Normal Forms of Hyperelliptic Curves of Genus 3

Gerhard Frey[1] & Ernst Kani [2,*]
[1] Institute for Experimental Mathematics
University of Duisburg-Essen
Essen, Germany
e-mail: frey@exp-math.uni-essen.de
[2] Department of Mathematics and Statistics
Queen's University
Kingston, Ontario, K7L 3N6, Canada
email: Kani@mast.queensu.ca *

July 8, 2015

Dedicated to the Memory of Scott A. Vanstone

Abstract

The main motivation for the paper is to understand which *hyperelliptic* curves of genus 3 defined over a field K of characteristic $\neq 2$ appear as the image of the Donagi-Livné-Smith construction. By results in [FK] this means that one has to determine the intersection W of a Hurwitz space defined by curves of genus 3 together with cover maps of degree 4 to $\mathbb{P}^1_K$ and a certain ramification type with the hyperelliptic locus in the moduli space of curves of genus 3.

To achieve this aim we first study hyperelliptic curves of genus g as smooth curves C in $\mathbb{P}^1_K \times \mathbb{P}^1_K$ and prove that, under mild conditions on K, the curve C can be given by a "$(g+1,2)$-*normal form*", namely by an affine equation in two variables of partial degrees $g+1$ and 2 and hence of total degree $\leq g+3$, which is smaller than the degree of Weierstraß normal forms. Such curves are naturally parameterized by a Hurwitz space $\overline{\mathcal{H}}_{g,g+1}$.

We then specialize to $g=3$ and introduce Hurwitz spaces for 4-covers with special ramification types. The study of these spaces enables us to determine that W is irreducible of dimension 4. Moreover we find an explicitly given K-rational family of curves C in $(4,2)$-normal form such that the isomorphism classes of its members are in $W(K)$ and such that the image of the family in W is Zariski-dense. For these curves we describe the "inverse" of the Donagi-Livné-Smith construction.

Keywords: hyperelliptic curves, normal forms, Hurwitz spaces attached to curves of genus 3
MSC 14H30, 14H45, 14Q05, 14G50

1 Introduction and Results

1.1 Motivation: A Relation to Public Key Cryptography

A well-known and very effective tool for public key cryptography is the use of discrete logarithms (DL) in divisor class groups Pic^0_C of degree 0 of curves C of genus g over finite

[*] Supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC)

fields $\mathbb{F}_q$ as crypto primitives for public key crypto systems. For details and following remarks see [CF].

The security of these systems depend on the hardness of the computation of the DL, and one of the most dangerous attacks is based on very refined versions of index-calculus methods. As result one can bound the (probabilistic) complexity of the computation of the DL in Pic^0_C, up to logarithmic factors, by $\mathcal{O}(q^{(2-2/g)})$ [DGTT]. Since, for fixed g, the asymptotic size of Pic^0_C is $\sim q^g$ one is forced to exclude curves C with genus ≥ 4.

Curves of genus 1 or 2 seem to be secure against this attack at least today and under certain precautions. Divisor class groups of curves of genus 3 lie on the border of security, if one looks at this estimate.

But it turns out that in addition to the genus the *degree* of plane equations for C is important.

Theorem 1 (Diem[D]) (a) *If C is a non-nyperelliptic curve of genus 3 over $\mathbb{F}_q$ which is given by a plane equation of degree $d = 4$, then there exists an algorithm for computing the discrete logarithm in the group of divisor classes $\mathrm{Pic}^0(C)$ of degree 0 of C that has, up to logarithmic factors, complexity $\mathcal{O}(q)$.*

(b) *If C is a any curve over $\mathbb{F}_q$ which is given by a reflexive plane equation of degree $d \geq 4$, then there exists an algorithm for computing the discrete logarithm that has, up to logarithmic factors, complexity $\mathcal{O}(q^{2-\frac{2}{d-2}})$.*

By the theory of curves we know that *non-hyperelliptic curves* of genus 3 can be always be given by a plane equation of degree 4 and that plane equations of *hyperelliptic* curves of genus 3 cannot have a degree smaller than 5. Hence for *hyperelliptic* curves the above mentioned results yield complexity $\mathcal{O}(q^{4/3})$ for the computation of the DL, which is not optimal but still acceptably near to the complexity of generic attacks.

But for *non-hyperelliptic* curves of genus 3 this complexity is, up to logarithmic factors, $\mathcal{O}(q)$ and hence very weak. We get the surprising

Consequence. Hyperelliptic curves of genus 3 are more secure than non-hyperelliptic (i.e., “generic”) curves of genus 3.

This result is exploited by Ben Smith [Sm] for an attack. He applies explicitly given isogenies η_* of degree 8 of Jacobian varieties of hyperelliptic curves C' of genus 3 whose image is again the Jacobian of a curve C of genus 3. This construction relies on the *trigonal construction* of Donagi-Livné and so we call it the Donagi-Livné-Smith construction. In [FK] we give an interpretation of this construction in terms of Hurwitz spaces and explain how η_* is obtained by a correspondence η between C' and C. As a consequence of this approach we get more information about C:

Fact. There is a *cover map* $f : C \to \mathbb{P}^1_K$ of degree 4 with monodromy group $\mathrm{Gal}(f) \simeq S_4$ such that exactly 4 points $P_1, \dots, P_4 \in \mathbb{P}^1(\overline{K})$ of the ramification points of f are of type $(2,2)$, and the other 4 are of type $(2,1,1)$.

Here, as usual, we mean by the *monodromy group* of f the Galois group of a Galois closure of the cover f. Moreover, we say that a point $P_i \in \mathbb{P}^1(\overline{K})$ *has ramification type* $(2,2)$ (respectively, $(2,1,1)$) with respect to f if $f^*(P_i) = 2(Q_{i,1} + Q_{i,2})$, (respectively, $f^*(P_i) = 2Q_{i,1} + Q_{i,2} + Q_{i,3}$), with $Q_{i,j} \in C(\overline{K})$ and $Q_{i,j} \neq Q_{i,k}$, for $j \neq k$.

Smith shows that there are curves C which are not hyperelliptic, and he assumes heuristically that the probability for C to be hyperelliptic should be $\sim 1/q$. One of the main aims of the paper is to give an explanation of this heuristic in terms of Hurwitz spaces.[1]

It turns out that for this the structure of the monodromy group and the ramification type of the cover f are crucial.

[1] We want to remark here that the arguments given in [FK], Subsection 5.2, for this claim are not sufficient. So part of the motivation for this paper is to repair this gap.

1.2 Results

This discussion motivates that we want to study the Hurwitz space $\overline{H}_{3,4,4}(S_4)$ which "classifies" equivalence classes of morphisms $f : C \to \mathbb{P}^1_K$ of degree 4 with monodromy group S_4 and ramification type $(2,2)^4(2,1,1)^4$, where C is a *hyperelliptic* curve of genus 3. In order to understand this Hurwitz space, we first study more generally the related Hurwitz spaces $\overline{H}_{3,4,k}$ which classify degree 4 covers $f : C \to \mathbb{P}^1_K$ (with C hyperelliptic of genus 3) ramified of type $(2,2)$ in at least k points (over $\overline{K}$), for $k = 3, 4$.

1.2.1 Hyperelliptic Curves in the Image of the Donagi-Livné-Smith construction

One of the main results of the paper is the following structure theorem.

Theorem 2 *The Hurwitz space $\overline{H}_{3,4,4}(S_4)$ is a unirational, irreducible variety of dimension 4, provided that char$(K) > 5$. Moreover, the natural forget map*

$$\overline{\mu}_3 : \overline{H}_{3,4,4}(S_4) \to M_3$$

to the moduli space M_3 of genus 3 curves has finite fibres and so its image $\overline{\mu}_3(\overline{H}_{3,4,4}(S_4))$ is also irreducible of dimension 4.

This theorem is proved in Subsection 4.2.5. Moreover, we shall present explicit equations of a generic family of curve covers defined over K and parameterized by 4 rational parameters such that these define an non-empty open subscheme U' of $\overline{H}_{3,4,4}(S_4)$; cf. Subsection 4.2.4.

In Subsection 4.2.5 we also describe the inverse of the Donagi-Livné-Smith construction applied to curve covers in $U'(K)$ (see Proposition 38) and give an explicit example.

Using this connection, it follows together with Theorem 2 that the isomorphism classes of hyperelliptic curves obtained by the Donagi-Livné-Smith Construction form a four-dimensional irreducible subspace W of the moduli space M_3^h of hyperelliptic curves of genus 3.

Now we are in a situation where we can use well-established results about the number of points on varieties over finite fields (see e.g. [GL]) and get that over finite fields $\mathbb{F}_q$ with q elements we have that $|W(\mathbb{F}_q)|/q^4 \sim 1$. Since $\dim M_3^h = 5$, this explains and proves the heuristics made in [Sm] and mentioned above.

1.2.2 Normal Forms

To prove Theorem 2 and other related results, we shall investigate normal forms for equations for curves C of genus g (mostly $g = 3$) which are different from the well-known Weierstraß normal form.

In Section 3 we show that hyperelliptic curves C of arbitrary genus g with at least $g(g-1)+1$ K-rational points can be given by a smooth curve in $\mathbb{P}^1_K \times \mathbb{P}^1_K$ with an equation $F(T_0, T_1; X_0, X_1) = 0$ homogenous of degree 2 in T_0, T_1 and homogenous of degree $g+1$ in X_0, X_1 whose de-homogenization yields an affine plane curve with **normal form equation**

$$F(T,X) \ = \ \sum_{i=0}^{g+1}\sum_{j=0}^{2} r_{ij}X^{g+1-i}T^j \text{ with } r_{ij} \in K$$

of total degree $\leq g+3$; [2] cf. formula (3) in Subsection 3.1.2. Since each such curve C comes equipped with two covers $f_i : C \to \mathbb{P}^1_K$, we see that these equations naturally

[2] By a linear change of variables that positions a K-rational point at $(\infty, \infty) \in \mathbb{P}^1_K \times \mathbb{P}^1_K$, one can even achieve degree $g+2$, which is optimal ([CM]). Recall that the Weierstraß normal forms have degree $\geq 2g+1$.

define a Hurwitz set $\tilde{\mathcal{H}}_{g,g+1}(K)$ which classifies isomorphism classes of triples (C, f_1, f_2), where f_1 and f_2 are cover of degree $g+1$ and 2, respectively.

