ψ^2. Because we want to examine the class number relation between F and F^{σ}, we are not interested in rational fixed fields[11]. Hence, only cases where $\Phi \notin \langle \sigma \rangle$ are of interest to us.

[11] The Jacobian of a rational function field is trivial. This is folklore knowledge and can easy be proved using proposition I.36

LEMMA VI.6. *Let $n > 1$ be an integer, G a cyclic group of order $2n$, ψ a generator of G, σ a generator of the cyclic subgroup of order n and $\Phi \in G$ the element of order 2. Then $\Phi \in \langle\sigma\rangle$ iff n is even.*

PROOF. By lemma VI.5 we obtain $\sigma = \psi^2$ and $\Phi = \psi^n$. The condition $\Phi \in \langle\sigma\rangle$ is equivalent to $\psi^{2\nu} = \sigma^\nu = \Phi = \psi^n$ for some ν, which is the same as $2n \bigm| 2\nu - n$, i.e. $2\mu n = 2\nu - n$, for some μ, ν. This in turn is equivalent to the existence of μ, ν such that $(2\mu + 1)n = 2\nu$, which is fulfilled iff n is even. □

Now, we are able to compute the fixed field of $\mathcal{C}_n$ in the current case:

PROPOSITION VI.7. *Let $F = k(x, y)$ be a hyperelliptic function field of type $\mathrm{F}[\mathcal{C}_n, k]$ over an algebraically closed constant field k of characteristic p such that $(n, p) = 1$. Furthermore, let $u^2 = t\prod_{j=0}^{s}(t^n - a_j)$ be the corresponding normal form and $\mathrm{U}(\mathcal{C}_n) = \langle\Phi, \psi\rangle$. Then $\langle\psi^2\rangle \cong \mathcal{C}_n$ is our cyclic group and the following holds:*

1. *If n is even, then F^{ψ^2} is rational.*
2. *If n is odd, then $F^{\psi^2} = k(t^n, t^{\frac{n-1}{2}}u)$ is given by the defining equation*
$$U^2 = T\prod_{j=0}^{s}(T - a_j),$$
where $T := t^n$, $U := t^{\frac{n-1}{2}}u$.

PROOF. From theorem V.6 we know that
$$\psi : t \mapsto \eta^2 t, \quad u \mapsto \eta u,$$
where η is a primitive $2n$-th root of unity. We have seen above that $\mathrm{U}(\mathcal{C}_n) \cong \mathcal{C}_{2n}$ and that this group is generated by ψ. From lemma VI.5, we know that there is exactly one cyclic subgroup $\mathcal{C}_n$ of $\mathrm{U}(\mathcal{C}_n)$ and that it is generated by $\sigma := \psi^2$. Furthermore, we have $\Phi = \psi^n$. Lemma VI.6 implies that $\Phi \in \langle\sigma\rangle$ iff n is even. According to this condition, we distinguish the following cases:

1. If n is even, we have $\Phi \in \langle\sigma\rangle$. We obtain the tower $F \supseteq F^\Phi \supseteq F^\sigma$ of fields. Because $F^\Phi = k(t)$ is rational, Lüroth's theorem[12] implies that F^σ also needs to be rational.
2. Let n be odd, now. First, we show that
$$k(t^n, t^{\frac{n-1}{2}}u) \subseteq F^\sigma.$$
To do so, we prove that both generators are fixed by σ:
$$\sigma(t^n) = \psi^2(t)^n = (\eta^4)^n t^n = (\eta^{2n})^2 t^n = t^n,$$
$$\sigma(t^{\frac{n-1}{2}}u) = \psi^2(t^{\frac{n-1}{2}}u) = (\eta^4)^{\frac{n-1}{2}} t^{\frac{n-1}{2}} \cdot \eta^2 u = \eta^{2n-2+2} t^{\frac{n-1}{2}} u = t^{\frac{n-1}{2}} u.$$
Since this implies the above inclusion, it remains to show
$$k(t^n, t^{\frac{n-1}{2}}u) \supseteq F^\sigma.$$

[12] Lüroth's theorem can be found in any good algebra book. See for example [**vdW93a**, §73].

$$\begin{tikzcd}
& F \arrow[d, dash, "n"'] \arrow[dr, dash, "2"] & \\
& F^{\sigma} \arrow[dl, dash] \arrow[dd, dash, "2"] & F^{\Phi} = k(t) \arrow[ddl, dash, "n"'] \\
k(t^n, t^{\frac{n-1}{2}}u) \arrow[dr, dash] & & \\
& F^{\langle\sigma,\Phi\rangle} = k(t^n) &
\end{tikzcd}$$

To verify this fact, we discuss the diagram on the right. Because n is odd, there exists a $\nu \in \mathbb{N}$ s.th. $n-2\nu = 1$, i.e. $\psi = \psi^{n-2\nu} = \psi^n\psi^{2n-2\nu} = \Phi\sigma^{n-\nu} \in \langle\sigma, \Phi\rangle$. Hence, $\langle\sigma, \Phi\rangle = \langle\psi\rangle \cong \mathcal{C}_{2n}$, which implies the extension degrees given in the diagram. $F^{\Phi} = k(t)$ is trivial. Above we have seen that $\sigma(t^n) = t^n$, i.e. $k(t^n) \subseteq F^{\langle\sigma,\Phi\rangle}$. Because t is a root of $X^n - t^n \in k(t^n)[X]$, we obtain $[k(t) : k(t^n)] \leq n$, which implies $k(t^n) = F^{\langle\sigma,\Phi\rangle}$. Hence, the diagram is correct.

Because $t^{\frac{n-1}{2}}u \notin k(t^n)$, we need to have $[k(t^n, t^{\frac{n-1}{2}}u) : k(t^n)] \geq 2$, which yields $[F^{\sigma} : k(t^n, t^{\frac{n-1}{2}}u)] = 1$, i.e. $F^{\sigma} = k(t^n, t^{\frac{n-1}{2}}u)$ as claimed.

Finally, we prove the defining equation. Let $T := t^n$, $U := t^{\frac{n-1}{2}}u$. Then,

$$U^2 = t^{n-1}u^2 = t^{n-1} \cdot t\prod_{j=0}^{s}(t^n - a_j) = t^n\prod_{j=0}^{s}(t^n - a_j) = T\prod_{j=0}^{s}(T - a_j)$$

as was to be shown.

□

Of course, remark VI.4 can be applied analogously. We will see this in the following example. Because rational subfields are not very interesting, we only give an example for the case where n is odd.

Example VI.3. Let $F = \mathbb{F}_{97}(x, y)$ be given by

$$y^2 = x^8 + 76x^7 + 63x^6 + 89x^5 + 61x^4 + 12x^3 + 55x^2 + 86x + 30.$$

Setting $t := \frac{74x+26}{x+22}$, $u := \frac{35}{(x+22)^4} \cdot y$ we obtain the normal form

$$u^2 = t(t^3 - 39)(t^3 - 18).$$

The mapping $\psi : t \mapsto 61t$, $u \mapsto 62u$ defines an automorphism with $\mathrm{U}(\mathcal{C}_3) = \langle\Phi, \psi\rangle$, $\langle\psi\rangle \cong \mathcal{C}_6$ and $\langle\psi^2\rangle \cong \mathcal{C}_3$. From proposition VI.7 we obtain the fixed field

$$(F\overline{\mathbb{F}_{97}})^{\psi^2} = \overline{\mathbb{F}_{97}}(t^3, tu) = \overline{\mathbb{F}_{97}}\left(\left(\frac{74x+26}{x+22}\right)^3, \frac{68x+37}{(x+22)^5} \cdot y\right) =: \overline{\mathbb{F}_{97}}(T, U),$$

where $U^2 = T(T - 39)(T - 18)$. Because both our automorphisms and our basis transformation are defined over $\mathbb{F}_{97}$ itself, we obtain $\mathrm{Aut}(F\overline{\mathbb{F}_{97}}/\overline{\mathbb{F}_{97}}) = \mathrm{Aut}(F/\mathbb{F}_{97})$ and $F^{\mathcal{C}_3} = \mathbb{F}_{97}(T, U)$. Using `KASH` ([**DFK**$^+$**97**]), we obtain the following class numbers:

$$|\mathbb{J}_{F^{\mathcal{C}_3}}| = 92, \quad |\mathbb{J}_F| = 783104 = 92 \cdot 8512.$$

In table 3, we list some hyperelliptic function fields of type $\mathrm{F}[\mathcal{C}_n, k]$, where $\nu = 1$, i.e. where the defining polynomial D_t is divisible by t and all elements of $\mathrm{U}(\mathcal{C}_n)$ are defined over k. Because n needs to be odd if we want non-rational fixed fields and large n results in large class numbers ($|\mathbb{J}| \approx |k|^{\mathrm{g}} = |k|^{ns}$ with $s \geq 3$, which also is needed for non-rational fixed fields), we only considered the case $n = 3$, here. The divisor class numbers have been computed using `KASH` ([**DFK**$^+$**97**]). Note that the given defining equations are the normal forms of general hyperelliptic fields of this

k	s	a_j	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_n}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_n}}\rvert}$
$\mathbb{F}_7$	3	$1,3,4$	2016	8	252
$\mathbb{F}_7$	3	$1,3,6$	2304	12	192
$\mathbb{F}_7$	3	$2,4,6$	1824	8	228
$\mathbb{F}_{13}$	3	$3,6,11$	20124	12	1677
$\mathbb{F}_{31}$	3	$1,22,26$	1954800	36	54300
$\mathbb{F}_{31}$	3	$2,5,18$	1954800	36	54300
$\mathbb{F}_{31}$	3	$4,9,19$	1083600	28	38700
$\mathbb{F}_{31}$	3	$6,10,17$	978984	24	40791
$\mathbb{F}_{31}$	3	$6,16,26$	1566864	36	43524
$\mathbb{F}_{31}$	3	$19,26,28$	2135484	36	59319

TABLE 3. Jacobian orders of hyperelliptic function fields $F = k(t,u)$ of the form $u^2 = t\prod_{j=0}^{s-1}(t^3 - a_j)$ and of their fixed fields $F^{\mathcal{C}_3} = k(t^3, tu)$

type. To get an idea of the relation between $|\mathbb{J}_{F^{\mathcal{C}_n}}|$ and the remaining factor of $|\mathbb{J}_F|$, we computed 126 examples[13] of fixed fields of $\mathcal{C}_3$. On the average, $|\mathbb{J}_{F^{\mathcal{C}_3}}|$ is about 0.7% of the remaining factor $|\mathbb{J}_F|/|\mathbb{J}_{F^{\mathcal{C}_3}}|$. This percentage is approximately the same as in the case $\nu = 0$ above.

We conjectured at the end of section 3.1 that exactly the cyclic automorphism subgroups of order 2 pose a major threat on the security of the corresponding Jacobian. The examples given in this section confirm this supposition: Automorphisms of order 3 yield fixed fields whose Jacobians are quite small.

3.3. Fixed Fields of $\mathcal{C}_p^m$. In the above sections, we computed fixed fields of cyclic automorphism subgroups whose order is prime to the characteristic p. As we would like to compute fixed fields of all kinds of cyclic subgroups, we consider the remaining case of fixed fields of elementary abelian p-groups, now. According to theorem V.6, the automorphism group has such a subgroup $\mathrm{U}(\mathcal{C}_p^m)$, if the hyperelliptic function field has the normal form

$$u^2 = \prod_{j=0}^{s-1}\left(\prod_{a\in A}(t+a) - a_j\right),$$

where $s \in \mathbb{N}_+$, the $a_j \in k$ are pairwise distinct and $A \leq (k,+)$, $|A| = p^m$. Then $\mathrm{U}_F(\mathcal{C}_p^m)$ is generated by Φ and all $\psi_a : t \mapsto t + a$, $u \mapsto u$ with $a \in A$. It is obvious that the corresponding $\mathcal{C}_p^m$ is generated by the ψ_a, $a \in A$. Computing the fixed field is quite easy in this case:

PROPOSITION VI.8. *Let $F = k(x,y)$ be a hyperelliptic function field of type* $\mathrm{F}[\mathcal{C}_p^m, k]$ *over an algebraically closed constant field k of characteristic p. Furthermore, let*

$$u^2 = \prod_{j=0}^{s-1}\left(\prod_{a\in A}(t+a) - a_j\right),$$

where $a_j \in k$ and $A \leq (k,+)$, $|A| = p^m$ be the corresponding normal form. Let $\mathrm{U}(\mathcal{C}_p^m) = \langle \Phi, (\psi_a)_{a\in A}\rangle$. Then $G := \langle(\psi_a)_{a\in A}\rangle \cong \mathcal{C}_p^m$ is our elementary abelian group and its fixed field is given by

$$F^G = k\left(\prod_{a\in A}(t+a), u\right).$$

[13] These examples can be found in the section 2 of appendix B.

Setting $T := \prod_{a\in A}(t+a)$, $U := u$, *we obtain* $F^G = k(T,U)$ *with the defining equation* $U^2 = \prod_{j=0}^{s=1}(T-a_j)$.

Proof. According to theorem V.6, the automorphisms ψ_a, $a \in A$ are given by $\psi_a : t \mapsto t+a$, $u \mapsto u$. From this, it is obvious that

$$\mathrm{U}(\mathcal{C}_p^m) = \langle \Phi, (\psi_a)_{a\in A}\rangle = \langle \Phi\rangle \times \langle (\psi_a)_{a\in A}\rangle = \langle \Phi \rangle \times G \cong \mathcal{C}_2 \times \mathcal{C}_p^m.$$

Thus, G is our elementary abelian group. We obtain $F^G \supseteq k(T,U)$ from the following equations, which are consequences of $a \in A$ and A being a group:

$$\begin{aligned}\psi_a(T) =& \psi_a\left(\prod_{\alpha\in A}(t+\alpha)\right) = \prod_{\alpha\in A}(t+a+\alpha) = \prod_{\alpha\in A}(t+\alpha) = T\\ \psi_a(U) =& \psi_a(u) = u = U.\end{aligned}$$

Next, we show $F^G = k(T,U)$: We consider the polynomial

$$\prod_{\alpha\in A}(X+\alpha) - T \in k(T,U)[X].$$

Its degree is $|A| = p^m$ and t is a zero. Thus, $[F : k(T,U)] \le p^m$. Because $[F : F^G] = p^m$, we obtain

$$p^m \ge [F : k(T,U)] = [F : F^G][F^G : k(T,U)] = p^m \cdot [F^G : k(T,U)] \ge p^m,$$

which implies $F^G = k(T,U)$ as claimed. Now, it is obvious that F^G has the defining equation $U^2 = \prod_{j=0}^{s-1}(T-a_j)$. □

Again we can apply remark VI.4 analogously. We will see this in the following example.