1.2.3 Normal Forms with Given Ramification Types for g=3

In Section 4 we restrict attention to the case $g = 3$. For $k = 3, 4$ we consider the subsets $\tilde{\mathcal{H}}'_{3,4,k}(K) \subset \tilde{\mathcal{H}}_{3,4}(K)$ which are defined by the condition that the degree 4 cover $f_1 : C \to \mathbb{P}^1_K$ has at least k ramification points of type $(2, 2)$. Moreover, by passing to equivalence classes of covers, we obtain the Hurwitz sets $\overline{\mathcal{H}}_{3,4,k}(K) \subset \overline{\mathcal{H}}_{3,4}(K)$.

In this section we shall investigate the geometric structure behind these sets. More precisely, we will show that the set $\tilde{\mathcal{H}}'_{3,4,k}(K)$ is the the set of K-rational points of a subscheme $\tilde{H}'_{3,4,k}$ of the Hurwitz space $\tilde{H}_{3,4}$, and that the elements of the set $\overline{\mathcal{H}}_{3,4,k}(K)$ give rise to K-rational points of a subscheme $\overline{H}_{3,4,k}$ of the scheme $\overline{H}_{3,4}$.

The case $k = 4$ is obviously motivated by the Donagi-Livné-Smith construction, and $k = 3$ is remarkable because of the fact that the forget map $\overline{\mu}_3 : \overline{H}_{3,4,3} \to M^h_3$ which sends classes of triples (C, f_1, f_2) to the isomorphism class of C is generically finite; see Theorem 19.

The Role of Families. At this stage we want to say a word about the our strategy in this paper. We give arguments mostly for "generic" cases, i.e. we describe open non-empty subspaces of the varieties under investigation. This helps to avoid the discussion of special cases.

Moreover, the "generic" approach in our context has the big advantage that we can work with explicitly given rational families of curves defined over K which induce generically finite and dominant maps to the spaces under consideration and for which we find simple normal forms for the involved curves C as equations. But we have to pay a price for this. First of all, one misses a good part of the geometric picture that can be detected in a much more subtle and precise analysis and which is presented in the preprint [K2].

Moreover, in order to get simple curve equations we have to assume that ramification points of f_1 are rational over K, and so rationality problems appear when $K \neq \overline{K}$.[3]

1.2.4 The Spaces $\tilde{\mathcal{H}}_{3,4,3}$ and $\overline{\mathcal{H}}_{3,4,3}$

In order to obtain relatively simple equations for the curve covers in $\tilde{\mathcal{H}}'_{3,4,3}(K)$, we use Proposition 6 below to choose special representatives for the isomorphism classes of triples (C, f_1, f_2): We view C as an embedded curve on $\mathbb{P}^1_K \times \mathbb{P}^1_K$, and let $f_1 = f_C := (\mathrm{pr}_1)_{|C}$ be the restriction to C of the first projection and let $f_2 = \pi_C := (\mathrm{pr}_2)_{|C}$ be the restriction to C of the second projection of $\mathbb{P}^1_K \times \mathbb{P}^1_K$. Then we investigate triples (C, f_C, π_C) with the following additonal properties.

The cover $f_C : C \to \mathbb{P}^1_K$ has the special projective points $P_0 = (1 : 0)$, $P_1 = (1 : 1)$ and $P_{-1} = (1 : -1)$ as ramification points of type $(2, 2)$. In addition, we impose some extra conditions on the points on C in the fibres over P_0, P_1 and P_{-1}; cf. equations (5) – (7) in Subsection 4.1.

The isomorphism classes of triples (C, f_C, π_C) satisfying these conditions form a certain subset $\tilde{\mathcal{H}}_{3,4,3}(K) \subset \tilde{\mathcal{H}}'_{3,4,3}(K)$ which is analyzed in detail in Subsection 4.1.

In particular, in Proposition 14 we determine a five-dimensional rational family defined over K with an explicitly given and simple **affine normal form** which defines an open subscheme $\tilde{H}^*_{3,4,3}$ of $\tilde{H}_{3,4,3}$.

[3] As an analogy, the reader might like to look at the Legendre family of elliptic curves E consisting of elliptic curves whose points of order 2 are K-rational.

This, together with more work done in [K2] yield that $\tilde{H}_{3,4,3}$ is a smooth rational K-variety of dimension 5 (Proposition 16).

For arbitrary K (e.g., $K = \mathbb{F}_q$), the natural map from $\tilde{\mathcal{H}}_{3,4,3}(K)$ to $\overline{\mathcal{H}}_{3,4,3}(K)$ is not surjective. But geometrically this is true (Lemma 11) and so for $K = \overline{K}$ we get that there is a surjective map with finite fibres from $\tilde{\mathcal{H}}_{3,4,3}(\overline{K})$ to $\overline{\mathcal{H}}_{3,4,3}(\overline{K})$.

The affine normal form of curves in $\tilde{\mathcal{H}}_{3,4,3}(K)$ can be transformed to equations in Weierstraß normal form. By computational methods Hindry and Ritzenthaler [HR] show (cf. Theorem 18) that this family is generic, and so we get in Theorem 19 the following geometric description of $\overline{H}_{3,4,3}$: It is an irreducible unirational variety of dimension 5, and the map $\overline{\mu}_3$ from $\overline{H}_{3,4,3}$ to the moduli space of hyperelliptic curves of genus 3 is generically finite and dominant. In particular, generic hyperelliptic curves of genus 3 over $\overline{K}$ can be given by affine normal forms with coefficients depending on five parameters.

1.2.5 The Spaces $\tilde{\mathcal{H}}^*_{3,4,4}$ and $\overline{\mathcal{H}}_{3,4,4}$

Similarly, to obtain simple equations for the curves covers in $\tilde{\mathcal{H}}'_{3,4,4}(K)$, we restrict our attention to the set $\tilde{\mathcal{H}}^*_{3,4,4}(K) := \tilde{\mathcal{H}}'_{3,4,4}(K) \cap \tilde{\mathcal{H}}^*_{3,4,3}(K)$. Thus, each curve cover $f_C : C \to \mathbb{P}^1_K$ in $\tilde{\mathcal{H}}^*_{3,4,4}(K)$ is ramified of type $(2,2)$ at P_0, P_1, P_{-1} and at one further point $P_t \in \mathbb{P}^1_K(K)$.

It turns out that the associated Hurwitz space $\tilde{H}^*_{3,4,4}$ is the union of precisely two irreducible components; cf. Corollary 25. Thus, using Lemma 26, it follows that the same is true for $\overline{H}_{3,4,4}$:

$$\overline{H}_{3,4,4} \;=\; V_1 \cup V_2.$$

We introduce in Subsection 4.2.2 two explicit families of curve covers by imposing polynomial inequalities (**Condition $\mathcal{U}$**) which define non-empty open subschemes U_1 and U_2 of $\tilde{H}^*_{3,4,4}$ (cf. Theorem 23) with the property that U_i maps to a dense subset of V_i for $i = 1, 2$.

The nature of the two families of curve covers is (generically) quite different. Those in the first family (which defines U_1) are curve covers $f_C : C \to \mathbb{P}^1_K$ with the property that f_C factors over an elliptic curve (so the monodromy group of f_C is contained in the dihedral group D_4), whereas those in the second family have generically the symmetric group S_4 as their monodromy group. In fact, it turns out that the desired Hurwitz space $\overline{H}_{3,4,4}(S_4)$ of Theorem 2 is an open subscheme of V_2; cf. Subsection 4.2.5.

2 Covers of Hyperelliptic Curves: Definitions and Notation

Throughout, K is a field of characteristic $\neq 2$, and $\overline{K}$ is an algebraic closure of K. If not otherwise stated, geometric objects are defined over K.

As was motivated in the introduction, this paper deals with cover maps from hyperelliptic curves C to the projective line $\mathbb{P}^1_K$ with various special properties. More precisely, we want to consider the set of all such cover maps (satisfying a fixed set of properties), modulo isomorphism or modulo equivalence of covers (cf. below).

For the convenience of the reader we give here an overview of the properties which we want to study.

It will be an important part of the paper to show that these sets have a "geometric interpretation" in terms of certain schemes, whose geometric properties are studied. Ideally, one would like to be able to identify these sets with the set of K-rational points of the associated scheme, but this is in general only possible when $K = \overline{K}$ is algebraically closed.

2.1 Covers of Hyperelliptic Curves C of Genus $g \geq 2$

M_g: the moduli scheme of curves of genus 3; its dimension is $3g-3$.
M_g^h: the locus of hyperelliptic curves of genus g on M_g; its dimension is $2g-1$.

Typical notation

- C, C_1, C_2: hyperelliptic curves of fixed genus $g \geq 2$,
- ω_C: the hyperelliptic involution of the hyperelliptic curve C,
- $f : C \to \mathbb{P}^1_K$ and $f_i : C_i \to \mathbb{P}^1_K$: non-constant morphisms ("*covers* ").

Isomorphism of covers. $f_1 \simeq f_2$ iff $\exists$ an isomorphism $\varphi : C_1 \xrightarrow{\sim} C_2$ with $f_2 \circ \varphi = f_1$.

Equivalence of covers. $f_1 \sim f_2$ iff $\exists \varphi : C_1 \xrightarrow{\sim} C_2$ and $\alpha \in \mathrm{Aut}(\mathbb{P}^1_K)$ with $f_2 \circ \varphi = \alpha \circ f_1$.

Example. If $C = C_1 = C_2$ and $\deg(f_i) = 2$ for $i = 1, 2$, then the covers f_i are equivalent (with $\varphi = id_C$) and are called *hyperelliptic covers* of C.

Isomorphism of triples (C, f_1, f_2), where $f_i : C \to \mathbb{P}^1_K$, are covers. (C, f_1, f_2) is isomorphic to (C', f_1', f_2') iff $\exists$ an isomorphism $\varphi : C \xrightarrow{\sim} C'$ with $f_i = f_i' \circ \varphi$ for $i = 1, 2$.

Notation. The isomorphism class of the triple (C, f_1, f_2) is denoted by $[C, f_1, f_2]$.

Convention. Let c be an isomorphism class of triples. The notation $c = [C, f_1, f_2]$ means that the triple (C, f_1, f_2) is a representative of c.

Factorization of covers. A cover $f_1 : C \to \mathbb{P}^1_K$ *factors over* a cover $f_2 : C \to \mathbb{P}^1_K$ iff $\exists$ a cover $\varphi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ such that $f_1 = \varphi \circ f_2$. If $\deg(f_2) = 2$, then f_1 factors over f_2 iff $f_1 = f_1 \circ \omega_C$. Thus, $f : C \to \mathbb{P}^1_K$ does not factor over a hyperelliptic cover of C iff $f \circ \omega_C \neq f$.

The basic Hurwitz sets

$\mathcal{H}_{g,n}(K)$: *Isomorphism* classes of covers of degree n that do not factor over a hyperelliptic cover.

$\overline{\mathcal{H}}_{g,n}(K)$: *Equivalence* classes of covers of degree n that do not factor over a hyperelliptic cover.

$\tilde{\mathcal{H}}_{g,n}(K)$: *Isomorphism* classes of triples (C, f_1, f_2) where $\deg(f_1) = n$, $\deg(f_2) = 2$, and f_1 does not factor over a hyperelliptic cover of C.

Group actions

The group $\mathrm{Aut}(\mathbb{P}^1_K) \simeq \mathrm{PGL}_2(K)$ acts on $\mathcal{H}_{g,n}(K)$ via $(\alpha, f) \mapsto \alpha \circ f$, and the product group $\mathrm{Aut}(\mathbb{P}^1_K) \times \mathrm{Aut}(\mathbb{P}^1_K)$ acts on $\tilde{\mathcal{H}}_{g,n}(K)$ via

$$((\alpha_1, \alpha_2), (C, f_1, f_2)) \mapsto (C, \alpha_1 \circ f_1, \alpha_2 \circ f_2).$$

Via these actions, the first two Hurwitz sets are naturally the orbit sets of the third set as follows:

$$\begin{aligned} \mathcal{H}_{g,n}(K) &= (1 \times \mathrm{Aut}(\mathbb{P}^1_K)) \backslash \tilde{\mathcal{H}}_{g,n}(K), \\ \overline{\mathcal{H}}_{g,n}(K) &= (\mathrm{Aut}(\mathbb{P}^1_K) \times \mathrm{Aut}(\mathbb{P}^1_K)) \backslash \tilde{\mathcal{H}}_{g,n}(K) \\ &= \mathrm{Aut}(\mathbb{P}^1_K) \backslash \mathcal{H}_{g,n}(K). \end{aligned}$$

Results

- $\tilde{\mathcal{H}}_{g,g+1}(K)$ is the set of K-rational points of a non-empty open subscheme $\tilde{H}_{g,g+1}$ of ${\mathbb{P}_K}^{3g+5}$, for every field K; cf. Proposition 6.

- $\mathcal{H}_{g,g+1}(\overline{K})$ is the set of $\overline{K}$-rational points of a unirational scheme $H_{g,g+1}$ of dimension $3g+2$. More precisely, for any field K we have a map $\mathcal{H}_{g,g+1}(K) \to H_{g,g+1}(K)$

which is compatible with base-change and which is a bijection when $K = \overline{K}$. We thus say that the scheme $H_{g,g+1}$ *classifies* the Hurwitz problem $\mathcal{H}_{g,g+1}(\cdot)$.

- $\overline{\mathcal{H}}_{g,g+1}(\overline{K})$ is the set of $\overline{K}$-rational points of a unirational scheme $\overline{H}_{g,g+1}$ of dimension $3g-1$. Moreover, the scheme $\overline{H}_{g,g+1}$ is a good geometric quotient $\pi_g : \tilde{H}_{g,g+1} \to \overline{H}_{g,g+1}$ of $\tilde{H}_{g,g+1}$, and so $\overline{H}_{g,g+1}$ classifies $\overline{\mathcal{H}}_{g,g+1}(\cdot)$; cf. Subsection 3.1.5.
- There is a surjective morphism $\mu_g : \tilde{H}_{g,g+1} \to M_g^h$, which is obtained by sending $[C, f_1, f_2]$ to the isomorphism class of C (over $\overline{K}$); cf. Corollary 7. Moreover, μ_g factors over π_g, and so we obtain a surjective morphism $\overline{\mu}_g : \overline{H}_{g,g+1} \to M_g^h$ with $\mu_g = \overline{\mu}_g \circ \pi_g$.

2.2 Covers of Hyperelliptic Curves C of Genus 3

In the following, C is a hyperelliptic curve of genus 3.

Special Hurwitz sets

$\overline{\mathcal{H}}_{3,4,k}(K)$: *Equivalence* classes of covers $f : C \to \mathbb{P}^1_K$ of degree 4 that do not factor over a hyperelliptic cover *and* with at least k ramification points (defined over $\overline{K}$) of type $(2,2)$; cf. Subsection 1.1.

$\overline{\mathcal{H}}_{3,4,4}(S_4)(K)$: *Equivalence* classes of covers $f : C \to \mathbb{P}^1_K$ of degree 4 with monodromy group S_4 and ramification type $(2,2)^4(2,1,1)^4$. (See Subsection 1.1 for the definitions of these terms.)

$\tilde{\mathcal{H}}'_{3,4,k}(K)$: *Isomorphism* classes of triples $[C, f_1, f_2] \in \tilde{\mathcal{H}}_{3,4}(K)$ such that f_1 has at least k ramification points of type $(2,2)$;

$\tilde{\mathcal{H}}_{3,4,3}(K)$ *Isomorphism* classes of triples $[C, f_1, f_2] \in \tilde{\mathcal{H}}'_{3,4,3}(K)$ with f_1 satisfying conditions (5), (6) and (7) in Subsection 4.1.

$\mathcal{U}_1(K)$ *Isomorphism* classes of triples $[C, f_1, f_2] \in \tilde{\mathcal{H}}'_{3,4,3}(K)$ for which C is given by an equation $F_1(T, X) = 0$ with F_1 as in (31).

$\mathcal{U}_2(K)$ *Isomorphism* classes of triples $[C, f_1, f_2] \in \tilde{\mathcal{H}}'_{3,4,3}(K)$ for which C is given by an equation $F_2(T, X) = 0$ with F_2 as in (32).

$\mathcal{U}(K) \quad = \quad \mathcal{U}_1(K) \cup \mathcal{U}_2(K)$

$\mathcal{U}'(K)$ *Isomorphism* classes of triples $[C, f_1, f_2] \in \mathcal{U}(K)$ such that f_1 has monodromy group S_4 and ramification type $(2,2)^4(2,1,1)^4$.

Results

- The Hurwitz space $\overline{H}_{3,4,3}$ which classifies $\overline{\mathcal{H}}_{3,4,3}(\cdot)$ is an irreducible unirational variety of dimension 5; cf. Theorem 19.
- The Hurwitz space $\overline{H}_{3,4,4}$ which classifies $\overline{\mathcal{H}}_{3,4,4}(\cdot)$ is the union of two irreducible unirational varieties V_1 and V_2 of dimension 4; cf. Theorem 20.
- The Hurwitz space $\overline{H}_{3,4,4}(S_4)$ which classifies $\overline{\mathcal{H}}_{3,4,4}(S_4)(\cdot)$ is irreducible of dimension 4 and is an open subscheme of one of the two components of $\overline{H}_{3,4,4}$; cf. Theorem 2 and Corollary 35.
- $\tilde{\mathcal{H}}_{3,4,3}(K)$ is the set of K-rational points of a smooth, rational scheme $\tilde{H}_{3,4,3}$, for every field K. Moreover, $\tilde{H}_{3,4,3}$ is a locally closed subscheme of $\tilde{H}_{3,4}$; cf. Proposition 16.
- $\mathcal{U}_i(K) = \bigcup_t \mathcal{U}_{i,t}(K)$ is the set of K-rational points of a rational scheme U_i of dimension 4, for every field K. Moreover, U_i is locally closed in $\tilde{H}_{3,4}$; cf. Theorem 23 and the discussion after Theorem 24.

- $\mathcal{U}'(K)$ is the set of K-rational points of a non-empty open subscheme U' of U_2, for every field K; cf. Corollary 35. Moreover, the image of U' (and of U_2) in M_3^h is irreducible of dimension 4; cf. Proposition 41.