Example VI.4. We consider the field $\mathbb{F}_3(x,y)$ given by

$$y^2 = x^9 + x^7 + x^6 + 2x^4 + 2x^3 + 2x.$$

Setting $t := \frac{1}{x+1}$ and $u := \frac{1}{(x+1)^5}y$, we obtain the normal form

$$\begin{aligned}u^2 =& (t^3-t)(t^3-t-1)(t^3-t+1)\\ =& \left(\prod_{a=0}^{2}(t-a)\right)\cdot\left(\prod_{a=0}^{2}(t-a)-1\right)\cdot\left(\prod_{a=0}^{2}(t-a)+1\right).\end{aligned}$$

For $a \in A = \{0,1,2\}$, set $\psi_a : t \mapsto t+a$, $u \mapsto u$, which yields $\mathrm{U}(\mathcal{C}_3) = \langle \Phi, \psi_0, \psi_1, \psi_2\rangle$. Let $G := \{\psi_0, \psi_1, \psi_2\}$. According to proposition VI.8, the fixed field is given by

$$F\overline{\mathbb{F}_3}^G = \overline{\mathbb{F}_3}(t^3-t, u) = \overline{\mathbb{F}_3}\left(\frac{1}{(x+1)^3} - \frac{1}{x+1}, u\right) = \overline{\mathbb{F}_3}\left(\frac{2x^2+x}{x^3+1}, \frac{1}{(x+1)^5}y\right).$$

Because all of the above is defined over $\mathbb{F}_3$ we further obtain

$$F^G = \mathbb{F}_3(t^3-t, u).$$

Using KASH ([**DFK**$^+$**97**]), we obtain the following class numbers:

$$|\mathbb{J}_{F^G}| = 4, \quad |\mathbb{J}_F| = 112 = 4\cdot 28.$$

In table 4, we list some hyperelliptic function fields of type $\mathrm{F}[\mathcal{C}_p^m, k]$, where $p = \mathrm{char}(k)$. Because we want non-rational fixed fields and the class numbers need to be computable reasonably fast, we only consider $m = 1$ and small p. The divisor class numbers have been computed using KASH. Note that the given defining equations are the normal forms of general hyperelliptic fields of this type. On the average over the examples given in table 4, $|\mathbb{J}_{F^{\mathcal{C}_3}}|$ is about 1.3% of the remaining factor $|\mathbb{J}_F|/|\mathbb{J}_{F^{\mathcal{C}_3}}|$.

k	s	a_j	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_n}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_n}}\rvert}$
$\mathbb{F}_3$	3	$0,1,2$	112	4	28
$\mathbb{F}_5$	3	$0,1,2$	99968	8	12496
$\mathbb{F}_5$	3	$0,1,3$	134464	4	33616
$\mathbb{F}_5$	3	$0,1,4$	46208	8	5776
$\mathbb{F}_5$	3	$0,2,3$	61504	4	15376
$\mathbb{F}_5$	3	$0,2,4$	134464	4	33616
$\mathbb{F}_5$	3	$0,3,4$	99968	8	12496
$\mathbb{F}_5$	3	$1,2,3$	262328	8	32791
$\mathbb{F}_5$	3	$1,2,4$	28684	4	7171
$\mathbb{F}_5$	3	$1,3,4$	28684	4	7171
$\mathbb{F}_5$	3	$2,3,4$	262328	8	32791

TABLE 4. Jacobian orders of hyperelliptic function fields $F = k(t,u)$ of the form $u^2 = \prod_{j=0}^{s-1}\left(\left(\prod_{a\in k}(t-a)\right) - a_j\right)$, and of their fixed fields $F^{\mathcal{C}_p} = k\left(\prod_{a\in k}(t-a), u\right)$, where $p := \mathrm{char}(k)$

At the end of sections 3.1 and 3.2 we conjectured that exactly the cyclic automorphism subgroups of order 2 pose a major threat on the security of the corresponding Jacobians. The examples given in this section confirm this supposition: Even for small characteristic p, automorphisms of order p yield fixed fields whose Jacobians are quite small.

4. Efficiency Considerations and Comparison to Stoll's Algorithm

In this section, we discuss some issues of the author's implementation of algorithm V.4. We consider its running time and compare it to that of Stoll's algorithm (algorithm V.5).

The author implemented algorithm V.4 for the computer algebra systems MuPAD ([**Sci02**]) and Singular ([**GPS$^+$02**]). The Gröbner basis steps are implemented for Singular, while anything else—i.e. Brandt's normal forms, computing their integer parameters, substitution, computing φ and the comparing of coefficients—is programmed for MuPAD. Both parts of the program are combined using Bash ([**Fre98**]) scripts. It was decided to separate the Gröbner basis steps from the rest of the computation, since on the one hand, Singular has one of the most efficient Gröbner basis implementations. On the other hand, Singular is restricted to characteristic $p \leq 32003$, which is too small for many fields of cryptographic relevance.

As a proof of concept, the implementation is not optimized for speed at all. For example, we actually test for all types of function fields, regardless of the fact whether $\mathrm{Aut}(F\overline{k}/\overline{k})/\langle\Phi\rangle$ contains cyclic subgroups. Of course, if no cyclic subgroups exist, the automorphism group needs to be trivial, so we check many field types in vain. We check for all types, because of our separation of code between MuPAD and Singular: Our MuPAD code writes code for Singular without obtaining any feedback on the types of F. Hence, checking for all types was easier to implement.

Because of these implementation issues, a speedup by a factor of at least 10 ought to be possible using a "proper" implementation. Nevertheless, the examples given in table 5 suggest that even our implementation computes the (reduced) automorphism group $\mathrm{Aut}(F\overline{k}/\overline{k})/\langle\Phi\rangle$ of an arbitrary hyperelliptic function field very efficiently. The performance seems to depend neither on the size of the constant

k	Defining Equation	$\lvert\mathrm{Aut}(\overline{k}(x,y)/\overline{k})\rvert$	seconds
$g=2$:			
$\mathbb{F}_{9491}$	$y^2 = x^5 - 4608x + 1124$	2	12.6
$\mathbb{F}_{10223}$	$y^2 = x^6 - 4x^4 - 4x^2 + 1$	4	52.5
$\mathbb{F}_{10711}$	$y^2 = x^6 + 394x^3 - 3378$	12	23.3
$\mathbb{F}_3$	$y^2 = x^6 + x^4 + x^2 + 1$	24	9.8
$\mathbb{F}_3$	$y^2 = x^6 + x^4 + x^2 + 1$	48	9.2
$\mathbb{F}_5$	$y^2 = x^5 + 4x$	240	22.7
$g=3$:			
$\mathbb{F}_{11}$	$y^2 = x^7 + 6x^6 + 5x^4 + 4x^3 + x + 3$	2	67.0
$\mathbb{F}_3$	$y^2 = x^8 + x^7 + 2x^5 + 2x + 2$	8	30.3
$\mathbb{F}_7$	$y^2 = x^7 + 6x^4 + 4x^3 + x^2 + 2$	42	67.8
$g=4$:			
$\mathbb{F}_5$	$y^2 = x^{10} + x^8 + 3x^6 + 4x^2 + 4$	4	81.8
$\mathbb{F}_3$	$y^2 = x^9 + 2x^7 + 2x^3 + 2x$	8	46.6

TABLE 5. Time to compute $\mathrm{Aut}(\overline{k}(x,y)/\overline{k})$ on an Intel® Celeron®, 1.7 GHz, ordered by genus and $\lvert\mathrm{Aut}(\overline{k}(x,y)/\overline{k})\rvert$

field, nor on the order of $\mathrm{Aut}(F\overline{k}/\overline{k})$. Even though increasing the genus increases the size of the systems of polynomials—the number of both the polynomials and the parameters increase linearly with g for types like $\mathrm{F}[\mathcal{C}_2, \overline{k}]$—, the examples indicate that even for fields of genus 4 and higher, the automorphism group computations are quite fast. More examples of running times can be found in sections 4 and 5 of appendix A.

Let us discuss the cryptographic application, briefly. As explained before, the initial goal was to provide an algorithm to check, whether a given hyperelliptic function field promises to yield a secure Jacobian, i.e. whether it is worthwhile to apply more expensive algorithms to check a given curve for security. Because of the attacks mentioned in section II.2, secure curves need to have small automorphism groups $\mathrm{Aut}(F/k)$. Since $\mathrm{Aut}(F/k) \leq \mathrm{Aut}(F\overline{k}/\overline{k})$, algorithm V.4 can be used to assure this property. The timings of table 5 also apply to the set of relevant curves, as secure curves are of genus ≤ 4 because of the Adleman-DeMarrais-Huang attack ([**ADH94**]) and as the characteristic of the constant field and the size of the automorphism group do not seem to influence the running time. Hence, algorithm V.4 can be applied efficiently to hyperelliptic function fields of practical relevance. On the other hand, the examples given in section 2 indicate that it is not very probable to identify hyperelliptic function fields with insecure Jacobian by investigating their automorphism groups.

The extensions to algorithm V.4 which compute the automorphism group over k itself or which construct the smallest k' such that $\mathrm{Aut}(Fk'/k') = \mathrm{Aut}(F\overline{k}/\overline{k})$ have not been implemented. Nevertheless, we will compare algorithm V.4 to Michael Stoll's `AutomorphismGroup` function (algorithm V.5), experimentally. To do so, we choose the constant field k of F large enough, such that $\mathrm{Aut}(F/k) = \mathrm{Aut}(F\overline{k}/\overline{k})$ holds[14], in each example. $\mathrm{Aut}(F\overline{k}/\overline{k})$ is computed using algorithm V.4, while Stoll's method is used to compute $\mathrm{Aut}(F/k)$. The running times for some examples are given in table 6.

[14] We start with a hyperelliptic function field $\tilde{F}$ over $\mathbb{F}_p$ for some prime p and compute $\mathrm{Aut}(\tilde{F}\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p})/\langle\Phi\rangle$ using algorithm V.4. Then, we try the extensions $k/\mathbb{F}_p$ by hand, until algorithm V.5 yields an automorphism group $\mathrm{Aut}(\tilde{F}k/k)$ of order $2 \cdot \lvert\mathrm{Aut}(\tilde{F}\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p})/\langle\Phi\rangle\rvert$. Setting $F := \tilde{F}k$, we obtain $\mathrm{Aut}(F/k) = \mathrm{Aut}(F\overline{k}/\overline{k})$.

Function Field $F = k(t, u)$			Running Time	
k	Defining Equation	$\lvert \mathrm{Aut}(F/k) \rvert$	Stoll	Göb
$\mathbb{F}_{3^6}$	$u^2 = t^9 + 2t^3 + t + 2$	36	2.9	27.7
$\mathbb{F}_{5^2}$	$u^2 = t^5 + 4t$	240	18.1	22.7
$\mathbb{F}_{7^2}$	$u^2 = t^7 + 6t$	672	228.3	61.0
$\mathbb{F}_{3^4}$	$u^2 = t^9 + 2t$	1440	1347.3	34.1
$\mathbb{F}_{11^2}$	$u^2 = t^{11} + 10t$	2640	5625.1	90.3 5

TABLE 6. Running time comparison between Michael Stoll's algorithm V.5 and algorithm V.4, timings in seconds on an Intel® Celeron®, 1.7 GHz

From these examples, Stoll's algorithm seems to be quite fast for small automorphism groups, while it is very slow for large ones. As stated above, our implementation does not seem to be influenced by the group size at all. Thus, if you are quite sure that the field you are investigating only has a small automorphism group, Stoll's algorithm ought to be preferred. Even though the majority of hyperelliptic function fields has a small automorphism group[15], the remaining fields do not seem to be suited for Stoll's algorithm. Hence, in order to compute the automorphism group of an arbitrary hyperelliptic function field, it might be sensible to use algorithm V.4 as it at least seems to be more predictable with respect to performance. Furthermore, Stoll's algorithm returns every single automorphism, while our method, gives the structure as well as the generators of the automorphism group. Thus, it also depends on the application, which of the algorithms ought to be preferred.

[15] See section 2.

Conclusion

In this thesis, we developed and investigated algorithms to compute the automorphism groups of hyperelliptic function fields[16]. Let us give a brief summary of the major steps to achieving this goal as well as of some interesting byproducts and open problems.

We devised methods to decide whether two hyperelliptic function fields F, G are isomorphic: If both F and G are known explicitly, i.e. if their defining equations do not contain parameters, algorithm IV.2 is very fast, but it can only decide between $F \not\cong G$ and knowing nothing at all. Furthermore, it can only be used if k is not algebraically closed. To find out whether $F \cong G$, we can apply algorithm IV.9, which uses specific normal forms developed in section IV.3. Even if G is only given up to some unknown parameters, we can find out, whether there exist parameter settings such that $F \cong G$. This time, we need to use the slower yet quite efficient algorithm IV.7 which uses Gröbner basis techniques. It remains unknown whether it is possible to extend algorithm IV.9 in such a way that it can also be used in this case[17]. If this could be done efficiently, we likely obtained an algorithm for computing automorphism groups, which was even faster than algorithm V.4.

Algorithm IV.7 is mainly based on theorem III.18, which makes the condition for isomorphy between hyperelliptic function fields very explicit: Given hyperelliptic function fields $k(t,u)$, $u^2 = D_t(t)$ and $k(X,Y)$, $Y^2 = D_x(X)$, we have $k(t,u) \cong k(X,Y)$ iff there are $x, y \in k(t,u)$ such that $y^2 = D_x(x)$ and the following holds: x is a fraction of linear polynomials from $k[t]$ and y is a $k(t)$-multiple of u, where the factor $\frac{y}{u}$ is given up to its sign by the relation between t and x. A theoretical application of this theorem arises for example in section VI.3, where we investigate fixed fields of automorphisms.

The above algorithms and the knowledge of Brandt's normal forms (theorem V.6) culminate in our technique to compute the structure of the reduced automorphism group $G := \mathrm{Aut}(F/k)/\langle\Phi\rangle$ as well as the generators of the automorphism group $\mathrm{Aut}(F/k)$ of any hyperelliptic function field F/k, efficiently (algorithm V.4 and its sub-algorithms). While this data is more than we need in most cases of practical interest, it would also be nice to know the structure of the automorphism group $\mathrm{Aut}(F/k)$ itself. One way to tackle this problem could be to investigate the ramification behavior of the function field extension F/F^G and apply theorems by Aristides Kontogeorgis ([**Kon99**], see remark V.13).

In order to show the usability of our algorithms and to check, whether our initial motivation for their development—identifying insecure Jacobians, quickly—can be fulfilled, we implemented several of our algorithms and computed a huge number

[16] For simplicity, all the function fields we talk about in this conclusion are assumed to be defined over algebraically closed constant fields.

[17] cf. remark IV.14

of examples[18]. We found out that even a bad (i.e. slow) implementation of algorithm V.4 runs quite fast. Hence a proper implementation ought to be very efficient. Concerning our motivation we investigated two aspects, experimentally:

(1) The probability for a hyperelliptic function field to have a non-trivial automorphism group and
(2) the class number relations $\frac{|\mathbb{J}_F|}{|\mathbb{J}_{F^\sigma}|}$, where $\sigma \in \mathrm{Aut}(F/k)$.

The probability of non-trivial automorphism groups seems to be quite high, if the field's characteristic is very small. If one is interested in fields of large characteristic however, it seems to be almost certain that the automorphism group is trivial. From the class number relations we computed, it appears to follow that automorphisms of small order (which ought to be the most probable) are a major threat to the Jacobian's security: $|\mathbb{J}_{F^\sigma}|$ seems to be approximately $\sqrt{|\mathbb{J}_F|}$, if $\mathrm{ord}(\sigma)$ is small. Of course, this is what is to be expected knowing the Hasse-Weil interval.

Note that our proof of Madan's theorem (theorem II.1) delivers insight to major parts of the relation between $|\mathbb{J}_{F^\sigma}|$ and $|\mathbb{J}_F|$. This relation is closely connected to the ramification properties of F/F^σ. Therefore, it would be interesting to investigate the theory of this relation in more detail, hopefully resulting in explicit formulas for $\frac{|\mathbb{J}_F|}{|\mathbb{J}_{F^\sigma}|}$.

Our experimental results imply that our cryptographic goal can be partially fulfilled: For hyperelliptic function fields of large characteristic, it seems unlikely to find non-trivial automorphisms. Hence, sorting out insecure Jacobians over large characteristic by computing automorphism groups will most probably not be successful. On the other hand, it appears to be quite probable to find automorphisms of fields of small characteristic. Furthermore, they seem to yield subgroups of Jacobians, which destroy security. Thus, for hyperelliptic curves of small characteristic, computing automorphism groups is a promising idea to identify insecure Jacobians.

[18] cf. chapter VI, the appendix and [**Göb03b**]

APPENDIX A

Function Fields with Nontrivial Automorphism Groups

1. All Imaginary Quadratic Hyperelliptic Fields of Genus 2 over $\mathbb{F}_3$

Defining Equation of $F = \mathbb{F}_3(t, u)$	$\mathrm{Aut}(F\overline{\mathbb{F}}_3/\overline{\mathbb{F}}_3)/\langle\Phi\rangle$
$u^2 = t^5 + 1$	$\mathcal{C}_5$
$u^2 = t^5 + t$	$\mathcal{S}_4$
$u^2 = t^5 + t^2 + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^3 + 1$	$\mathcal{C}_5$
$u^2 = t^5 + t^3 + t^2 + 2t$	$\mathcal{D}_3$
$u^2 = t^5 + t^3 + 2$	$\mathcal{C}_5$
$u^2 = t^5 + t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 2t^2 + 2t$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 2t^2 + 1$	$\mathcal{S}_4$
$u^2 = t^5 + t^4 + t^3 + 2t^2 + t$	$\mathcal{S}_4$
$u^2 = t^5 + t^4 + t^3 + 2t^2 + 2t$	$\mathcal{C}_5$
$u^2 = t^5 + t^4 + t^3 + 2t^2 + 2t + 1$	$\mathcal{C}_5$
$u^2 = t^5 + t^4 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^2 + t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + t^4 + 2t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + t^2 + 1$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 2t^3 + 2t$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 2t^3 + 2t^2 + t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + t^4 + 2t^3 + 2t^2 + 2t$	$\mathcal{C}_5$
$u^2 = t^5 + t^4 + 2t^3 + 2t^2 + 2t + 2$	$\mathcal{C}_5$
$u^2 = t^5 + 2$	$\mathcal{C}_5$
$u^2 = t^5 + 2t$	$\mathcal{S}_4$
$u^2 = t^5 + 2t^2 + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^3 + t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^3 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^3 + 2t^2 + t + 2$	$\mathcal{C}_2$

Table 1: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_3$ with non-trivial automorphism groups over $\overline{\mathbb{F}_3}$ *(continued)*

Defining Equation of $F = \mathbb{F}_3(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_3}/\overline{\mathbb{F}_3})/\langle\Phi\rangle$
$u^2 = t^5 + 2t^4 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^2 + t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^4 + t^3 + t^2 + t$	$\mathcal{S}_4$
$u^2 = t^5 + 2t^4 + t^3 + t^2 + 2$	$\mathcal{S}_4$
$u^2 = t^5 + 2t^4 + t^3 + t^2 + 2t$	$\mathcal{C}_5$
$u^2 = t^5 + 2t^4 + t^3 + t^2 + 2t + 2$	$\mathcal{C}_5$
$u^2 = t^5 + 2t^4 + t^3 + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + t^2 + t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + t^2 + 2t$	$\mathcal{C}_5$
$u^2 = t^5 + 2t^4 + 2t^3 + t^2 + 2t + 1$	$\mathcal{C}_5$
$u^2 = t^5 + 2t^4 + 2t^3 + 2t$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 2t^3 + 2t^2 + 2$	$\mathcal{D}_3$

Table 1: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_3$ with non-trivial automorphism groups over $\overline{\mathbb{F}_3}$

2. All Imaginary Quadratic Hyperelliptic Fields of Genus 3 over $\mathbb{F}_3$

Defining Equation of $F = \mathbb{F}_3(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_3}/\overline{\mathbb{F}_3})/\langle\Phi\rangle$
$u^2 = t^7 + 1$	$\mathcal{C}_7$
$u^2 = t^7 + t^3 + t$	$\mathcal{C}_2$
$u^2 = t^7 + t^3 + t^2 + 2t + 1$	$\mathcal{D}_2$
$u^2 = t^7 + t^3 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + t^3 + 2t^2 + 2t + 2$	$\mathcal{D}_2$
$u^2 = t^7 + t^4 + t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^4 + 2t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + t^4 + 2t^3 + 2t^2 + 2t$	$\mathcal{D}_2$
$u^2 = t^7 + t^4 + 2t^3 + 2t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^5 + t$	$\mathcal{C}_2$
$u^2 = t^7 + t^5 + t^3 + t$	$\mathcal{D}_8$
$u^2 = t^7 + t^5 + t^3 + t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^5 + t^3 + t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^5 + t^3 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + t^5 + t^4 + 2t^3 + 2t^2 + 2$	$\mathcal{D}_2$
$u^2 = t^7 + t^5 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + t^5 + 2t^3 + t$	$\mathcal{C}_2$
$u^2 = t^7 + t^5 + 2t^3 + t + 1$	$\mathcal{D}_2$
$u^2 = t^7 + t^5 + 2t^3 + t + 2$	$\mathcal{D}_2$
$u^2 = t^7 + t^5 + 2t^4 + 2$	$\mathcal{C}_2$

Table 2: All imaginary quadratic hyperelliptic function fields of genus 3 over $\mathbb{F}_3$ with non-trivial automorphism groups over $\overline{\mathbb{F}_3}$ *(continued)*

Defining Equation of $F = \mathbb{F}_3(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_3}/\overline{\mathbb{F}_3})/\langle\Phi\rangle$
$u^2 = t^7 + t^5 + 2t^4 + 2t^3 + t^2 + 1$	$\mathcal{D}_2$
$u^2 = t^7 + t^5 + 2t^4 + 2t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^4 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^4 + t^2 + t + 2$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + t^4 + t^3 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^4 + t^3 + 2t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^5 + t^3 + t^2 + t + 2$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + t^5 + t^3 + 2t^2 + t + 2$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + t^5 + t^4 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^5 + t^4 + t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$	$\mathcal{D}_8$
$u^2 = t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^5 + t^4 + 2t^3 + t^2 + t$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + t^5 + t^4 + 2t^3 + t^2 + t + 1$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + t^5 + t^4 + 2t^3 + t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^5 + 2t^3 + t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^5 + 2t^4 + t^2 + 1$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + t^5 + 2t^4 + t^3 + t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + t^5 + 2t^4 + 2t$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + 2t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^3 + 2t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^3 + 2t^2 + 2t + 2$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + 2t^4 + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^4 + t^2 + 2t$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + 2t^4 + t^3 + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^4 + t^3 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^4 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^4 + 2t^2 + t + 2$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + 2t^4 + 2t^3 + t$	$\mathcal{C}_7$
$u^2 = t^7 + t^6 + 2t^4 + 2t^3 + t + 2$	$\mathcal{C}_7$
$u^2 = t^7 + t^6 + 2t^5 + t^3 + 2t^2 + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + t^3 + 2t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + t^4 + t^3 + t + 2$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + 2t^5 + t^4 + t^3 + t^2 + t$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + 2t^5 + t^4 + t^3 + t^2 + 2t$	$\mathcal{D}_4$
$u^2 = t^7 + t^6 + 2t^5 + t^4 + t^3 + 2t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + t^4 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + t^4 + 2t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + t^4 + 2t^3 + t^2 + 2t + 1$	$\mathcal{C}_7$
$u^2 = t^7 + t^6 + 2t^5 + 2t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + 2t^3 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + 2t^3 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + 2t^3 + 2t^2 + t$	$\mathcal{D}_8$

Table 2: All imaginary quadratic hyperelliptic function fields of genus 3 over $\mathbb{F}_3$ with non-trivial automorphism groups over $\overline{\mathbb{F}_3}$ *(continued)*

Defining Equation of $F = \mathbb{F}_3(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_3}/\overline{\mathbb{F}_3})/\langle\Phi\rangle$
$u^2 = t^7 + t^6 + 2t^5 + 2t^3 + 2t^2 + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + 2t^4 + t + 1$	$\mathcal{C}_7$
$u^2 = t^7 + t^6 + 2t^5 + 2t^4 + t^3 + t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + 2t^4 + t^3 + 2t^2 + 2$	$\mathcal{C}_2$
$u^2 = t^7 + t^6 + 2t^5 + 2t^4 + 2t^3 + 1$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + 2t^5 + 2t^4 + 2t^3 + t$	$\mathcal{D}_4$
$u^2 = t^7 + t^6 + 2t^5 + 2t^4 + 2t^3 + t^2 + t$	$\mathcal{D}_2$
$u^2 = t^7 + t^6 + 2t^5 + 2t^4 + 2t^3 + 2t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2$	$\mathcal{C}_7$
$u^2 = t^7 + 2t^3 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^4 + t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^4 + 2t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^4 + 2t^3 + t^2 + 2t$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^4 + 2t^3 + t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + t^3 + t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + t^3 + t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + t^3 + 2t$	$\mathcal{D}_8$
$u^2 = t^7 + 2t^5 + t^3 + 2t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + t^4 + t^3 + t^2 + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + t^4 + t^3 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + t^4 + 2t^2 + t$	$\mathcal{C}_7$
$u^2 = t^7 + 2t^5 + t^4 + 2t^3 + t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + t^4 + 2t^3 + 2t^2 + 1$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^5 + t^4 + 2t^3 + 2t^2 + t$	$\mathcal{D}_4$
$u^2 = t^7 + 2t^5 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + 2t^4 + t^2 + t$	$\mathcal{C}_7$
$u^2 = t^7 + 2t^5 + 2t^4 + t^3 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + 2t^4 + t^3 + 2t^2 + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + 2t^4 + 2t^3 + t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^5 + 2t^4 + 2t^3 + t^2 + t$	$\mathcal{D}_4$
$u^2 = t^7 + 2t^5 + 2t^4 + 2t^3 + t^2 + 2$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^5 + 2t^4 + 2t^3 + 2t^2 + 2t + 1$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^4 + t^2 + t + 1$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + t^4 + t^3 + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^4 + t^3 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^4 + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^4 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^4 + 2t^2 + 2t$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + t^4 + 2t^3 + t$	$\mathcal{C}_7$
$u^2 = t^7 + 2t^6 + t^4 + 2t^3 + t + 1$	$\mathcal{C}_7$
$u^2 = t^7 + 2t^6 + t^5 + t^3 + t^2 + t + 1$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + t^5 + t^3 + 2t^2 + t + 1$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + t^5 + t^4 + t^3 + 2t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^5 + t^4 + 2t^2 + 2$	$\mathcal{D}_2$

Table 2: All imaginary quadratic hyperelliptic function fields of genus 3 over $\mathbb{F}_3$ with non-trivial automorphism groups over $\overline{\mathbb{F}_3}$ *(continued)*