Spaces defined for technical reasons

By Proposition 6, the isomorphism classes in $\tilde{\mathcal{H}}_{3,4}(K)$ can be represented by triples (C, f_C, π_C) with C a smooth curve of genus 3 in $\mathbb{P}^1_K \times \mathbb{P}^1_K$ and $f_C = \mathrm{pr}_1$ is of degree 4, $\pi_C = \mathrm{pr}_2$ is of degree 2 where pr_i is the i-th projection of $\mathbb{P}^1_K \times \mathbb{P}^1_K$ restricted to C. With this notation, we define:

$\tilde{\mathcal{H}}^*_{3,4,3}(K)$: $[C, f_C, \pi_C] \in \tilde{\mathcal{H}}_{3,4,3}(K)$ such that $P_{1,\infty} \notin C$ (see **Notation** in Subsection 4.1);

$\tilde{\mathcal{H}}^*_{3,4,4,t}(K)$: $[C, f_C, \pi_C] \in \tilde{\mathcal{H}}^*_{3,4,3}(K)$ with f_C ramified of type $(2,2)$ at $P_t = (1:t)$, for $t \in K \cup \{\infty\} \setminus \{0, 1, -1\}$.

We thus have the inclusions $\tilde{\mathcal{H}}^*_{3,4,4,t}(K) \subset \tilde{\mathcal{H}}^*_{3,4,3}(K) \subset \tilde{\mathcal{H}}_{3,4,3}(K) \subset \tilde{\mathcal{H}}_{3,4}(K)$. Moreover, put: $\tilde{\mathcal{H}}^*_{3,4,4}(K) = \bigcup_t \tilde{\mathcal{H}}^*_{3,4,4,t}(K)$.

3 Hyperelliptic Covers and Related Hurwitz Spaces

3.1 Hyperelliptic Curves in $\mathbb{P}^1_K \times \mathbb{P}^1_K$

As was mentioned in the previous sections, we are interested in studing triples (C, f_1, f_2), where C is a hyperelliptic curve of genus g, $f_1 : C \to \mathbb{P}^1_K$ a cover map of degree n with $f_1 \neq f_1 \circ \omega_C$ and $f_2 : C \to \mathbb{P}^1_K$ is a hyperelliptic cover, i.e., $\deg(f_2) = 2$. Note that Castelnovo's Inequality ([St], [K1]) implies that $n \geq g + 1$.

Each triple (C, f_1, f_2) as above defines (by the universal property of products) a unique K-morphism $\pi = \pi_{f_1,f_2} : C \to \mathbb{P}^1_K \times \mathbb{P}^1_K$ such that $f_i = \mathrm{pr}_i \circ \pi$, and the image $C_{f_1,f_2} = \pi_{f_1,f_2}(C)$ is an irreducible curve on the surface $\mathbb{P}^1_K \times \mathbb{P}^1_K$. Note that since $f_1 \neq f_1 \circ \omega_C$, the curve C_{f_1,f_2} is birationally equivalent to C (but C_{f_1,f_2} may be singular). Moreover, C_{f_1,f_2} is a divisor of type $(2, n)$ on $\mathbb{P}^1_K \times \mathbb{P}^1_K$ i.e.,

$$C_{f_1,f_2} \sim D_{2,n} := 2(P \times \mathbb{P}^1_K) + n(\mathbb{P}^1_K \times P), \quad \text{for } P \in \mathbb{P}^1_K(K).$$

In other words, $C_{f_1,f_2} \in |D_{2,n}|_K := \{D \in \mathrm{Div}(\mathbb{P}^1_K \times \mathbb{P}^1_K) : D \geq 0, D \sim D_{2,n}\}$, the *complete linear system* of effective K-rational divisors defined by $D_{2,n}$; cf. [Ha], p. 157 (when $K = \overline{K}$). Note that $|D_{2,n}|_K$ has the structure of a (naive) projective space of dimension $3n + 2$ over K. Thus, if we choose (homogeneous) coordinates on $\mathbb{P}^1_K$ such that $P = (0 : 1)$, then C_{f_1,f_2} is given by an equation $F(T_0, T_1; X_0, X_1) = 0$, where $F(T_0, T_1; X_0, X_1) \in K[T_0, T_1, X_0, X_1]$ is a polynomial of the form

$$F(T_0, T_1; X_0, X_1) \; = \; \sum_{i=0}^{n} \sum_{j=0}^{2} r_{ij} X_0^i X_1^{n-i} T_0^{2-j} T_1^j, \tag{1}$$

because the (bihomogeneous) monomials $\{X_0^i X_1^{n-i} T_0^{2-j} T_1^j\}_{i,j}$ form a basis of the K-vector space of K-rational sections of the sheaf $\mathcal{L}(D_{2,n})$. We note this result:

Proposition 3 *Every element in $\tilde{\mathcal{H}}_{g,n}(K)$ can be represented by a triple (C, f_C, π_C) where $C \subset \mathbb{P}^1_K \times \mathbb{P}^1_K$ is an irreducible curve of genus g contained in $|D_{2,n}|_K$, and $f_C = pr_1$, $\pi_C = pr_2$. Moreover, C can be given by an equation of the form* (1).

3.1.1 The Existence of $g+1$-Covers

In the case that $n = g+1$, much more can be said. For this, we first observe that a given hyperelliptic curve C/K of genus g always has subcover $f_1 : C \to \mathbb{P}^1_K$ of degree $g+1$ with $f_1 \neq f_1 \circ \omega_C$, provided that $C(K)$ is large enough. This follows from:

Lemma 4 *Let C/K be a curve of genus $g \geq 2$. If $T \subset C(K)$ is a set consisting of at least $g(g-1)+1$ K-rational points, then there is an effective divisor $D \in \mathrm{Div}(C)$ of degree $g+1$ with support in T such that* $\dim |D| = 1$ *and $|D|$ is base-point free. In particular, there exists a K-morphism $f : C \to \mathbb{P}^1_K$ of degree $g+1$.*

Proof. As is well-known (cf. [St], p. 35), there exists a non-special effective divisor $D_0 = P_1 + \ldots + P_g$ of degree g with support in T. Then for any $P \in C(K)$ we have that $\dim |D_0 + P| = 1$ by the Theorem of Riemann-Roch. Now if Q is a base point of $|D_0 + P|$, then $Q = P_i$ for some i with $1 \leq i \leq g$. Thus, if K_C denotes a canonical divisor, then by Riemann-Roch $\dim |K_C - D_0 + P_i - P| = \dim |D_0 + P - P_i| - 1 = 0$, and so $P \leq D_i$, where $D_i \geq 0$ is the unique effective divisor such that $D_i \sim K_C - D_0 + P_i$. (Note that by Riemann-Roch, $\dim |K_C - D_0 + P_i| = |D_0 - P_i| = 0$.) Thus, $|D_0 + P|$ is base point free whenever $P \not\leq \sum_{i=1}^{g} D_i$. Since the latter divisor has degree $g(g-1)$, it is clear that we can choose a $P \in T$ with this property.

Remark 5 Note that $|C(K)| > g(g-1)+1$ if $K = \overline{K}$ or if $K = \mathbb{F}_q$ with q sufficiently large. More precisely, we have that $q \geq 6g^2$ is enough because the Hasse-Weil bound (cf. [St], p. 198) yields that $|C(\mathbb{F}_q)| \geq (\sqrt{q} - g)^2 - g^2 + 1 \geq (\sqrt{6} - 1)^2 g^2 - g^2 + 1 > g^2 \geq g(g-1)+1$. (For example, if $g = 3$, then it is enough to have $q \geq 59$.)

The following result is fundamental for much of what follows.

Proposition 6 *The rule $(C, f_1, f_2) \mapsto C_{f_1,f_2}$ induces a bijection*

$$\kappa_g = \kappa_{g,K} : \tilde{\mathcal{H}}_{g,g+1}(K) \overset{\sim}{\to} |D_{2,g+1}|^{sm}_K,$$

where $|D_{2,g+1}|^{sm}_K \subset |D_{2,g+1}|_K$ denotes the subset of smooth divisors on $\mathbb{P}^1_K \times \mathbb{P}^1_K$ which are contained in $|D_{2,g+1}|_K$. Thus, $\tilde{\mathcal{H}}_{g,g+1}(K)$ is parameterized by the K-rational points of a non-empty open subscheme $\tilde{H}_{g,g+1}$ of $\mathbb{P}^{3g+5}_K$.

Proof. Let $[C, f_1, f_2]$ be in $\tilde{\mathcal{H}}_{g,g+1}(K)$. As was seen above, $C_{f_1,f_2} \sim D_{2,g+1}$. By the adjunction formula, the arithmetic genus of C_{f_1,f_2} is $p_a(C_{f_1,f_2}) = g$; cf. [Ha] or [K1]. Thus, C_{f_1,f_2} is a smooth curve on $\mathbb{P}^1_K \times \mathbb{P}^1_K$, and therefore $C_{f_1,f_2} \in |D_{2,g+1}|^{sm}_K$. Thus, since C_{f_1,f_2} depends only on the isomorphism class of (C, f_1, f_2), we obtain a map $\kappa_g : \tilde{\mathcal{H}}_{g,g+1}(K) \to |D_{2,g+1}|^{sm}_K$.

Now since $D_{2,g+1}$ is (very) ample (cf. [Ha], II, 7.6.2), every divisor $D \in |D_{2,g+1}|_K$ is connected ([Ha], III, 7.9.1) and so every $D \in |D_{2,g+1}|^{sm}_K$ is a smooth, irreducible curve of genus $g_D = p_a(D) = g$. Thus, the rule $D \mapsto (D, \mathrm{pr}_{1|D}, \mathrm{pr}_{2|D})$ induces a map $\kappa'_g : |D_{2,g+1}|^{sm}_K \to \tilde{\mathcal{H}}_{g,g+1}(K)$ which is clearly inverse to κ_g, and so both are bijections.