Defining Equation of $F = \mathbb{F}_3(t, u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_3}/\overline{\mathbb{F}_3})/\langle\Phi\rangle$
$u^2 = t^7 + 2t^6 + t^5 + 2t^3 + 2t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^5 + 2t^4 + t^3 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^5 + 2t^4 + t^3 + 2t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^5 + 2t^4 + t^3 + 2t^2 + t + 2$	$\mathcal{D}_8$
$u^2 = t^7 + 2t^6 + t^5 + 2t^4 + t^3 + 2t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^5 + 2t^4 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^5 + 2t^4 + 2t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^5 + 2t^4 + 2t^3 + 2t^2 + t$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + t^5 + 2t^4 + 2t^3 + 2t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + t^5 + 2t^4 + 2t^3 + 2t^2 + t + 2$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + 2t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^3 + t^2 + 2t + 1$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + 2t^3 + t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^4 + t^3 + t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^4 + t^3 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^4 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^4 + 2t^2 + t + 1$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + t^3 + t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + t^3 + t^2 + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + t^4 + t + 2$	$\mathcal{C}_7$
$u^2 = t^7 + 2t^6 + 2t^5 + t^4 + t^3 + t^2 + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + t^4 + t^3 + 2t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + t^4 + 2t^3 + t$	$\mathcal{D}_4$
$u^2 = t^7 + 2t^6 + 2t^5 + t^4 + 2t^3 + t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + t^4 + 2t^3 + 2$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + t^4 + 2t^3 + 2t^2 + t$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + 2t^3 + t^2 + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + 2t^3 + t^2 + t$	$\mathcal{D}_8$
$u^2 = t^7 + 2t^6 + 2t^5 + 2t^3 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + 2t^4 + t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + 2t^4 + t^3 + t + 1$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + 2t^4 + t^3 + t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + 2t^4 + t^3 + 2t^2 + t$	$\mathcal{D}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + 2t^4 + t^3 + 2t^2 + 2t$	$\mathcal{D}_4$
$u^2 = t^7 + 2t^6 + 2t^5 + 2t^4 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^7 + 2t^6 + 2t^5 + 2t^4 + 2t^3 + 2t^2 + 2t + 2$	$\mathcal{C}_7$

Table 2: All imaginary quadratic hyperelliptic function fields of genus 3 over $\mathbb{F}_3$ with non-trivial automorphism groups over $\overline{\mathbb{F}_3}$

3. All Imaginary Quadratic Hyperelliptic Fields of Genus 2 over $\mathbb{F}_5$

Defining Equation of $F = \mathbb{F}_5(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_5}/\overline{\mathbb{F}_5})/\langle\Phi\rangle$
$u^2 = t^5 + t$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + t + 1$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + t + 2$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + t + 3$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + t + 4$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + t^3 + t$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + t^2 + 1$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + t^2 + 3t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + t^2 + 4t + 4$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 2t^2 + 1$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 2t^2 + t$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 2t^2 + 4t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 3t$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 3t^2 + t$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 3t^2 + 4$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 3t^2 + 4t + 3$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 4t^2 + 3t + 3$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 4t^2 + 4$	$\mathcal{D}_2$
$u^2 = t^5 + t^3 + 4t^2 + 4t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + t^4 + t^2 + 3t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^2 + 4$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + t^2 + 3t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^5 + t^4 + t^3 + 2t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 2t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 3t^2 + t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 3t^2 + t + 4$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + t^3 + 3t^2 + 3t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 3t^2 + 3t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 3t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 4t + 2$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + t^3 + 4t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 4t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 4t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 4t^2 + 3t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + t^3 + 4t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^2 + 4t + 1$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 2t^3 + t^2 + t$	$\mathcal{C}_2$

Table 3: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_5$ with non-trivial automorphism groups over $\overline{\mathbb{F}_5}$ *(continued)*

Defining Equation of $F = \mathbb{F}_5(t, u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_5}/\overline{\mathbb{F}_5})/\langle\Phi\rangle$
$u^2 = t^5 + t^4 + 2t^3 + t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + t^2 + 2t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 2t^3 + t^2 + 4t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + 2t^2 + 2t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + 2t^2 + 2t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + 2t^2 + 4$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 2t^3 + 2t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + 3t^2 + t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + t^4 + 2t^3 + 3t^2 + 3t + 2$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 2t^3 + 3t^2 + 3t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + 3t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + 4t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 2t^3 + 4t^2 + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^2 + t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^2 + 3t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^2 + 4t + 1$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 3t^3 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + t^2 + t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 3t^3 + t^2 + 4t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + 2t^2 + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + 2t^2 + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + 2t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + 2t^2 + 3t + 4$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 3t^3 + 3t^2 + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + 3t^2 + 2t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + t^4 + 3t^3 + 3t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 3t^3 + 3t^2 + 4t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + 4t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 3t^3 + 4t^2 + 4t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^2 + t + 4$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 4t^2 + 2t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^2 + 4t$	$\mathcal{D}_2$
$u^2 = t^5 + t^4 + 4t^3 + t$	$\mathcal{D}_2$
$u^2 = t^5 + t^4 + 4t^3 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 2t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 2t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 3t + 1$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 4t^3 + 3t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 3t^2 + 1$	$\mathcal{C}_2$

Table 3: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_5$ with non-trivial automorphism groups over $\overline{\mathbb{F}_5}$ *(continued)*

Defining Equation of $F = \mathbb{F}_5(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_5}/\overline{\mathbb{F}_5})/\langle\Phi\rangle$
$u^2 = t^5 + t^4 + 4t^3 + 3t^2 + 2t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 3t^2 + 2t + 4$	$\mathcal{D}_3$
$u^2 = t^5 + t^4 + 4t^3 + 3t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 3t^2 + 4t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 4t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 4t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 4t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 4t^2 + 3t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + t^4 + 4t^3 + 4t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 2t$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 2t + 1$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 2t + 2$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 2t + 3$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 2t + 4$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 2t^3 + t^2 + 2$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + t^2 + 3t$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + t^2 + 4t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 2t^2 + t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 2t^2 + 2t + 4$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 2t^2 + 3t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 3t$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 3t^2 + t + 3$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 3t^2 + 2t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 3t^2 + 3t + 4$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 4t$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 4t^2 + 3$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 4t^2 + 3t$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^3 + 4t^2 + 4t + 4$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^4 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^2 + t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^2 + 4t + 2$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + t^3 + t$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^4 + t^3 + t^2 + t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + 2t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + 2t^2 + 3t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + 2t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + t^3 + 3t + 2$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + t^3 + 3t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + 3t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + 4t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + 4t^2 + 2$	$\mathcal{C}_2$

Table 3: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_5$ with non-trivial automorphism groups over $\overline{\mathbb{F}_5}$ *(continued)*

Defining Equation of $F = \mathbb{F}_5(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_5}/\overline{\mathbb{F}_5})/\langle\Phi\rangle$
$u^2 = t^5 + 2t^4 + t^3 + 4t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + 4t^2 + 2t + 3$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + t^3 + 4t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + t^3 + 4t^2 + 4t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^2 + t + 3$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 2t^2 + 2t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^2 + 4t$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + t^2 + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + t^2 + 3t + 3$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 2t^3 + t^2 + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + 2t^2 + 4t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + 3t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + 3t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + 3t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + 3t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 2t^3 + 3t^2 + 4t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + 4t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + 4t^2 + 2t + 4$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + 4t^2 + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 2t^3 + 4t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 2t^3 + 4t^2 + 4t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^2 + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^2 + 3t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + t^2 + 2t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + t^2 + 3$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 3t^3 + t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + 2t^2 + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + 3t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + 3t^2 + t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + 3t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + 3t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 3t^3 + 3t^2 + 4t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + 4t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + 4t^2 + t + 4$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + 4t^2 + 3t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 3t^3 + 4t^2 + 3t + 4$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 3t^3 + 4t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^2 + t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^2 + 3t$	$\mathcal{C}_2$

Table 3: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_5$ with non-trivial automorphism groups over $\overline{\mathbb{F}_5}$ *(continued)*

Defining Equation of $F = \mathbb{F}_5(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_5}/\overline{\mathbb{F}_5})/\langle\Phi\rangle$
$u^2 = t^5 + 2t^4 + 4t^2 + 4t + 2$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 4t^3 + t^2 + 2t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 2t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 2t^2 + t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 2t^2 + 3t$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 2t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 4t^3 + 3t^2 + 3t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 4t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 4t + 4$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 4t^3 + 4t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 4t^2 + t + 3$	$\mathcal{D}_3$
$u^2 = t^5 + 2t^4 + 4t^3 + 4t^2 + 3t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 4t^2 + 3t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 2t^4 + 4t^3 + 4t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 3t + 1$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 3t + 2$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 3t + 3$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 3t + 4$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 3t^3 + t^2 + t + 4$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + t^2 + 2t + 3$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + t^2 + 3t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 2t^2 + 1$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 2t^2 + 3t$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 2t^2 + 4t + 3$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 3t$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 3t^2 + 3t$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 3t^2 + 4$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 3t^2 + 4t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 4t$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 4t^2 + t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 4t^2 + 2t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^3 + 4t^2 + 3t + 3$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^4 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^2 + 3t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^2 + 4t + 3$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + t^3 + t$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^4 + t^3 + t^2 + 2t + 2$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + t^3 + t^2 + 2t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^3 + t^2 + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^3 + t^2 + 4t$	$\mathcal{C}_2$

Table 3: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_5$ with non-trivial automorphism groups over $\overline{\mathbb{F}_5}$ *(continued)*

Defining Equation of $F = \mathbb{F}_5(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_5}/\overline{\mathbb{F}_5})/\langle\Phi\rangle$
$u^2 = t^5 + 3t^4 + t^3 + t^2 + 4t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^3 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^3 + 3t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^3 + 3t + 3$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + t^3 + 3t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^3 + 3t^2 + t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^3 + 3t^2 + 3t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^3 + 3t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + t^3 + 4t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^3 + 4t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + t^3 + 4t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^2 + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^2 + 3t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + t^2 + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + t^2 + 2t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 2t^3 + t^2 + 4t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + 2t^2 + t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + 2t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + 2t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 2t^3 + 2t^2 + 4t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + 3t^2 + 4t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + 4t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + 4t^2 + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + 4t^2 + 2t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + 4t^2 + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 2t^3 + 4t^2 + 3t + 2$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 3t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^2 + t + 2$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 3t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^2 + 4t$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + t^2 + t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + t^2 + 3t + 1$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 3t^3 + t^2 + 3t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + 2t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + 2t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + 2t^2 + 2t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + 2t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 3t^3 + 2t^2 + 4t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + 3t^2 + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + 4t + 1$	$\mathcal{C}_2$

Table 3: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_5$ with non-trivial automorphism groups over $\overline{\mathbb{F}_5}$ *(continued)*

Defining Equation of $F = \mathbb{F}_5(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_5}/\overline{\mathbb{F}_5})/\langle\Phi\rangle$
$u^2 = t^5 + 3t^4 + 3t^3 + 4t^2 + 2$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 3t^3 + 4t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + 4t^2 + 2t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 3t^3 + 4t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^2 + 4t + 3$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 4t^3 + t^2 + t + 2$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 4t^3 + t^2 + t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + t^2 + 3t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + t^2 + 3t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + 2t^2 + 3t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + 3t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + 3t^2 + t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + 3t^2 + 3t$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + 3t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 4t^3 + 4t + 1$	$\mathcal{D}_3$
$u^2 = t^5 + 3t^4 + 4t^3 + 4t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + 4t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 3t^4 + 4t^3 + 4t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 4t + 1$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 4t + 2$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 4t + 3$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 4t + 4$	$\mathrm{PGL}_2(5)$
$u^2 = t^5 + 4t^3 + t$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + t^2 + t$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + t^2 + 2$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + t^2 + 4t + 4$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 2t^2 + 3$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 2t^2 + 3t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 2t^2 + 4t + 2$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 3t$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 3t^2 + 2$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 3t^2 + 3t + 4$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 3t^2 + 4t + 3$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 4t^2 + t$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 4t^2 + 3$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^3 + 4t^2 + 4t + 1$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^4 + t^2 + t$	$\mathcal{C}_2$

Table 3: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_5$ with non-trivial automorphism groups over $\overline{\mathbb{F}_5}$ *(continued)*

Defining Equation of $F = \mathbb{F}_5(t,u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_5}/\overline{\mathbb{F}_5})/\langle\Phi\rangle$
$u^2 = t^5 + 4t^4 + t^2 + t + 1$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^2 + 4t$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^4 + t^3 + t^2 + t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + t^2 + t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + t^2 + 3t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + t^3 + 2t$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^4 + t^3 + 2t^2 + t + 1$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + t^3 + 2t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + 2t^2 + 3t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + 2t^2 + 3t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + 2t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + 3t^2 + 2t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + 3t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + 4t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + t^3 + 4t + 3$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + t^3 + 4t^2 + 3t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^2 + t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^2 + 3t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^2 + 4t + 4$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 2t^3 + t^2 + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 2t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 2t^2 + t + 3$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 2t^2 + 3t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 2t^2 + 3t + 3$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 2t^3 + 2t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 3t^2 + 1$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 2t^3 + 3t^2 + 2t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 3t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 3t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 4t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 4t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 4t^2 + t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 4t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 2t^3 + 4t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 2t^3 + 4t^2 + 4t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^2 + t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^2 + 4t + 4$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 3t^3 + t + 4$	$\mathcal{C}_2$

Table 3: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_5$ with non-trivial automorphism groups over $\overline{\mathbb{F}_5}$ *(continued)*

Defining Equation of $F = \mathbb{F}_5(t, u)$	$\mathrm{Aut}(F\overline{\mathbb{F}_5}/\overline{\mathbb{F}_5})/\langle\Phi\rangle$
$u^2 = t^5 + 4t^4 + 3t^3 + t^2 + 4t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 2t^2 + 2t + 3$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 2t^2 + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 2t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 3t^3 + 2t^2 + 4t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 3t^2 + 2t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 3t^2 + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 3t^2 + 3t + 1$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 3t^3 + 3t^2 + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 4t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 4t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 4t^2 + t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 4t^2 + 2t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 3t^3 + 4t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 3t^3 + 4t^2 + 4t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^2 + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^2 + 3t + 1$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + t$	$\mathcal{D}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + t^2 + t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + t^2 + t + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + t^2 + 3t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + t^2 + 4t$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 4t^3 + 2t^2 + 2t + 1$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 4t^3 + 2t^2 + 2t + 2$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + 2t^2 + 4$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + 2t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + 2t^2 + 4t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + 3t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + 3t + 4$	$\mathcal{D}_3$
$u^2 = t^5 + 4t^4 + 4t^3 + 3t^2 + t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + 3t^2 + 4t$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + 4t + 3$	$\mathcal{C}_2$
$u^2 = t^5 + 4t^4 + 4t^3 + 4t^2 + t$	$\mathcal{C}_2$

Table 3: All imaginary quadratic hyperelliptic function fields of genus 2 over $\mathbb{F}_5$ with non-trivial automorphism groups over $\overline{\mathbb{F}_5}$

4. Random Hyperelliptic Fields of Genus 3

We computed the reduced automorphism group $\mathrm{Aut}(F\overline{k}/\overline{k})/\langle\Phi\rangle$ of 10000 random genus 3 hyperelliptic fields of small characteristic $3 \leq p \leq 257$, as well as of 10000 random genus 3 hyperelliptic fields of large[1] characteristic $16411 \leq p \leq 32003$. All of the fields of large characteristic had trivial automorphism group, while we found the 15 fields listed in table 4 to have non-trivial automorphism groups. The complete list of examples can be found in [**Göb03b**].