To prove the last assertion, let $N = 3g+5$, and let $\mathcal{D} := \mathcal{D}_{2,g+1}$ be the subscheme of $\mathbb{P}^N_K \times (\mathbb{P}^1_K \times \mathbb{P}^1_K)$ defined by equation (1) with $n = g+1$, where we view the coefficients (r_{ij}) as variables of $\mathbb{P}^N_K$. Let $p_{g,g+1} = (\mathrm{pr}_1)_{|\mathcal{D}} : \mathcal{D} \to \mathbb{P}^N_K$ be the projection. It is immediate that the fibres of $p_{g,g+1}$ at the K-rational points of $\mathbb{P}^N_K$ give precisely the elements of $|D_{2,g+1}|_K$, and that this construction is compatible with base change. Thus, $\mathcal{D}$ defines an algebraic family of divisors on $\mathbb{P}^1_K \times \mathbb{P}^1_K$ parametrized by $\mathbb{P}^N_K$ (in the sense of [Ha], p. 261). Thus, if $\tilde{H}_{g,g+1} \subset \mathbb{P}^N_K$ denotes the open subscheme of $\mathbb{P}^N_K$ where $p_{g,g+1}$ is smooth, then the fibres of $p_{g,g+1}$ at the points of $\tilde{H}_{g,g+1}(K)$ are precisely the elements of $|D_{2,g+1}|^{sm}_K$. Since this construction is functorial in K, we have our desired parametrization.

Finally, to see that $\tilde{H}_{g,g+1}$ is non-empty, we can use either Bertini's Theorem (cf. [Ha],II.8.18) or Lemma 4 to show that $|D_{2,g+1}|_{\overline{K}} \neq \emptyset$, which implies that $\tilde{H}_{g,g+1}(\overline{K}) \neq \emptyset$.

Corollary 7 *The rule $(C, f_1, f_2) \mapsto C$ induces a surjective morphism*

$$\mu_g : \tilde{H}_{g,g+1} \;\to\; M^h_g$$

with ${\mu_g}_*(\tilde{H}_{g,g+1})(\overline{K}) = \mathcal{M}^h_g(\overline{K})$.

Proof. Since $p_{g,g+1} : \mathcal{D}^{sm}_{2,g+1} \to \tilde{H}_{g,g+1}$ is a family of genus g curves, it induces (by the coarse moduli property of M_g) a morphism $\mu_g : \tilde{H}_{g,g+1} \to M_g$ such that $\mu_g(x) =$ (isomorphism class of) $p^{-1}_{2,g+1}(x) \in |D_{2,g+1}|^{sm}_{\overline{K}}$, for $x \in \tilde{H}_{g,g+1}(\overline{K})$; cf. [Ha], p. 347. Thus, via the identifications of (the proof of) Proposition 6, this morphism is given by the rule $(C, f_1, f_2) \mapsto C$. Moreover, since each C is hyperelliptic, it is clear that the image of μ_g is contained in the hyperelliptic locus M^h_g.

To see that μ_g is surjective, let $C/\overline{K}$ be an arbitrary hyperelliptic curve of genus g. By Lemma 4 we get a morphism $f := \varphi_D : C \to \mathbb{P}^1_{\overline{K}}$ of degree $g+1$ attached to a divisor $D \in \mathrm{Div}(C)$ such that

$$\dim|D| = 1, \ \deg(D) = g+1, \text{ and } |D| \text{ is base-point free.}$$

φ_D cannot factor over a hyperelliptic cover π_C because if $\varphi_D = \varphi\circ\pi_C$ for some $\varphi : \mathbb{P}^1_K \to \mathbb{P}^1_K$, then $\deg(\varphi) = \frac{g+1}{2}$ (so g is odd) and then $\dim|\varphi^*_D(\overline{P})| \geq \dim|\varphi^*(\overline{P})| = \frac{g+1}{2} > 1$, contradiction. Thus, $(C, \varphi_D, \pi_C) \in \tilde{H}_{g,g+1}(\overline{K})$, and hence μ_g is surjective.

3.1.2 Equations for Hyperelliptic Curves

We fix the genus g of curves.

In this subsection we shall assume that K has the following property: Every curve C of genus g over K has at least $g(g-1)+1$ K-rational points. As was mentioned in Remark 5, this condition is satisfied if $K = \overline{K}$ or if $K = \mathbb{F}_q$ with q sufficiently large.

To get equations to represent hyperelliptic curves C of genus g by plane curves we fix coordinates on $\mathbb{P}^1_K$. Then as explained above, each divisor D in $|D_{2,g+1}|_K$ can be represented by an equation $F(T_0, T_1; X_0, X_1) = 0$, where F has the form (1), i.e., F is homogeneous of degree 2 in T_0, T_1 and of degree $g+1$ in X_0, X_1, so

$$F(T_0, T_1; X_0, X_1) \;=\; \sum_{i=0}^{g+1}\sum_{j=0}^{2} r_{ij} X_0^i X_1^{g+1-i} T_0^{2-j} T_1^j, \qquad (2)$$

where $r_{ij} \in K$.

Since F is uniquely determined by D up to a multiplicative constant, we can view the coefficients of F as a point $P_D = (r_{00} : r_{01} : r_{02} : r_{10} : \ldots : r_{(g+1)2}) \in \mathbb{P}^N(K)$, where $N = 3g+5$, and the rule $D \mapsto P_D$ gives the inverse of the above mentioned parametrization of $|D_{2,g+1}|_K$. This gives a concrete realization of the projective space structure on $|D_{2,g+1}|_K$ over K.

Note that on the affine open subset $U = \{T_0 X_0 \neq 0\}$ of $\mathbb{P}^1_K \times \mathbb{P}^1_K$ we can represent each $D \in |D_{2,g+1}|_K$ by an affine equation

$$F(T, X) \;=\; \sum_{i=0}^{g+1}\sum_{j=0}^{2} r_{ij} X^{g+1-i} T^j, \qquad (3)$$

with $T = T_1/T_0$ and $X = X_1/X_0$ and $r_{ij} \in K$.

It follows from Lemma 4 that if C/K is a hyperelliptic curve of genus g, then C/K can be described by an affine equation in $\mathbb{A}^2_K$ in two variables T, X, where the degree in T is 2 and the degree in X is $g+1$, and so the total degree is $\leq g+3$, which is smaller than the degree of a Weierstraß equation (see also the footnote in Subsection 1.2.2).

3.1.3 Smoothness of Divisors

As was pointed out above, we are interested in smooth divisors. Having equations we can express this condition by discriminants and get the following explicit characterization of the divisors in $|D_{2,g+1}|^{sm}_K$.

Proposition 8 *Let $C \in |D_{2,g+1}|_K$ be given by $F(T_0, T_1; X_0, X_1)$ as in* (2)*, and let*

$$D^h_F(X_0, X_1) = \left(\sum_{i=0}^{g+1} r_{i1} X_0^i X_1^{g+1-i}\right)^2 - 4\left(\sum_{i=0}^{g+1} r_{i0} X_0^i X_1^{g+1-i}\right)\left(\sum_{i=0}^{g+1} r_{i2} X_0^i X_1^{g+1-i}\right) \quad (4)$$

denote its homogeneous discriminant *with respect to T. Then $C \in |D_{2,g+1}|^{sm}_K$ if and only if $D^h_F(X_0, X_1)$ is separable, i.e., D^h_F factors over $\overline{K}$ into $2(g+1)$ distinct linear factors.*

Proof.[4] From the proof of Proposition 4 we know that $C \in |D_{2,g+1}|^{sm}_K$ if and only if (2) defines an irreducible curve. To examine this condition, write F as

$$F(T_0, T_1; X_0, X_1) \;=\; g_0(X_0, X_1)T_1^2 + g_1(X_0, X_1)T_0T_1 + g_2(X_0, X_1)T_0^2.$$

Now if g_0, g_1, and g_2 have common factor g, then clearly F is reducible, and then $g^2 | D^h_F = g_1^2 - 4g_0g_2$, so D^h_F is not separable, and hence the proposition holds in this case. Moreover, if $g_0 = 0$, then F is again reducible (because $T_0|F$) and $D^h_F = g_1^2$ is not separable. Thus, assume henceforth that $\gcd(g_0, g_1, g_2) = 1$ and that $g_0 \neq 0$.

In this situation we see that F is irreducible if and only if its dehomogenization $\bar{F}(T, X) := F(1, T, 1, X) = \bar{g}_0(X)T^2 + \bar{g}_1(X)T + \bar{g}_2(X)$ is irreducible. Moreover, since our hypotheses imply that $\gcd(\bar{g}_0, \bar{g}_1, \bar{g}_2) = 1$ and $\bar{g}_0 \neq 0$, it follows from Gauss that $\bar{F}(T, X)$ is irreducible if and only if its discriminant $\bar{g}_1(X)^2 - 4\bar{g}_0(X)\bar{g}_2(X) = D^h_F(1, X)$ is not a square in $K[X]$. Thus, if $D^h_F(X_0, X_1)$ is separable, then clearly $D^h_F(1, X)$ cannot be a square and so $\bar{F}$ and F are irreducible, so C is smooth.

Conversely, suppose that $\bar{F}$ is irreducible, i.e., that $D^h_F(1, X)$ is not a square in $K[X]$. Then the affine curves

$$C_a : \quad \bar{F}(T, X) = 0 \quad \text{and} \quad C' : \quad Y^2 = D^h_F(1, X)$$

are both irreducible, and it is immediate that C' is birationally equivalent to C_a because the substitution $T = (Y - \bar{g}_1)/2\bar{g}_0$ defines a birational equivalence between them. Thus, since C has genus g, the same is true for C' (in the sense that its function field has genus g). Now since $D^h_F(X_0, X_1)$ is homogeneous of degree $2g+2$, we see that $\deg D^h_F(1, X) \leq 2g+2$. Thus, from the Hurwitz genus formula it follows that either $\deg(D^h_F(1, X)) = 2g+2$ and $D^h_F(1, X)$ has $2g+2$ distinct roots (in $\overline{K}$) or that $\deg(D^h_F(1, X)) = 2g+1$ and $D^h_F(1, X)$ has $2g+1$ distinct roots. Then in both cases $D^h_F(X_0, X_1) = X_0^{2g+2} D_h(1, X_1/X_0)$ is separable, so the assertion follows.