[1] Because the characteristic of a field is restricted to be ≤ 32003 in Singular ([**GPS$^+$02**]), this is the largest characteristic achievable with our implementation of algorithm V.4.

k	Defining Equation of $F = \mathbb{F}_5(t,u)$	$\mathrm{Aut}(F\overline{k}/\overline{k})/\langle\Phi\rangle$	Time
$\mathbb{F}_3$	$u^2 = t^7 + t^6 + t^4 + t^3 + t^2 + t$	$\mathcal{C}_2$	22.6
$\mathbb{F}_3$	$u^2 = t^7 + 2t^5 + t^4 + t^3 + 2t$	$\mathcal{C}_2$	26.9
$\mathbb{F}_3$	$u^2 = t^8 + t^5 + 2t^4 + t^3 + t^2 + 2$	$\mathcal{C}_2$	21.0
$\mathbb{F}_3$	$u^2 = t^8 + t^7 + 2t^5 + 2t + 2$	$\mathcal{D}_2$	24.9
$\mathbb{F}_5$	$u^2 = t^8 + t^6 + 3t^2 + t$	$\mathcal{C}_2$	20.4
$\mathbb{F}_5$	$u^2 = t^8 + 4t^7 + 4t^6 + t^3 + t$	$\mathcal{C}_2$	27.9
$\mathbb{F}_7$	$u^2 = t^7 + 6t^4 + 4t^3 + t^2 + 2$	$\mathcal{D}_3$	36.8
$\mathbb{F}_{11}$	$u^2 = t^7 + 4t^6 + 10t^5 + 6t^3 + 9$	$\mathcal{C}_2$	57.2
$\mathbb{F}_{11}$	$u^2 = t^7 + 9t^5 + 10t^4 + 8t^3 + 5t^2 + 6t$	$\mathcal{C}_2$	51.4
$\mathbb{F}_{13}$	$u^2 = t^7 + 12t^6 + t^5 + 10t^3 + 3t^2 + 7t + 4$	$\mathcal{C}_2$	60.5
$\mathbb{F}_{17}$	$u^2 = t^8 + 8t^5 + 5t^4 + 10t^3 + 14t + 12$	$\mathcal{C}_2$	35.4
$\mathbb{F}_{19}$	$u^2 = t^7 + 8t^6 + 8t^5 + 18t^4 + 18t^3 + 8t + 1$	$\mathcal{C}_2$	63.6
$\mathbb{F}_{37}$	$u^2 = t^8 + 24t^6 + 3t^5 + 5t^4 + 19t^3 + 13t^2 + 1$	$\mathcal{C}_2$	44.9
$\mathbb{F}_{41}$	$u^2 = t^8 + 5t^7 + 22t^5 + 38t^4 + 36t^3 + 28t^2 + 29$	$\mathcal{C}_2$	60.9
$\mathbb{F}_{89}$	$u^2 = t^7 + 16t^5 + 10t^4 + 37t^3 + 37t^2 + 63t + 8$	$\mathcal{C}_2$	64.6

Table 4: Genus-3 hyperelliptic function fields $F = k(t,u)$ with non-trivial automorphism group over $\overline{k}$, together with the running times of algorithm V.4 on an Intel® Celeron®, 1.7 GHz, in seconds

5. Random Hyperelliptic Fields of Genus 4

We computed the reduced automorphism group $\mathrm{Aut}(F\overline{k}/\overline{k})/\langle\Phi\rangle$ of 6900 random genus 4 hyperelliptic fields of small characteristic $3 \leq p \leq 257$, as well as of 6685 random genus 4 hyperelliptic fields of large[2] characteristic $16411 \leq p \leq 32003$. All of the fields of large characteristic had trivial automorphism group, while we found the 8 fields listed in table 5 to have non-trivial automorphism groups. The complete list of examples can be found in [**Göb03b**].

k	Defining Equation of $F = \mathbb{F}_5(t,u)$	$\mathrm{Aut}(F\overline{k}/\overline{k})/\langle\Phi\rangle$	Time
$\mathbb{F}_3$	$u^2 = t^9 + 2t^3 + t + 1$	$\mathcal{C}_3^2 \rtimes \mathcal{C}_2$	23.4
$\mathbb{F}_3$	$u^2 = t^9 + 2t^3 + t + 2$	$\mathcal{C}_3^2 \rtimes \mathcal{C}_2$	22.9
$\mathbb{F}_3$	$u^2 = t^9 + 2t^7 + 2t^3 + 2t$	$\mathcal{D}_2$	34.7
$\mathbb{F}_5$	$u^2 = t^9 + 2t^7 + t^5 + 3t^3 + 2t$	$\mathcal{C}_2$	62.6
$\mathbb{F}_5$	$u^2 = t^{10} + t^6 + 3t^5 + t^4 + 4t^3 + t^2 + 4$	$\mathcal{D}_2$	114.2
$\mathbb{F}_5$	$u^2 = t^{10} + t^8 + 3t^6 + 4t^2 + 4$	$\mathcal{C}_2$	53.1
$\mathbb{F}_5$	$u^2 = t^{10} + 2t^9 + 3t^6 + t^4 + 2t + 2$	$\mathcal{C}_2$	327.7
$\mathbb{F}_7$	$u^2 = t^{10} + t^8 + 5t^7 + t^5 + 4t^4 + 2t$	$\mathcal{C}_2$	1141.6

Table 5: Genus-4 hyperelliptic function fields $F = k(t,u)$ with non-trivial automorphism group over $\overline{k}$, together with the running times of algorithm V.4 on an Intel® Celeron®, 1.7 GHz, in seconds

[2] 32003 is the largest possible characteristic, see footnote 1 above.

APPENDIX B

Jacobian Orders of Subfields

1. Fixed Fields of $\mathcal{C}_n$, where $(n, \mathrm{char}(k)) = 1$ and $\nu = 0$

k	s	a_j	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_2}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_2}}\rvert}$
$\mathbb{F}_5$	3	1, 3, 4	32	4	8
$\mathbb{F}_5$	3	2, 3, 4	64	8	8
$\mathbb{F}_7$	5	1, 2, 3, 4, 5	2304	48	48
$\mathbb{F}_7$	5	2, 3, 4, 5, 6	2304	48	48
$\mathbb{F}_{11}$	5	1, 3, 8, 9, 10	19712	112	176
$\mathbb{F}_{11}$	4	1, 4, 7, 10	1152	8	144
$\mathbb{F}_{11}$	3	2, 4, 5	96	8	12
$\mathbb{F}_{11}$	5	3, 6, 8, 9, 10	22528	176	128
$\mathbb{F}_{11}$	4	4, 5, 8, 9	2048	16	128
$\mathbb{F}_{11}$	3	5, 8, 10	128	8	16
$\mathbb{F}_{13}$	3	3, 5, 12	144	12	12
$\mathbb{F}_{13}$	5	3, 6, 7, 11, 12	30976	176	176
$\mathbb{F}_{13}$	5	3, 7, 9, 10, 11	30976	176	176
$\mathbb{F}_{13}$	5	4, 7, 9, 10, 12	28160	176	160
$\mathbb{F}_{17}$	5	1, 2, 7, 12, 16	110592	384	288
$\mathbb{F}_{17}$	3	1, 6, 9	400	20	20
$\mathbb{F}_{17}$	3	1, 6, 14	384	24	16
$\mathbb{F}_{17}$	4	3, 4, 6, 10	3584	16	224
$\mathbb{F}_{17}$	5	3, 4, 11, 15, 16	88320	240	368
$\mathbb{F}_{17}$	5	3, 8, 13, 14, 16	147456	384	384
$\mathbb{F}_{17}$	3	4, 5, 16	288	12	24
$\mathbb{F}_{17}$	4	4, 12, 14, 15	7296	24	304
$\mathbb{F}_{17}$	5	5, 6, 7, 8, 11	87552	288	304
$\mathbb{F}_{17}$	6	5, 6, 7, 11, 14, 15	1566720	272	5760
$\mathbb{F}_{17}$	3	5, 7, 13	384	16	24
$\mathbb{F}_{17}$	4	7, 10, 13, 14	4416	12	368
$\mathbb{F}_{17}$	4	10, 11, 13, 14	3840	16	240
$\mathbb{F}_{19}$	4	3, 13, 16, 18	5568	12	464
$\mathbb{F}_{19}$	3	8, 10, 16	672	24	28
$\mathbb{F}_{19}$	4	9, 10, 11, 14	8448	24	352
$\mathbb{F}_{23}$	4	2, 5, 6, 18	20480	32	640
$\mathbb{F}_{23}$	3	3, 8, 13	576	24	24

Table 1: Jacobian orders of hyperelliptic function fields $F = k(t, u)$ of the form $u^2 = \prod_{j=0}^{s-1}(t^2 - a_j)$ and of their fixed fields $F^{\mathcal{C}_2} = k(t^2, u)$. Because some defining equations would be too large to fit in a single line, we only list the parameters s and a_j. *(continued)*

k	s	a_j	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_2}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_2}}\rvert}$
$\mathbb{F}_{23}$	4	4, 10, 14, 16	15232	28	544
$\mathbb{F}_{23}$	4	6, 7, 9, 11	17920	32	560
$\mathbb{F}_{23}$	3	6, 7, 10	384	16	24
$\mathbb{F}_{23}$	6	8, 10, 14, 15, 16, 19	5541888	528	10496
$\mathbb{F}_{23}$	3	10, 13, 20	768	24	32
$\mathbb{F}_{29}$	3	4, 14, 26	1296	36	36
$\mathbb{F}_{29}$	3	7, 20, 23	960	40	24
$\mathbb{F}_{29}$	3	8, 10, 24	1296	36	36
$\mathbb{F}_{29}$	4	9, 16, 19, 26	20480	32	640
$\mathbb{F}_{29}$	4	10, 11, 19, 27	17280	24	720
$\mathbb{F}_{29}$	3	10, 17, 25	896	28	32
$\mathbb{F}_{29}$	4	12, 14, 18, 19	31360	40	784
$\mathbb{F}_{31}$	5	4, 8, 16, 17, 22	952576	976	976
$\mathbb{F}_{31}$	6	6, 8, 17, 18, 23, 27	33516544	1136	29504
$\mathbb{F}_{37}$	4	1, 13, 33, 35	56448	36	1568
$\mathbb{F}_{37}$	4	2, 4, 8, 12	76032	48	1584
$\mathbb{F}_{37}$	4	3, 13, 14, 30	58368	48	1216
$\mathbb{F}_{37}$	3	3, 13, 30	1760	40	44
$\mathbb{F}_{37}$	3	4, 6, 36	896	28	32
$\mathbb{F}_{37}$	5	4, 8, 12, 27, 34	2045440	1360	1504
$\mathbb{F}_{37}$	3	5, 7, 14	1280	32	40
$\mathbb{F}_{37}$	4	5, 7, 14, 17	38400	32	1200
$\mathbb{F}_{37}$	3	5, 12, 30	1280	40	32
$\mathbb{F}_{37}$	4	9, 21, 24, 26	51264	36	1424
$\mathbb{F}_{37}$	4	10, 13, 21, 34	55808	32	1744
$\mathbb{F}_{37}$	4	10, 32, 34, 36	50112	36	1392
$\mathbb{F}_{37}$	3	11, 20, 32	1728	48	36
$\mathbb{F}_{37}$	4	14, 15, 23, 32	62080	40	1552
$\mathbb{F}_{37}$	4	18, 19, 25, 33	39744	36	1104
$\mathbb{F}_{41}$	4	1, 16, 22, 26	90688	52	1744
$\mathbb{F}_{41}$	4	3, 11, 12, 25	86528	52	1664
$\mathbb{F}_{41}$	3	4, 6, 33	2112	44	48
$\mathbb{F}_{41}$	3	5, 6, 25	1440	40	36
$\mathbb{F}_{41}$	4	7, 19, 33, 34	55296	32	1728
$\mathbb{F}_{41}$	6	8, 25, 29, 31, 32, 39	152678400	2272	67200
$\mathbb{F}_{41}$	4	12, 16, 38, 39	55680	40	1392
$\mathbb{F}_{41}$	3	15, 23, 40	1920	40	48
$\mathbb{F}_{43}$	5	4, 7, 28, 30, 35	3512320	2240	1568
$\mathbb{F}_{43}$	4	7, 24, 36, 39	72960	48	1520
$\mathbb{F}_{43}$	3	7, 36, 39	1152	32	36
$\mathbb{F}_{43}$	3	9, 28, 35	2112	48	44
$\mathbb{F}_{43}$	3	14, 18, 32	1440	36	40
$\mathbb{F}_{43}$	3	23, 30, 38	2496	52	48
$\mathbb{F}_{47}$	5	3, 18, 20, 35, 43	6451200	2880	2240

Table 1: Jacobian orders of hyperelliptic function fields $F = k(t, u)$ of the form $u^2 = \prod_{j=0}^{s-1}(t^2 - a_j)$ and of their fixed fields $F^{\mathcal{C}_2} = k(t^2, u)$. Because some defining equations would be too large to fit in a single line, we only list the parameters s and a_j. *(continued)*

k	s	a_j	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_2}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_2}}\rvert}$
$\mathbb{F}_{47}$	3	8, 27, 36	2688	48	56
$\mathbb{F}_{53}$	6	4, 16, 21, 37, 44, 47	402259968	2816	142848
$\mathbb{F}_{53}$	3	9, 30, 49	2640	60	44
$\mathbb{F}_{53}$	6	15, 18, 21, 27, 38, 39	356099072	2416	147392
$\mathbb{F}_{59}$	3	5, 14, 33	2304	48	48
$\mathbb{F}_{59}$	3	20, 48, 50	3072	64	48
$\mathbb{F}_{59}$	3	40, 52, 58	3136	56	56
$\mathbb{F}_{61}$	6	2, 9, 15, 23, 34, 57	679450624	3296	206144
$\mathbb{F}_{67}$	4	3, 8, 42, 59	235648	56	4208
$\mathbb{F}_{67}$	3	4, 41, 48	5472	72	76
$\mathbb{F}_{67}$	3	8, 36, 61	5184	72	72
$\mathbb{F}_{67}$	3	11, 31, 56	4864	64	76
$\mathbb{F}_{67}$	6	14, 46, 54, 56, 60, 62	1589575680	4608	344960
$\mathbb{F}_{67}$	3	28, 31, 57	5120	80	64
$\mathbb{F}_{67}$	3	33, 36, 58	5760	72	80
$\mathbb{F}_{71}$	3	6, 57, 66	6400	80	80
$\mathbb{F}_{71}$	3	8, 14, 70	6048	72	84
$\mathbb{F}_{71}$	4	9, 27, 30, 33	347072	68	5104
$\mathbb{F}_{71}$	3	16, 55, 64	5184	72	72
$\mathbb{F}_{71}$	3	21, 54, 56	5184	72	72
$\mathbb{F}_{71}$	3	28, 43, 60	4608	64	72
$\mathbb{F}_{71}$	3	31, 49, 63	5760	72	80
$\mathbb{F}_{73}$	6	1, 5, 11, 27, 39, 44	2069971968	5424	381632
$\mathbb{F}_{73}$	3	10, 35, 63	5712	68	84
$\mathbb{F}_{79}$	3	1, 13, 72	5760	72	80
$\mathbb{F}_{79}$	6	4, 15, 25, 50, 58, 66	3374530560	6368	529920
$\mathbb{F}_{79}$	3	6, 17, 54	8448	88	96
$\mathbb{F}_{79}$	5	6, 23, 40, 44, 49	37355520	7296	5120
$\mathbb{F}_{79}$	3	6, 29, 70	6336	88	72
$\mathbb{F}_{79}$	4	7, 12, 29, 77	611328	96	6368
$\mathbb{F}_{79}$	5	20, 26, 28, 46, 73	49110016	7712	6368
$\mathbb{F}_{79}$	3	22, 42, 71	7392	88	84
$\mathbb{F}_{79}$	3	26, 27, 43	5440	68	80
$\mathbb{F}_{79}$	3	26, 44, 75	5632	64	88
$\mathbb{F}_{79}$	4	33, 54, 61, 73	473600	80	5920
$\mathbb{F}_{79}$	3	62, 65, 69	6688	88	76
$\mathbb{F}_{83}$	6	1, 5, 12, 16, 46, 69	4198547456	6976	601856
$\mathbb{F}_{83}$	6	1, 8, 26, 27, 59, 78	4009239552	7376	543552
$\mathbb{F}_{83}$	3	3, 34, 48	7680	80	96
$\mathbb{F}_{83}$	3	20, 47, 62	8448	88	96
$\mathbb{F}_{89}$	3	11, 12, 28	6080	80	76
$\mathbb{F}_{89}$	3	20, 78, 88	8448	96	88
$\mathbb{F}_{89}$	4	28, 42, 77, 80	774144	96	8064

Table 1: Jacobian orders of hyperelliptic function fields $F = k(t, u)$ of the form $u^2 = \prod_{j=0}^{s-1}(t^2 - a_j)$ and of their fixed fields $F^{\mathcal{C}_2} = k(t^2, u)$. Because some defining equations would be too large to fit in a single line, we only list the parameters s and a_j. *(continued)*

k	s	a_j	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_2}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_2}}\rvert}$
$\mathbb{F}_{89}$	4	42, 50, 54, 77	724224	92	7872
$\mathbb{F}_{97}$	5	3, 16, 19, 25, 53	84999424	9712	8752
$\mathbb{F}_{97}$	5	3, 26, 39, 83, 94	73516800	8400	8752
$\mathbb{F}_{97}$	5	4, 24, 31, 41, 52	96422400	10800	8928
$\mathbb{F}_{97}$	3	4, 45, 88	7392	84	88
$\mathbb{F}_{97}$	3	5, 10, 22	10800	100	108
$\mathbb{F}_{97}$	5	6, 20, 24, 45, 65	98267136	11632	8448
$\mathbb{F}_{97}$	3	6, 45, 52	8064	84	96
$\mathbb{F}_{97}$	3	7, 10, 33	12096	108	112
$\mathbb{F}_{97}$	3	8, 52, 86	8096	92	88
$\mathbb{F}_{97}$	3	9, 18, 29	9568	104	92
$\mathbb{F}_{97}$	4	10, 14, 17, 91	976768	104	9392
$\mathbb{F}_{97}$	3	12, 74, 81	8064	84	96
$\mathbb{F}_{97}$	3	21, 23, 94	9984	104	96
$\mathbb{F}_{97}$	3	21, 35, 95	7728	84	92
$\mathbb{F}_{97}$	3	25, 48, 64	9072	108	84
$\mathbb{F}_{97}$	3	25, 54, 63	9568	92	104
$\mathbb{F}_{97}$	3	37, 43, 78	11136	96	116
$\mathbb{F}_{97}$	3	61, 65, 78	8400	100	84
$\mathbb{F}_{101}$	5	1, 34, 49, 50, 90	95422720	10160	9392
$\mathbb{F}_{101}$	3	33, 54, 64	11648	104	112

Table 1: Jacobian orders of hyperelliptic function fields $F = k(t, u)$ of the form $u^2 = \prod_{j=0}^{s-1}(t^2 - a_j)$ and of their fixed fields $F^{\mathcal{C}_2} = k(t^2, u)$. Because some defining equations would be too large to fit in a single line, we only list the parameters s and a_j.

k	Defining Equation of $F = k(t, u)$	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_3}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_3}}\rvert}$
$\mathbb{F}_7$	$u^2 = (t^3 - 1)(t^3 - 2)(t^3 - 4)(t^3 - 6)$	19968	8	2496
$\mathbb{F}_7$	$u^2 = (t^3 - 1)(t^3 - 3)(t^3 - 4)$	5328	12	444
$\mathbb{F}_7$	$u^2 = (t^3 - 2)(t^3 - 3)(t^3 - 4)$	2904	8	363
$\mathbb{F}_7$	$u^2 = (t^3 - 2)(t^3 - 3)(t^3 - 4)(t^3 - 5)$	16200	8	2025
$\mathbb{F}_{13}$	$u^2 = (t^3 - 2)(t^3 - 3)(t^3 - 10)$	19764	12	1647
$\mathbb{F}_{13}$	$u^2 = (t^3 - 2)(t^3 - 5)(t^3 - 12)$	18816	8	2352
$\mathbb{F}_{31}$	$u^2 = (t^3 - 13)(t^3 - 14)(t^3 - 16)$	1288656	36	35796
$\mathbb{F}_{37}$	$u^2 = (t^3 - 2)(t^3 - 9)(t^3 - 22)$	2072412	36	57567
$\mathbb{F}_{37}$	$u^2 = (t^3 - 9)(t^3 - 11)(t^3 - 19)(t^3 - 23)$	64659456	32	2020608
$\mathbb{F}_{97}$	$u^2 = (t^3 - 15)(t^3 - 65)(t^3 - 77)$	81870336	96	852816

Table 2: Jacobian orders of hyperelliptic function fields $F = k(t, u)$ of the form $u^2 = \prod_{j=0}^{s-1}(t^3 - a_j)$ and of their fixed fields $F^{\mathcal{C}_3} = k(t^3, u)$

k	Defining Equation of $F = k(t,u)$	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_4}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_4}}\rvert}$
$\mathbb{F}_5$	$u^2 = (t^4-1)(t^4-2)(t^4-3)$	5120	8	640
$\mathbb{F}_5$	$u^2 = (t^4-1)(t^4-2)(t^4-4)$	4096	4	1024
$\mathbb{F}_{29}$	$u^2 = (t^4-18)(t^4-24)(t^4-26)$	12729600	36	353600
$\mathbb{F}_{37}$	$u^2 = (t^4-23)(t^4-34)(t^4-36)$	88657920	36	2462720
$\mathbb{F}_{53}$	$u^2 = (t^4-16)(t^4-23)(t^4-49)$	400717824	52	7706112
$\mathbb{F}_{53}$	$u^2 = (t^4-18)(t^4-34)(t^4-50)$	212808960	40	5320224
$\mathbb{F}_{53}$	$u^2 = (t^4-35)(t^4-37)(t^4-47)$	317611008	52	6107904
$\mathbb{F}_{53}$	$u^2 = (t^4-37)(t^4-39)(t^4-45)$	550850560	52	10593280
$\mathbb{F}_{61}$	$u^2 = (t^4-14)(t^4-31)(t^4-34)$	1102049280	72	15306240
$\mathbb{F}_{73}$	$u^2 = (t^4-18)(t^4-42)(t^4-57)$	2107438080	60	35123968
$\mathbb{F}_{97}$	$u^2 = (t^4-1)(t^4-8)(t^4-64)$	13530240000	100	135302400
$\mathbb{F}_{97}$	$u^2 = (t^4-7)(t^4-11)(t^4-23)$	8977152000	96	93512000
$\mathbb{F}_{97}$	$u^2 = (t^4-13)(t^4-47)(t^4-87)$	8479539200	100	84795392
$\mathbb{F}_{101}$	$u^2 = (t^4-5)(t^4-84)(t^4-100)$	9599975424	96	99999744

Table 3: Jacobian orders of hyperelliptic function fields $F = k(t,u)$ of the form $u^2 = \prod_{j=0}^{s-1}(t^4 - a_j)$ and of their fixed fields $F^{\mathcal{C}_4} = k(t^4, u)$

2. Fixed Fields of $\mathcal{C}_n$, where $(n, \mathrm{char}(k)) = 1$ and $\nu = 1$

k	Defining Equation of $F = k(t,u)$	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_3}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_3}}\rvert}$
$\mathbb{F}_7$	$u^2 = t(t^3-1)(t^3-2)(t^3-3)$	2400	8	300
$\mathbb{F}_7$	$u^2 = t(t^3-1)(t^3-2)(t^3-4)$	4464	12	372
$\mathbb{F}_7$	$u^2 = t(t^3-1)(t^3-2)(t^3-5)$	5328	12	444
$\mathbb{F}_7$	$u^2 = t(t^3-1)(t^3-2)(t^3-6)$	2688	8	336
$\mathbb{F}_7$	$u^2 = t(t^3-1)(t^3-3)(t^3-4)$	2016	8	252
$\mathbb{F}_7$	$u^2 = t(t^3-1)(t^3-3)(t^3-6)$	2304	12	192
$\mathbb{F}_7$	$u^2 = t(t^3-1)(t^3-4)(t^3-5)$	5472	8	684
$\mathbb{F}_7$	$u^2 = t(t^3-1)(t^3-4)(t^3-6)$	2304	12	192
$\mathbb{F}_7$	$u^2 = t(t^3-1)(t^3-5)(t^3-6)$	2688	8	336
$\mathbb{F}_7$	$u^2 = t(t^3-2)(t^3-3)(t^3-4)$	5868	12	489
$\mathbb{F}_7$	$u^2 = t(t^3-2)(t^3-3)(t^3-5)$	2904	8	363
$\mathbb{F}_7$	$u^2 = t(t^3-2)(t^3-3)(t^3-6)$	5472	8	684
$\mathbb{F}_7$	$u^2 = t(t^3-2)(t^3-4)(t^3-5)$	2904	8	363
$\mathbb{F}_7$	$u^2 = t(t^3-2)(t^3-4)(t^3-6)$	1824	8	228
$\mathbb{F}_7$	$u^2 = t(t^3-2)(t^3-5)(t^3-6)$	5328	12	444
$\mathbb{F}_7$	$u^2 = t(t^3-3)(t^3-4)(t^3-5)$	5868	12	489
$\mathbb{F}_7$	$u^2 = t(t^3-3)(t^3-4)(t^3-6)$	2016	8	252
$\mathbb{F}_7$	$u^2 = t(t^3-3)(t^3-5)(t^3-6)$	4464	12	372
$\mathbb{F}_7$	$u^2 = t(t^3-4)(t^3-5)(t^3-6)$	2400	8	300