Remark 9 If $C \in |D_{2,g+1}|^{sm}_K$ is given by the equation (2), then the above proof shows implicitly that the hyperelliptic cover $\pi_C : C \to \mathbb{P}^1_K$ is ramified at the point $P_\infty = (0:1)$ if and only if X_0 is a factor of $D^h_F(X_0, X_1)$. This is equivalent to the condition that $D^h_F(0, 1) = r_{01}^2 - 4r_{00}r_{02} = 0$.

[4] We want to thank the anonymous referee for the key idea of this proof which considerably shortens our original argument.

3.1.4 Weierstraß Normal Form

We state an immediate consequence of the proof of Proposition 8 and Remark 9:

Proposition 10 *Assume that C is a curve of genus g given by*

$$F(T_0, T_1; X_0, X_1) \ = \ \sum_{i=0}^{g+1}\sum_{j=0}^{2} r_{ij} X_0^i X_1^{g+1-i} T_0^{2-j} T_1^j$$

with $r_{01}^2 - 4r_{00}r_{02} \neq 0$. Then

$$Y^2 X_0^{2g} = \left(\sum_{i=0}^{g+1} r_{i1} X_0^i X_1^{g+1-i}\right)^2 - 4\left(\sum_{i=0}^{g+1} r_{i0} X_0^i X_1^{g+1-i}\right)\left(\sum_{i=0}^{g+1} r_{i2} X_0^i X_1^{g+1-i}\right)$$

is a Weierstraß equation for C.

It is an easy exercise to get an analogous result (with a homogenous equation of degree $2g+1$) in the case that $(0:1)$ is a ramification point of f_2. Note that in the case that at least one of the Weierstraß points of C is K-rational the two cases can be transformed into each other by a K-rational projective transformation as usual.

3.1.5 The Hurwitz space $\overline{H}_{g,g+1}$

Let $G = \mathrm{PGL}_2$. Then the $G \times G$ action on $\mathbb{P}^1_{\overline{K}} \times \mathbb{P}^1_{\overline{K}}$ permutes the elements of the complete linear system $|D_{2,g+1}|_{\overline{K}}$ and hence induces an action on $\mathbb{P}^N_{\overline{K}}$ (via $p_{g,g+1}$).

Since $|D_{2,g+1}|^{sm}_{\overline{K}}$ is stable under this action, we have an induced action on $\tilde{H}_{g,g+1}$. By using the techniques of Mumford[Mu], one can show that the quotient scheme $\overline{H}_{g,g+1} = (G \times G)\backslash H_{g,g+1}$ exists, and that the quotient map

$$\pi_g : \tilde{H}_{g,g+1} \ \rightarrow \ \overline{H}_{g,g+1}$$

satisfies the properties of a good geometric quotient; cf. [K2]. Thus, since $\tilde{H}_{g,g+1}$ is a rational variety of dimension $3g+5$, it follows that $\overline{H}_{g,g+1}$ is a unirational variety of dimension $3g + 5 - 2\dim G = 3g - 1$. Moreover, it follows from properties of good geometric quotients and from Proposition 6 and its proof that $\kappa_{g,\overline{K}}$ induces a bijection

$$\overline{\kappa}_{g,\overline{K}} : \overline{\mathcal{H}}_{g,g+1}(\overline{K}) \quad \xrightarrow{\sim} \quad \overline{H}_{g,g+1}(\overline{K}).$$

More generally, if $L \subset \overline{K}$ is any subfield, then the bijection $\kappa_{g,L} : \tilde{H}_{g,g+1}(L) \xrightarrow{\sim} \tilde{H}_{g,g+1}(L)$ of Proposition 6 induces a map

$$\overline{\kappa}_{g,L} : \overline{\mathcal{H}}_{g,g+1}(L) = (G(L) \times G(L))\backslash\tilde{\mathcal{H}}_{g,g+1}(L) \quad \rightarrow \quad \overline{H}_{g,g+1}(L),$$

The maps $\overline{\kappa}_{g,L}$ are compatible with field extensions. We thus see that the quotient scheme $\overline{H}_{g,g+1}$ "classifies" the Hurwitz problem $\overline{\mathcal{H}}_{g,g+1}(\cdot)$. Note, however, that for an arbitrary subfield $L \subset \overline{K}$, the map $\overline{\kappa}_{g,L}$ is in general neither injective nor surjective.

3.2 Hurwitz Spaces with Given Ramification Type

We assume in this subsection that $K = \overline{K}$.

We have seen in Subsection 3.1.5 that the Hurwitz space $\overline{H}_{g,g+1}$ is a unirational variety of dimension $3g-1$. Moreover, since the forget map $\mu_g : (C, f_1, f_2) \mapsto C$ of

Corollary 7 is $G \times G$-invariant, it follows that μ_g factors over the quotient map π_g, and so there exists a unique morphism

$$\overline{\mu}_g : \overline{H}_{g,g+1} \ \rightarrow \ M_g^h$$

such that $\mu_g = \overline{\mu}_g \circ \pi_g$. Note that M_g^h has dimension $2g-1$ and so $\overline{\mu}_g$ is obviously not finite.

But till now we have used only rudimentary parts of information that one can connect with Hurwitz spaces and we did not restrict the ramification type of the morphism f_1. (Since f_2 is assumed to be a hyperelliptic cover, its ramification type has to be: $2g+2$ points are ramified of order 2.) Moreover, we did not prescribe the monodromy group of f_1. Since $\deg(f_1) = g+1$, the Riemann-Hurwitz genus formula shows that

$$4g = d_{f_1},$$

where d_{f_1} is the degree of the discriminant divisor of f_1.

The "generic" ramification type for covers of $\mathbb{P}^1_K$ of degree $g+1$ is expected to be as follows: Each ramified point on $\mathbb{P}^1_K$ has *one* ramified extension of ramification order 2 and so there should be $4g$ ramified points. Using the action of the automorphism group of $\mathbb{P}^1_K$ we should expect a "Hurwitz Space" of dimension $4g-3$. Speculating further that in our context we have to intersect this space with the space of covers attached to hyperelliptic curves, which is a subspace of the moduli space of curves of genus g of codimension $g-2$, we can expect that as result of the "generic" ramification situation we would get a space of dimension $3g-1$ and so exactly of the dimension of $\overline{H}_{g,g+1}$.

If we change the ramification conditions by assuming that more than one point in the fibres of f_1 can be ramified, then we will have fewer ramification points of $\mathbb{P}^1_K$ for f_1 and so the cover lies in a lower dimensional attached Hurwitz space. It is an interesting task to find out for which ramification type we get a finite map from the attached Hurwitz space to the moduli space of hyperelliptic curves, and to study the geometric properties of the resulting Hurwitz space.

To do this for $g = 3$ will be the content of the next section.

4 Hyperelliptic Curves of Genus 3

We assume in the whole section that K is a field with the property that every hyperelliptic curve of genus 3 has at least 7 K-rational points. For $K = \mathbb{F}_q$ it suffices that $q \geq 59$; cf. Remark 5. Hence we know by Lemma 4 (and the proof of Corollary 7) that for every hyperelliptic curve C of genus 3 there is a K-rational 4-cover

$$f_1 : C \rightarrow \mathbb{P}^1_K,$$

which does not factor over a hyperelliptic cover of C.

In fact we know more. In the isomorphism class of (C, f_1, f_2) we find a triple $(C', f_{C'}, \pi_{C'})$ with C' a smooth curve in $\mathbb{P}^1_K \times \mathbb{P}^1_K$ and $f_{C'} = \mathrm{pr}_{1|C'}$, $\pi_{C'} = \mathrm{pr}_{2|C'}$; cf. Proposition 6. Such triples are called "embedded".

In the following we shall choose such embedded triples in isomorphism classes in $\tilde{\mathcal{H}}_{3,4}(K)$ and indicate this choice by the notation (C, f_C, π_C) respectively $[C, f_C, \pi_C]$.

We recall that after this choice we have an affine equation for C:

$$C: \quad \sum_{i=0}^{4} \left(\sum_{j=0}^{2} r_{ij} T^j \right) X^{4-i} = 0$$

with $r_{ij} \in K$.

As was announced in Subsection 3.2, we introduce special ramification types for f_C.

We only allow ramification orders ≤ 2. (This is generically no restriction). So the ramified points $Q \in \mathbb{P}^1_K(\overline{K})$ of f_C are either of type $(2,1,1)$ (i.e., there is exactly one ramified point P_1 and two unramified points P_2, P_3 in the fiber $f_C^{-1}(Q)$) or it is of type $(2,2)$ (the fiber of $f_C^{-1}(Q)$ consists of two distinct ramified points P_1, P_2).

For $k = 3, 4$ we define the set $\tilde{\mathcal{H}}'_{3,4,k}(K)$ as the subset of $\tilde{\mathcal{H}}_{3,4}(K)$ consisting of those classes $[C, f_C, \pi_C]$ such that f_C has at least k ramification points on $\mathbb{P}^1_K(\overline{K})$ that ramify of type $(2,2)$. As we shall see below (cf. Remark 4.1.2), the set $\tilde{\mathcal{H}}'_{3,4,k}(K)$ consists of the K-rational points of a locally closed subscheme $\tilde{H}'_{3,4,k}$ of $\tilde{H}_{3,4}$.