Table 4: Jacobian orders of hyperelliptic function fields $F = k(t,u)$ of the form $u^2 = t\prod_{j=0}^{s-1}(t^3 - a_j)$ and of their fixed fields $F^{\mathcal{C}_3} = k(t^3, tu)$ *(continued)*

k	Defining Equation of $F = k(t,u)$	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_3}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_3}}\rvert}$
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-2)(t^3-5)$	26880	20	1344
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-2)(t^3-9)$	16128	16	1008
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-3)(t^3-5)$	33024	16	2064
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-3)(t^3-6)$	69312	16	4332
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-3)(t^3-7)$	25536	16	1596
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-3)(t^3-10)$	37440	20	1872
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-4)(t^3-7)$	45504	12	3792
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-5)(t^3-6)$	18816	8	2352
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-5)(t^3-8)$	36864	16	2304
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-6)(t^3-7)$	24768	16	1548
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-7)(t^3-10)$	17856	12	1488
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-8)(t^3-12)$	36864	16	2304
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-9)(t^3-10)$	43776	16	2736
$\mathbb{F}_{13}$	$u^2 = t(t^3-1)(t^3-9)(t^3-11)$	37632	16	2352
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-3)(t^3-8)$	52080	20	2604
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-3)(t^3-10)$	20496	16	1281
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-3)(t^3-11)$	20496	16	1281
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-4)(t^3-7)$	52020	20	2601
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-4)(t^3-8)$	17856	12	1488
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-4)(t^3-9)$	20556	12	1713
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-4)(t^3-10)$	49860	20	2493
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-4)(t^3-11)$	56784	16	3549
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-5)(t^3-8)$	21312	12	1776
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-5)(t^3-9)$	25536	16	1596
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-6)(t^3-12)$	37632	16	2352
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-7)(t^3-8)$	43776	16	2736
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-7)(t^3-12)$	41280	20	2064
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-8)(t^3-9)$	35520	20	1776
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-8)(t^3-11)$	37440	20	1872
$\mathbb{F}_{13}$	$u^2 = t(t^3-2)(t^3-8)(t^3-12)$	55872	12	4656
$\mathbb{F}_{13}$	$u^2 = t(t^3-3)(t^3-4)(t^3-12)$	43776	16	2736
$\mathbb{F}_{13}$	$u^2 = t(t^3-3)(t^3-5)(t^3-8)$	33024	16	2064
$\mathbb{F}_{13}$	$u^2 = t(t^3-3)(t^3-6)(t^3-7)$	20556	12	1713
$\mathbb{F}_{13}$	$u^2 = t(t^3-3)(t^3-6)(t^3-11)$	20124	12	1677
$\mathbb{F}_{13}$	$u^2 = t(t^3-3)(t^3-7)(t^3-10)$	56784	16	3549
$\mathbb{F}_{13}$	$u^2 = t(t^3-3)(t^3-7)(t^3-12)$	35520	20	1776
$\mathbb{F}_{13}$	$u^2 = t(t^3-3)(t^3-8)(t^3-12)$	21312	12	1776
$\mathbb{F}_{13}$	$u^2 = t(t^3-3)(t^3-10)(t^3-12)$	37440	20	1872
$\mathbb{F}_{13}$	$u^2 = t(t^3-4)(t^3-5)(t^3-6)$	24768	16	1548
$\mathbb{F}_{13}$	$u^2 = t(t^3-4)(t^3-5)(t^3-11)$	35520	20	1776
$\mathbb{F}_{13}$	$u^2 = t(t^3-4)(t^3-6)(t^3-11)$	44688	16	2793
$\mathbb{F}_{13}$	$u^2 = t(t^3-4)(t^3-6)(t^3-12)$	66480	20	3324
$\mathbb{F}_{13}$	$u^2 = t(t^3-4)(t^3-7)(t^3-9)$	55632	16	3477
$\mathbb{F}_{13}$	$u^2 = t(t^3-4)(t^3-7)(t^3-11)$	17736	8	2217
$\mathbb{F}_{13}$	$u^2 = t(t^3-4)(t^3-9)(t^3-11)$	20556	12	1713

Table 4: Jacobian orders of hyperelliptic function fields $F = k(t,u)$ of the form $u^2 = t\prod_{j=0}^{s-1}(t^3 - a_j)$ and of their fixed fields $F^{\mathcal{C}_3} = k(t^3, tu)$ *(continued)*

k	Defining Equation of $F = k(t,u)$	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_3}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_3}}\rvert}$
$\mathbb{F}_{13}$	$u^2 = t(t^3-4)(t^3-9)(t^3-12)$	45504	12	3792
$\mathbb{F}_{13}$	$u^2 = t(t^3-5)(t^3-6)(t^3-8)$	47040	20	2352
$\mathbb{F}_{13}$	$u^2 = t(t^3-5)(t^3-6)(t^3-9)$	66480	20	3324
$\mathbb{F}_{13}$	$u^2 = t(t^3-5)(t^3-6)(t^3-10)$	16128	16	1008
$\mathbb{F}_{13}$	$u^2 = t(t^3-5)(t^3-9)(t^3-12)$	29760	20	1488
$\mathbb{F}_{13}$	$u^2 = t(t^3-5)(t^3-10)(t^3-11)$	52080	20	2604
$\mathbb{F}_{13}$	$u^2 = t(t^3-6)(t^3-7)(t^3-9)$	55632	16	3477
$\mathbb{F}_{13}$	$u^2 = t(t^3-6)(t^3-7)(t^3-12)$	24768	16	1548
$\mathbb{F}_{13}$	$u^2 = t(t^3-6)(t^3-8)(t^3-12)$	29760	20	1488
$\mathbb{F}_{13}$	$u^2 = t(t^3-6)(t^3-11)(t^3-12)$	42048	12	3504
$\mathbb{F}_{13}$	$u^2 = t(t^3-7)(t^3-9)(t^3-12)$	14400	12	1200
$\mathbb{F}_{13}$	$u^2 = t(t^3-8)(t^3-9)(t^3-12)$	36864	16	2304
$\mathbb{F}_{13}$	$u^2 = t(t^3-8)(t^3-10)(t^3-11)$	14976	8	1872
$\mathbb{F}_{19}$	$u^2 = t(t^3-1)(t^3-10)(t^3-13)$	116880	20	5844
$\mathbb{F}_{19}$	$u^2 = t(t^3-1)(t^3-10)(t^3-16)$	98496	16	6156
$\mathbb{F}_{19}$	$u^2 = t(t^3-2)(t^3-10)(t^3-11)$	115776	16	7236
$\mathbb{F}_{19}$	$u^2 = t(t^3-3)(t^3-5)(t^3-11)$	109152	24	4548
$\mathbb{F}_{19}$	$u^2 = t(t^3-3)(t^3-14)(t^3-17)$	140616	24	5859
$\mathbb{F}_{19}$	$u^2 = t(t^3-4)(t^3-17)(t^3-18)$	275184	28	9828
$\mathbb{F}_{19}$	$u^2 = t(t^3-5)(t^3-8)(t^3-15)$	233568	24	9732
$\mathbb{F}_{19}$	$u^2 = t(t^3-6)(t^3-7)(t^3-10)$	177360	20	8868
$\mathbb{F}_{19}$	$u^2 = t(t^3-6)(t^3-7)(t^3-17)$	122976	24	5124
$\mathbb{F}_{19}$	$u^2 = t(t^3-7)(t^3-9)(t^3-10)$	161616	28	5772
$\mathbb{F}_{19}$	$u^2 = t(t^3-7)(t^3-11)(t^3-15)$	134784	24	5616
$\mathbb{F}_{19}$	$u^2 = t(t^3-7)(t^3-13)(t^3-16)$	115776	16	7236
$\mathbb{F}_{19}$	$u^2 = t(t^3-11)(t^3-12)(t^3-13)$	69888	16	4368
$\mathbb{F}_{19}$	$u^2 = t(t^3-12)(t^3-13)(t^3-17)$	233568	24	9732
$\mathbb{F}_{19}$	$u^2 = t(t^3-13)(t^3-16)(t^3-18)$	146496	16	9156
$\mathbb{F}_{31}$	$u^2 = t(t^3-1)(t^3-3)(t^3-9)$	1259040	40	31476
$\mathbb{F}_{31}$	$u^2 = t(t^3-1)(t^3-7)(t^3-12)$	744912	28	26604
$\mathbb{F}_{31}$	$u^2 = t(t^3-1)(t^3-7)(t^3-13)$	1341312	32	41916
$\mathbb{F}_{31}$	$u^2 = t(t^3-1)(t^3-7)(t^3-25)$	1053312	32	32916
$\mathbb{F}_{31}$	$u^2 = t(t^3-1)(t^3-7)(t^3-26)$	696192	32	21756
$\mathbb{F}_{31}$	$u^2 = t(t^3-1)(t^3-14)(t^3-19)$	1241760	40	31044
$\mathbb{F}_{31}$	$u^2 = t(t^3-1)(t^3-22)(t^3-26)$	1954800	36	54300
$\mathbb{F}_{31}$	$u^2 = t(t^3-2)(t^3-5)(t^3-18)$	1954800	36	54300
$\mathbb{F}_{31}$	$u^2 = t(t^3-2)(t^3-5)(t^3-26)$	1054560	40	26364
$\mathbb{F}_{31}$	$u^2 = t(t^3-2)(t^3-5)(t^3-29)$	775296	24	32304
$\mathbb{F}_{31}$	$u^2 = t(t^3-2)(t^3-9)(t^3-12)$	1288656	36	35796
$\mathbb{F}_{31}$	$u^2 = t(t^3-2)(t^3-13)(t^3-28)$	853200	36	23700
$\mathbb{F}_{31}$	$u^2 = t(t^3-3)(t^3-9)(t^3-21)$	565152	32	17661
$\mathbb{F}_{31}$	$u^2 = t(t^3-4)(t^3-9)(t^3-19)$	1083600	28	38700
$\mathbb{F}_{31}$	$u^2 = t(t^3-4)(t^3-11)(t^3-13)$	1011360	40	25284
$\mathbb{F}_{31}$	$u^2 = t(t^3-4)(t^3-22)(t^3-28)$	1038240	40	25956
$\mathbb{F}_{31}$	$u^2 = t(t^3-5)(t^3-6)(t^3-11)$	548856	24	22869

Table 4: Jacobian orders of hyperelliptic function fields $F = k(t,u)$ of the form $u^2 = t\prod_{j=0}^{s-1}(t^3 - a_j)$ and of their fixed fields $F^{\mathcal{C}_3} = k(t^3, tu)$ *(continued)*

k	Defining Equation of $F = k(t,u)$	$\lvert\mathbb{J}_F\rvert$	$\lvert\mathbb{J}_{F^{\mathcal{C}_3}}\rvert$	$\frac{\lvert\mathbb{J}_F\rvert}{\lvert\mathbb{J}_{F^{\mathcal{C}_3}}\rvert}$
$\mathbb{F}_{31}$	$u^2 = t(t^3-5)(t^3-8)(t^3-30)$	1190400	32	37200
$\mathbb{F}_{31}$	$u^2 = t(t^3-6)(t^3-10)(t^3-17)$	978984	24	40791
$\mathbb{F}_{31}$	$u^2 = t(t^3-6)(t^3-16)(t^3-26)$	1566864	36	43524
$\mathbb{F}_{31}$	$u^2 = t(t^3-6)(t^3-18)(t^3-22)$	853152	32	26661
$\mathbb{F}_{31}$	$u^2 = t(t^3-7)(t^3-9)(t^3-30)$	591264	24	24636
$\mathbb{F}_{31}$	$u^2 = t(t^3-8)(t^3-10)(t^3-12)$	1292928	32	40404
$\mathbb{F}_{31}$	$u^2 = t(t^3-8)(t^3-10)(t^3-26)$	761472	32	23796
$\mathbb{F}_{31}$	$u^2 = t(t^3-10)(t^3-13)(t^3-14)$	1130400	32	35325
$\mathbb{F}_{31}$	$u^2 = t(t^3-10)(t^3-15)(t^3-19)$	726768	28	25956
$\mathbb{F}_{31}$	$u^2 = t(t^3-10)(t^3-16)(t^3-24)$	841440	40	21036
$\mathbb{F}_{31}$	$u^2 = t(t^3-10)(t^3-17)(t^3-20)$	1231008	32	38469
$\mathbb{F}_{31}$	$u^2 = t(t^3-10)(t^3-23)(t^3-28)$	865152	32	27036
$\mathbb{F}_{31}$	$u^2 = t(t^3-11)(t^3-14)(t^3-23)$	753696	24	31404
$\mathbb{F}_{31}$	$u^2 = t(t^3-11)(t^3-25)(t^3-26)$	853152	32	26661
$\mathbb{F}_{31}$	$u^2 = t(t^3-12)(t^3-16)(t^3-30)$	808704	36	22464
$\mathbb{F}_{31}$	$u^2 = t(t^3-19)(t^3-26)(t^3-28)$	2135484	36	59319
$\mathbb{F}_{31}$	$u^2 = t(t^3-19)(t^3-28)(t^3-30)$	915072	32	28596

Table 4: Jacobian orders of hyperelliptic function fields $F = k(t,u)$ of the form $u^2 = t\prod_{j=0}^{s-1}(t^3 - a_j)$ and of their fixed fields $F^{\mathcal{C}_3} = k(t^3, tu)$

Bibliography

[ADH94] L. M. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. In L. M. Adleman and M.-D. Huang, editors, *Algorithmic Number Theory Symposium ANTS-I*, pages 28–40. Springer-Verlag, May 1994. LNCS 877.

[Art24] Emil Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. *Mathematische Zeitschrift*, 19:152–246, 1924.

[Art73] Emil Artin. *Galoissche Theorie*. Harri Deutsch Verlag, 2., unveränderte auflage edition, 1973.

[Bos93] Siegfried Bosch. *Algebra*. Springer-Verlag, 1993.

[Bra88] Rolf Brandt. *Über die Automorphismengruppen von algebraischen Funktionenkörpern*. PhD thesis, Universität-Gesamthochschule Essen, 1988.

[Can87] David G. Cantor. Computing in the jacobian of a hyperelliptic curve. *Mathematics of Computation*, 48(177):95–101, 1987.

[ccG] cv cryptovision GmbH. Kurvenfabrik. `http://www.cryptovision.com/Kurvenfabrik/textFabrik.html`.

[DFK$^+$97] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, and K. Wildanger. KANT V4. *Journal of Symbolic Computation*, 24:267–283, 1997. The software is available at `http://www.math.tu-berlin.de/~kant`.

[DGM99] Iwan M. Duursma, Pierrick Gaudry, and Francois Morain. Speeding up the discrete log computation on curves with automorphisms. In *ASIACRYPT '99*, volume 1838 of *Lecture Notes on Computer Science*, pages 103–121. Springer, 1999.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[DV02] Jan Denef and Frederik Vercauteren. Extensions of kedlaya's algorithm. Talk held at the Elliptic Curve Conference (ECC 2002), Essen, 2002. Slides are available at `http://www.exp-math.uni-essen.de/~weng/vercauteren_Presentation.ps.gz`.

[FGH00] Mireille Fouquet, Pierrick Gaudry, and Robert Harley. On satoh´s algorithm and its implementation. *Journal of the Ramanujan Mathematical Society*, December 2000.

[Fis56] Irwin Fischer. The moduli of hyperelliptic curves. *Transactions of the American Mathematical Society*, 82:64–84, 1956.

[FR94] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206):865–874, April 1994.

[Fre98] Free Software Foundation, Inc. Gnu bourne-again shell (bash). `http://www.gnu.org/software/bash/bash.html`, 1998.

[Gal01] Steven Galbraith. Weil descent of jacobians. presented at WCC 2001, February 2001.

[Gau00] Pierrick Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In B. Preneel, editor, *Eurocrypt 2000*, pages 19–34. Springer, 2000. LNCS 1807.

[Gau02] Pierrick Gaudry. Cardinality of a genus 2 hyperelliptic curve over GF$(5 \cdot 10^{24} + 41)$. Mail to the mailing list `NMBRTHRY` LISTSERV.NODAK.EDU, September 2002. The list's archive is available at `http://listserv.nodak.edu/archives/nmbrthry.html`.

[Gey74] Wulf-Dieter Geyer. Invarianten binärer Formen. In H. Popp, editor, *Classification of Algebraic Varieties and Compact Complex Manifolds*, volume 412 of *Lecture Notes in Mathematics*, pages 36–69. Springer, 1974.

[GH00] Pierrick Gaudry and Robert Harley. Counting points on hyperellptic curves over finite fields. In *Algorithmic Number Theory*, volume 1838 of *Lecture Notes on Computer Science*, pages 313–332. Springer, July 2000.

[GHS00] Pierrick Gaudry, Florian Hess, and Nigel P. Smart. Constructive and destructive facets of weil descent on elliptic curves. Technical Report CSTR-00-016, Department of Computer Science, University of Bristol, October 2000. to appear in Journal of Cryptology.

[Göb03a] Norbert Göb. Computing the automorphism groups of hyperelliptic function fields, May 2003. `http://arxiv.org/abs/math.NT/0305284`, presented at the MEGA 2003 conference.

[Göb03b] Norbert Göb. Examples of reduced automorphism groups of hyperelliptic function fields. `http://www.itwm.fhg.de/mab/competences/Crypto/aut/goeb_examples.zip`, September 2003.

[GPS$^+$02] G.-M. Greuel, G. Pfister, H. Schoenemann, et al. Singular—a computer algebra system for polynomial computations, version 2.0.3. `http://www.singular.uni-kl.de/`, February 2002.

[Has34a] Helmut Hasse. Theorie der Differentiale in algebraischen Funktionenkörpern mit vollkommenem Konstantenkörper. *Journal für die Reine und Angewandte Mathematik*, 172:55–64, 1934.

[Has34b] Helmut Hasse. Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper. *Journal für die Reine und Angewandte Mathematik*, 172:37–54, 1934.

[Hes99] Florian Hess. *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern.* PhD thesis, Technische Universität Berlin, 1999.

[HSS00] Florian Hess, Gadiel Seroussi, and Nigel Smart. Two topics in hyperelliptic cryptography. Technical Report HPL-2000-118, HP Laboratories, Palo Alto, 2000.

[Hum96] John F. Humphreys. *A Course in Group Theory.* Oxford University Press, 1996.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using monsky-washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16:323–338, 2001.

[Kob89] Neal Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1:139–150, 1989.

[Kob99] Neal Koblitz. *Algebraic Aspects of Cryptography.* Springer, 1999.

[Kon99] Aristides Kontogeorgis. The group of automorphisms of cyclic extensions of rational function fields. *Journal of Algebra*, 216(2):665–706, June 1999.

[Kun94] Ernst Kunz. *Algebra.* Vieweg, München, 2nd edition, 1994.

[Kux03] Georg Kux. *Algebraic Correspondences Between Hyperelliptic Function Fields.* PhD thesis, Universität Kaiserslautern, 2003.

[Lin97] Scott Charles Lindhurst. *Computing Roots in Finite Fields and Groups, with a Jaunt through Sums of Digits.* PhD thesis, Department of Mathematics, University of Wisconsin, Madison, August 1997.

[LL93] Arjen K. Lenstra and Hendrik W. Lenstra jun. *The Development of the Number Field Sieve.* LNCS 1554. Springer, 1993.

[Loc94] P. Lockhart. On the discriminant of a hyperelliptic curve. *Transactions of the American Mathematical Society*, 342(2):729–752, April 1994.

[Mad68] Manohar L. Madan. Class number and ramification in fields of algebraic functions. *Archiv der Mathematik*, 19:121–124, 1968.

[Mad69] Manohar L. Madan. Class number relations in fields of algebraic functions. *Journal für die Reine und angewandte Mathematik*, 238:89–92, 1969.

[Mad70] Manohar L. Madan. On class numbers in fields of algebraic functions. *Archiv der Mathematik*, 21:167–171, 1970.

[MOV93] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, September 1993.

[MvOV96] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer, 1992.

[PH78] Stephen C. Pohlig and Martin E. Hellman. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Transactions on Information Theory*, 24(1):106–110, January 1978.

[Pol78] J. M. Pollard. Monte carlo methods for index computation (mod$p$). *Mathematics of Computation*, 32(143):918–924, July 1978.

[Pol00] J. M. Pollard. Kangaroos, monopoly and discrete logarithms. *Journal of Cryptology*, 13:437–447, 2000.

[PS98] Sachar Paulus and Andreas Stein. Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves. In *Algorithmic Number Theory*, volume 1423 of *Lecture Notes on Computer Science*, pages 576–591. Springer, June 1998.

[Roq53] Peter Roquette. Arithmetischer Beweis der Riemannschen Vermutung in Kongruenzfunktionenkörpern beliebigen Geschlechts. *Journal für die Reine und Angewandte Mathematik*, 191:199–252, 1953.

[Roq70] Peter Roquette. Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik. *Mathematische Zeitschrift*, 117:157–163, 1970.

[Ros02] Michael Rosen. *Number Theory in Function Fields*. Springer, 2002.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[Rüc99] Hans-Georg Rück. On the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 68(226):805–806, April 1999.

[Sat00] Takazuka Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[Sch31] Friedrich Karl Schmidt. Analytische Zahlentheorie in Körpern der Charakteristik p. *Mathematische Zeitschrift*, 33:1–32, 1931.

[Sch38] Hermann Ludwig Schmid. Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik. *Journal für die Reine und Angewandte Mathematik*, 179:5–14, 1938.

[Sch39] Friedrich Karl Schmidt. Zur arithmetischen Theorie der algebraischen Funktionen. II. Algemeine Theorie der Weierstraßpunkte. *Mathematische Zeitschrift*, 45:75–96, 1939.

[Sch95] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres*, 7:219–254, 1995.

[Sch96] Bruce Schneier. *Applied Cryptography. Protocols, Algorithms, and Source Code in C.* John Wiley, 2nd edition, 1996.

[Sci02] SciFace Software GmbH & Co. KG. MuPAD 2.5.0—The Open Computer Algebra System. `http://www.mupad.com/`, 1997–2002.

[Sha00] Tony Shaska. Genus 2 function fields with degree 2 elliptic subfields. Preprint, December 2000.

[Sha03] Tony Shaska. Computational aspects of hyperelliptic curves. In Ziming Li and William Sit, editors, *COMPUTER MATHEMATICS—Proceedings of the Sixth Asian Symposium (ASCM 2003)*, volume 10 of *Lecture Notes Series on Computing*, pages 13–27. World Scientific, April 2003.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in Graduate Texts in Mathematics. Springer Verlag, New York, 1986.

[Sin02] Simon Singh. *The Code Book*. Fourth Estate, 2002.

[SS98] Y. Sakai and K. Sakurai. Design of hyperelliptic cryptosystems in small characteristic and a software implementation over F_{2^n}. *Lecture Notes in Computer Science*, 1514:80–94, 1998.

[SSI98] Y. Sakai, K. Sakurai, and H. Ishizuka. Secure hyperelliptic cryptosystems and their performance. *Lecture Notes in Computer Science*, 1431:164–181, 1998.

[Ste01] Andreas Stein. Sharp upper bounds for arithmetics in hyperelliptic function fields. *Journal of the Ramanujan Mathematical Society*, 16(2):119–203, 2001.

[Sti93] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer, 1993.

[Sto00] Michael Stoll. Hyperelliptic curves magma package. `http://www.math.uni-duesseldorf.de/~stoll/magma/` or as part of Magma, Version 2.9-23, `http://magma.maths.usyd.edu.au/magma/`, September 2000.

[vdW93a] B. L. van der Waerden. *Algebra I*. Springer, 9th edition, 1993.

[vdW93b] B. L. van der Waerden. *Algebra II*. Springer, 6th edition, 1993.

[Wen03] Annegret Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Mathematics of Computation*, 72:435–458, 2003.

Index

adele, 13
adele space, 13
algebraic extension of a function field, 15
algebraic function field, 9
alternating group, 87
automorphism group, 20

basis, 21
birthday paradox algorithm, 40
Brandt's normal forms, 88

canonical divisor, 14
Cantor representation, 30
central extension, 87
conorm, 17
constant field extension, 15
constant field, 9
cyclic group, 87

defining equation, 21
degree, 10
different, 18
different exponent, 18
differential, Hasse's definition, 14
dihedral group, 87
dimension of a divisor, 12
discrete logarithm problem, 34
divisor group, 10
divisor class group, 11
divisor of a Weil differential, 14
divisors, 10
DL, 34

elliptic curve, 22
elliptic function field, 21
equivalent divisors, 11
extension of a function field, 15

finite function field extension, 15
fixed field, 20
full constant field, 9
function field, 9

gap number, 26
general linear group, 88
generators, 21
genus, 13

Hasse-Weil interval, 40
Hasse-Witt matrix, 40
HECDL, 34
hyperelliptic curve, 22
hyperelliptic curve discrete logarithm problem, 34
hyperelliptic involution, 87
hyperelliptic function field, 21

imaginary quadratic basis, 21
imaginary quadratic representation, 21
inert, 17
infinite place, 24

Jacobi symbol, 36
Jacobian, 12

lie over (places), 15
lie under (places), 15

natural numbers, 9
normal form, 79

over (place P' over place P), 15

perfect field, 15
place, 9
pole, 10
pole divisor, 11
pole number, 26
positive integers, 9
prime, 10
prime element, 10
principal adele, 13
principal divisor, 11
projective general linear group, 88
projective special linear group, 88

ramification index, 17
ramified, 17
rational function field, 9
real quadratic basis, 21
real quadratic representation, 21
reduced automorphisms, 87
regular, 17
relative degree, 17
Riemann-Roch space, 12

semidirect product, 88
separable, 21
separable function field extension, 15
special linear group, 88
spectre, 61

subfield of a function field, 15
support, 10
symbols
- $A \sim B$, 11
- F/k, 9
- $\mathcal{A}_F(A)$, 13
- $\mathcal{A}_F$, 13
- $\mathcal{A}_n$, 87
- $\mathrm{Aut}(F/k)$, 20
- $\mathrm{Con}_{F'/F}$, 17
- $\mathcal{C}_n$, 87
- $\mathrm{Diff}(F'/F)$, 18
- $\mathcal{D}_n$, 87
- $\mathcal{C}_F^0$, 11
- $\mathcal{C}_F$, 11
- $\mathcal{D}_F^0$, 10
- $\mathcal{D}_F$, 10
- F^G, 20
- $\mathrm{GL}_n(q)$, 88
- $\mathbb{J}_F$, 11
- $\left(\frac{D}{a}\right)$, 36
- $\mathbb{N}$, 9
- $\mathbb{N}_+$, 9
- $\mathrm{PGL}_n(q)$, 88
- $\mathrm{PSL}_n(q)$, 88
- $\mathbb{P}_F$, 9
- $\mathcal{P}_F$, 11
- $\mathcal{L}(A)$, 12
- $\mathrm{SL}_n(q)$, 88
- $G \rtimes H$, 88
- $\mathcal{S}_n$, 87
- $\mathcal{O}_P$, 9
- $\Omega_F(A)$, 13
- Ω_F, 13
- $\deg(D)$, 10
- $\mathrm{d}(P'/P)$, 18
- $\dim(A)$, 12
- $\dim(\mathcal{L}(A))$, 12
- $\mathrm{div}(a, b)$, 30
- $\tilde{k}$, 9
- g_F, 13
- Φ, 87
- ∞_x, 24
- $P' \mid P$, 15
- $(l \cdot c)$, where $l \in \mathbb{N}$, $c \in k^m$, 92
- $(x)_\infty^F$, 11
- $(x)_\infty$, 11
- $(x)^F$, 11
- (x), 11
- $\mathrm{e}(P'/P)$, 17
- $\mathrm{f}(P'/P)$, 17
- $\sigma(P')$, 21
- $\mathrm{supp}(D)$, 10
- $\mathrm{U}_F(G)$, 87
- $\mathrm{F}[G, k]$, 87
- v_P, 9
- $\mathrm{v}_P(A)$, 10
- $\mathrm{v}_P(\alpha)$, 13
- $(x)_0^F$, 11
- $(x)_0$, 11

symmetric group, 87

type $\mathrm{F}[G, k]$, 87

under (place P under place P'), 15
unramified, 17

valuation, 9
valuation ring, 9
variety, 22

Weierstraß point, 26
Weil descent, 39
Weil differentials, 13
Weil restriction, 39

zero, 10
zero divisor, 11

Lebenslauf des Autors

Angaben zur Person

Name	Göb, Norbert
Staatsangehörigkeit	Deutsch
Geburtsdatum	6. März 1974

Schul- und Berufsausbildung

Datum	1984–1994
Bildungseinrichtung	Kurfürst-Ruprecht-Gynmasium Neustadt an der Weinstraße
Abschluß	Abitur

Datum	1994–2000
Bildungseinrichtung	Universität Kaiserslautern
Art der Ausbildung	Mathematikstudium, Nebenfach: Informatik
Abschluß	Diplom-Mathematiker, Gesamtnote „Mit Auszeichnung“

Datum	2000–2004
Bildungseinrichtung	Technische Universität Kaiserslautern
Art der Ausbildung	Promotion über hyperelliptische Kurven Kryptographie

Veröffentlichungen

[**Göb03a**]	„Computing the Automorphism Group of Hyperelliptic Function Fields“, Vorgetragen auf der Effective Methods in Algebraic Geometry (MEGA) 2003

Author's Curriculum Vitae

Personal Information

Name	Göb, Norbert
Nationality	German
Date of Birth	March 6, 1974

Education

Date	1984–1994
School	Kurfürst-Ruprecht-Gynmasium Neustadt an der Weinstraße
Qualification	Abitur

Date	1994–2000
School	University of Kaiserslautern
Principal Subjects	Study of mathematics, subsidiary: Computer sciences
Qualification	Diplom-Mathematiker, exams passed with distinction

Date	2000–2004
School	University of Kaiserslautern
Principal Subjects	Doctorate on hyperelliptic curve cryptography

Publications

[**Göb03a**] "Computing the Automorphism Group of Hyperelliptic Function Fields", presented at the conference Effective Methods in Algebraic Geometry (MEGA) 2003