Moreover, if we put $\overline{H}_{3,4,k} := \pi_3(\tilde{H}'_{3,4,k}) \subset \overline{H}_{3,4}$, then we see by the discussion in Subsection 3.1.5 that the elements of $\overline{H}_{3,4,k}(\overline{K})$ correspond (via $\overline{\kappa}_3$) to equivalence classes of pairs $(C, f_C) \in \overline{\mathcal{H}}_{3,4}(\overline{K})$ such that f_C has at least k ramification points on $\mathbb{P}^1_K(\overline{K})$ of type $(2,2)$. Note that the set $\tilde{\mathcal{H}}'_{3,4,k}(K)$ is stable under the action of the group $\mathrm{PGL}_2(K) \times \mathrm{PGL}_2(K)$. In the next two subsections we will introduce subsets $\tilde{\mathcal{H}}_{3,4,k}(K) \subset \tilde{\mathcal{H}}'_{3,4,k}(K)$ which serve (at least for $K = \overline{K}$) as a (partial) system of representatives for this action; cf. Lemmata 11 and 26. This allows us to find representatives of elements in $\overline{\mathcal{H}}_{3,4,k}(\overline{K})$ with simple equations.

4.1 The Hurwitz Space $\overline{H}_{3,4,3}$

Notation. Fix coordinates on $\mathbb{P}^1_K$. Let $P_\infty = (0:1) \in \mathbb{P}^1_K$ be the point at infinity, and let $P_a = (1:a)$, for $a \in K$. Thus, any K-rational point on the product surface $\mathbb{P}^1_K \times \mathbb{P}^1_K$ has the form $P_{a,b} := P_a \times P_b \in \mathbb{P}^1_K(K) \times \mathbb{P}^1_K(K)$, for $a, b \in K \cup \{\infty\}$.

Let $\tilde{\mathcal{H}}_{3,4,3}(K)$ denote the set of isomorphism classes in $\tilde{\mathcal{H}}_{3,4}(K)$ with representatives (C, f_C, π_C) satisfying the following conditions:

$$\begin{aligned} f_C^*(P_0) &= 2P_{0,\infty} + 2P_{0,0} && (5)\\ f_C^*(P_1) &= 2P_{1,1} + 2P_{1,\alpha}, \quad \text{for some } \alpha \in K, \alpha \neq 1 && (6)\\ f_C^*(P_{-1}) &= 2D, \text{ for some } D \in \mathrm{Div}(C), D \neq P_{-1,\infty} + P_{-1,0}, D \neq 2P, \forall P. && (7)\end{aligned}$$

Thus, f_C is ramified at P_0, P_1, P_{-1} of type $(2,2)$ and so $(C, f_C, \pi_C) \in \tilde{\mathcal{H}}'_{3,4,3}(K)$.

Although the above curves might seem to be rather special, they are general enough to represent all curves in $\overline{\mathcal{H}}_{3,4,3}(\overline{K})$. More precisely (cf. [K2]):

Lemma 11 *The map $\tilde{\mathcal{H}}_{3,4,3}(\overline{K}) \to \overline{\mathcal{H}}_{3,4,3}(\overline{K})$, which sends isomorphism classes of triples (C, f_C, π_C) to equivalence classes of covers $f_C : C \to \mathbb{P}^1{}_{\overline{K}}$, is surjective and has finite fibres.*

The strategy to find equations for embedded curves attached to elements in $\tilde{\mathcal{H}}_{3,4,3}(K)$ is obvious. We shall "plug in" the ramification conditions into the equation

$$C: \quad \sum_{i=0}^{4} \left(\sum_{j=0}^{2} r_{ij} T^j \right) X^{4-i}$$

and get normal forms for curves in $\tilde{\mathcal{H}}_{3,4,3}(K)$ and so, by using Lemma 11, for representatives for all classes in $\overline{\mathcal{H}}_{3,4,k}(\overline{K})$.

Here are immediate consequences of our normalization for the coefficients r_{ij}:

First we use that $P_{0,0}$ is a point on C ramified of order 2. It follows that $r_{40} = 0 = r_{30}$.

Similarly, since $P_{0,\infty}$ is ramified, we have $r_{00} = 0 = r_{10}$. Hence the equation for C has the form

$$C : F(X,T) = \sum_{i=0}^{4} (r_{i1} T + r_{i2} T^2) X^{4-i} + r_{20} X^2.$$

Next we observe that $P_\infty \in \mathbb{P}^1_K$ is not a ramification point of the hyperelliptic cover π_C, for otherwise $\pi_C^* P_\infty = 2P_{0,\infty}$, and then $P_{0,\infty}$ would be ramified under both projections of $\mathbb{P}^1_K \times \mathbb{P}^1_K$, which contradicts the smoothness of $C \subset \mathbb{P}^1_K \times \mathbb{P}^1_K$. This yields:

The discriminant of $F(X,T)$ with respect to T has 8 distinct zeroes and so

$$D_F(X) = \left(\sum_{i=0}^{4} r_{i1} X^{4-i}\right)^2 - 4r_{20}X^2 \left(\sum_{i=0}^{4} r_{i2} X^{4-i}\right)$$

is a separable polynomial. Thus, by Proposition 10 we obtain that

$$W_C : \quad Y^2 = \left(\sum_{i=0}^{4} r_{i1} X^{4-i}\right)^2 - 4r_{20}X^2 \left(\sum_{i=0}^{4} r_{i2} X^{4-i}\right)$$

is a Weierstraß equation for C.

Recall that the fiber of P_1 consists of the points $P_{1,1}$ and $P_{1,\alpha}$, for some $\alpha \neq \infty$. Thus, $P_{1,\infty} \notin C$, and hence it follows that

$$r_{01} + r_{02} \neq 0.$$

The equation $F(X,T)$ is uniquely determined up to a non-zero scalar factor, so we normalize it. Thus, we can and will assume that

$$r_{02} = 1 - r_{01}.$$

To continue, we will exploit the other ramification conditions. For this, it is useful to write down an elementary statement about points ramified of type $(2,2)$ under the map f_C.

4.1.1 A Criterion for Points of Type $(2,2)$

Lemma 12 *Let $Q(X) = AX^4 + BX^3 + CX^2 + DX + E \in K[X]$.*

(a) *If $A \neq 0$, then $Q(X) = Aq(X)^2$ for some monic quadratic polynomial $q(X) = X^2 + bX + c$ if and only if*

$$u_1 := B\Delta - 8A^2D = 0 \text{ and } u_2 := 64EA^3 - \Delta^2 = 0, \quad \text{where } \Delta = 4AC - B^2. \tag{8}$$

Moreover, if this holds, then $b = B/(2A)$ and $c = \Delta/(8A^2)$, and so $q(X)$ has distinct roots in $\overline{K}$ if and only if $\delta_1 = B^2 - 2\Delta = 3B^2 - 8AC \neq 0$. In addition, (8) implies that

$$g \;:=\; AD^2 - EB^2 \;=\; 0. \tag{9}$$

(b) *If $E \neq 0$, then $Q(X) = E(aX^2 + bX + 1)^2$, for some $a, b \in K$ if and only if*

$$u_1^* := D\Delta' - 8E^2B = 0 \text{ and } u_2^* := 64AE^3 - (\Delta')^2 = 0, \text{ where } \Delta' = 4EC - D^2. \tag{10}$$

Moreover, if this holds, then also (9) holds and $b = D/(2E)$ and $a = \Delta'/(8E^2)$, and so $b^2 - 4a \neq 0$ if and only if $\delta_2 := D^2 - 2\Delta' = 3D^2 - 8EC \neq 0$.

(c) *$Q(X) = \lambda(\alpha X^2 + \beta X + \gamma)^2$, for some $\alpha, \beta, \gamma, \lambda \in K$ with $\lambda \neq 0$ if and only if $u_1 = u_2 = u_1^* = u_2^* = 0$, and then also $g = 0$. Moreover, in that case the discriminant $\delta := \lambda(\beta^2 - 4\alpha\gamma) = 0$ if and only if $\delta_1 = \delta_2 = \delta_3 = 0$, where $\delta_3 := C^2 - 36AE$.*

Proof. (a) Since $q(X)^2 = X^4 + 2bX^3 + (b^2 + 2c)X^2 + 2bcX + c^2$, we see that the equation $Q(X) = Aq(X)^2$ implies that

$$B = 2Ab, \quad C = A(b^2 + 2c), \quad D = 2Abc \quad \text{and} \quad E = Ac^2. \tag{11}$$

Thus $\Delta = 4AC - B^2 = 8A^2c$ and so $B\Delta = 16A^3bc = 8A^2D$ and $\Delta^2 = 64A^4c^2 = 64A^3E$. This shows that (8) holds and that $b = B/(2A)$ and $c = \Delta/(8A^2)$. Moreover, since $b^2 - 4c = \left(\frac{B}{2A}\right)^2 - 4\frac{\Delta}{8A^2} = \frac{B^2-2\Delta}{4A^2} = \frac{3B^2-8AC}{4A^2}$, we see that $q(X)$ has distinct roots in $\overline{K}$ if and only if $B^2 - 2\Delta = 3B^2 - 8AC \neq 0$. In addition, $EB^2 = (Ac^2)(2Ab)^2 = A(2Abc)^2 = AD^2$, which proves (9). Conversely, suppose that (8) holds. Put $b = B/(2A)$ and $c = \Delta/(8A^2)$. Then $Aq(X)^2 = AX^4 + BX^3 + (\frac{B^2}{4A} + \frac{\Delta}{4A})X^2 + \left(B\frac{\Delta}{8A^2}\right)X + \frac{\Delta^2}{64A^3} = Q(X)$ by (8).

(b) Apply part (a) to $Q_1(X) = X^4Q(1/X) = A + BX + CX^2 + DX^3 + EX^4$.

(c) Suppose first that $u_1 = u_2 = u_1^* = u_2^* = 0$. If $A \neq 0$, then part (a) shows that $Q(X) = \lambda(\alpha X^2 + \beta X + \gamma)$ with $\lambda = A$, $\alpha = 1$, $\beta = \frac{B}{2A}$ and $\gamma = \frac{\Delta}{8A^2}$, and that $g = 0$. Similarly, if $E \neq 0$, then part (b) shows that $Q(X) = \lambda(\alpha X^2 + \beta X + \gamma)$ with $\lambda = E$, $\alpha = \frac{\Delta'}{8E^2}$, $\beta = \frac{D}{2E}$ and $\gamma = 1$. Now suppose that $A = E = 0$. Then the condition $u_2 = 0$ implies that $B = 0$, and $u_2^* = 0$ shows that $D = 0$. Thus, $Q(X) = CX^2 = \lambda(\beta X)^2$, for suitable $\lambda \in K^\times$, $\beta \in K$. Clearly $g = 0^3 - 0^3 = 0$.

Conversely, suppose that $Q(X) = \lambda(\alpha X^2 + \beta X + \gamma)^2$. If $AE \neq 0$, then by parts (a) and (b) we see that (8) and (10) hold. If $A \neq 0$ and $E = 0$, then $\gamma = 0$, and then $D = 2\lambda\gamma = 0$. Thus $\Delta' = 0$ and so $u_1^* = u_2^* = 0$. Moreover, $u_1 = u_2 = 0$ by part (a). Similarly, if $A = 0$ and $E \neq 0$, then $\alpha = B = \Delta = 0$, so $u_1 = u_2 = 0$, and $u_1^* = u_2^* = 0$ by part(b). Finally, if $A = E = 0$, then $\alpha = \gamma = 0$, so $B = D = \Delta = \Delta' = 0$, and hence (8) and (10) hold trivially.

To prove the assertion about δ, note first that δ only depends on Q and not on the choice of $\lambda, \alpha, \beta, \gamma$, as is easy to check. Now if $A \neq 0$, then a short computation (using $\lambda = A$) shows that $\delta_1 = 4A\delta$, $\delta_2 = 4E\delta$ and $\delta_3 = \delta(C + \frac{3\Delta}{4A})$, so $\delta = 0 \Rightarrow \delta_1 = \delta_2 = \delta_3 = 0 \Rightarrow \delta_1 = 0 \Rightarrow \delta = 0$, which proves the assertion in this case. Similarly, if $E \neq 0$, then $\delta_1 = 4E\delta$, $\delta_2 = 4A\delta$ and $\delta_3 = \delta(C + \frac{3\Delta'}{4E})$, and so the assertion follows. Finally, if $A = E = 0$, then $\delta = \lambda\beta^2 = C$ and $\delta_1 = \delta_2 = 0$, $\delta_3 = C^2 = C\delta$, so we see that here $\delta = 0 \Leftrightarrow \delta_3 = 0 \Leftrightarrow \delta_1 = \delta_2 = \delta_3 = 0$, and so the assertion holds here well.

We will use the above Lemma 12 in the following way:

Proposition 13 *Let $C \subset \mathbb{P}^1_K \times \mathbb{P}^1_K$ be a genus 3 curve given by an equation $F(T, X) = 0$ of the form (3) with $n = 4$, and let $f_C = (pr_1)_{|C} : C \to \mathbb{P}^1_K$ be the associated cover of degree 4. Moreover, let $t \in K$, and let $u_1, u_2, u_1^*u_2^*$ and δ_i be the elements associated to $Q(X) = F(t, X)$. Then $f_C^*(P_t)$ has type $(2, 2)$ if and only if $u_1 = u_2 = u_1^* = u_2^* = 0$ and some $\delta_i \neq 0$, for $i = 1, 2, 3$.*

Proof. Suppose first that $\deg Q = 4$. Then $Q(X) = A(X - \alpha_1)^{m_1} \cdots (X - \alpha_s)^{m_s}$ with distinct $\alpha_1, \ldots, \alpha_s \in \overline{K}$, and then $f_C^*(P_t) = \sum m_i P_{t,\alpha_i}$. It is thus clear that $f_C^*(P_t)$ has type $(2, 2)$ if and only if $Q(X)/A$ is a square with distinct roots, and so the assertion follows from Lemma 12(c).

Next, suppose that $\deg Q = 4 - m$, where $m \geq 1$. Then $P_{t,\infty}$ has multiplicity m in $f_C^*(P_t)$, and so $f_C^*(P_t)$ has type $(2, 2) \Leftrightarrow f_C^*(P_t) = 2P_{t,\infty} + 2P_{t,\alpha}$, for some $\alpha \in K$ $\Leftrightarrow Q(X) = \lambda(X - \alpha)^2$, for some $\alpha \in K$, $\lambda \in K^\times \Leftrightarrow Q(X)/\lambda$ is a square and $\delta \neq 0$. Thus, the assertion follows from Lemma 12(c).

Application to the ramification at P_1. We apply this to the fiber over P_1 and recall that $f_C^*(P_1) = 2(P_{1,1} + P_{1,\alpha})$. So

$$F(1, X) = (X - 1)^2(X - \alpha)^2.$$

Thus, from (11) it follows that

$$\begin{array}{rclrcl} r_{11} + r_{12} & = & -2(\alpha + 1), & r_{20} + r_{21} + r_{22} & = & \alpha^2 + 4\alpha + 1, \\ r_{31} + r_{32} & = & -2\alpha(\alpha + 1), & r_{41} + r_{42} & = & \alpha^2. \end{array} \qquad (12)$$

Note that the first relation shows that $\alpha = -\frac{1}{2}(r_{11} + r_{12} + 2)$.

Application to the ramification at P_{-1}. We have still to exploit that P_{-1} is ramified of type $(2,2)$, and we have to use elimination to find a system of independent parameters for $\tilde{\mathcal{H}}_{3,4,3}(K)$. It is not surprising that we have to make a case discussion. This leads two subsets $\tilde{\mathcal{H}}^*_{3,4,3}(K)$ and $\tilde{\mathcal{H}}^{**}_{3,4,3}(K)$ which cover $\tilde{\mathcal{H}}_{3,4,3}(K)$. Following our strategy expressed in the introduction, we shall discuss only $\tilde{\mathcal{H}}^*_{3,4,3}(K)$ in the sequel; cf. [K2] for $\tilde{\mathcal{H}}^{**}_{3,4,3}(K)$. The set $\tilde{\mathcal{H}}^*_{3,4,3}(K)$ is defined by

$$\tilde{\mathcal{H}}^*_{3,4,3}(K) = \{[C, f_C, \pi_C] \in \tilde{\mathcal{H}}_{3,4,3}(K) \text{ with } P_{-1,\infty} \notin C\}.$$

The assumption that $P_{-1,\infty} \notin C$ is equivalent to the condition that $a_0 := 1 - 2r_{01} \neq 0$ because if F^h is the bi-homogenization of F, then $F^h(1,-1;0,1) = r_{02} - r_{01} = 1 - 2r_{01}$.

We now use that P_{-1} is ramified of type $(2,2)$. Since the leading coefficient of $F(-1,X)$ is $a_0 \neq 0$, condition (7) is equivalent to the assertion that

$$F(-1,X) = a_0(X^2 + bX + c)^2,$$

for some $b, c \in K$, and so by Lemma 12(a) we obtain the relations (8) which yield

$$r_{32} - r_{31} \;=\; \tfrac{1}{8}(r_{12} - r_{11})\Delta \quad\text{and}\quad r_{42} - r_{41} \;=\; \tfrac{1}{64}a_0\Delta^2, \tag{13}$$

with $\Delta = (4a_0(r_{20} - r_{21} + r_{22}) - (r_{12} - r_{11})^2)/a_0^2$. Thus, by using the first relation of (13) and the third relation of (12) we can solve for r_{31} and r_{32} and so we obtain

$$r_{31} = -\alpha^2 - \alpha - \frac{1}{16}(r_{12} - r_{11})\Delta$$

and

$$r_{32} = -\alpha^2 - \alpha + \frac{1}{16}(r_{12} - r_{11})\Delta.$$

Similarly, we can solve for r_{41} and r_{42} by using the second relation of (13) and the fourth relation of (12), and so we obtain

$$r_{41} = \frac{1}{2}\alpha^2 - \frac{1}{128}(1 - 2r_{01})\Delta^2$$

and

$$r_{42} = \frac{1}{2}\alpha^2 + \frac{1}{128}(1 - 2r_{01})\Delta^2$$

with

$$\Delta = \frac{4(1 - 2r_{01})(\alpha^2 + 4\alpha + 1 - 2r_{21}) - (r_{12} - r_{11})^2}{(1 - 2r_{01})^2}.$$

Moreover, since $X^2 + bX + c$ has distinct roots, it follows from Lemma 12(a) that

$$(r_{12} - r_{11})^2 \neq 2(1 - 2r_{01})^2\Delta.$$

We summarize our results as follows:

Proposition 14 *Every element in $\tilde{\mathcal{H}}^*_{3,4,3}(K)$ has a representative (C, f_C, π_C) with a curve C given by an equation $F(T,X) = 0$, where*

$$F(T,X) \;=\; \sum_{i=0}^{4}(r_{i1}T + r_{i2}T^2)X^{4-i} + r_{20}X^2 \tag{14}$$

and the $r_{ij} \in K$ are such that the polynomial

$$D_F(X) := \left(\sum_{i=0}^{4} r_{i1}X^{4-i}\right)^2 - 4r_{20}X^2\left(\sum_{i=0}^{4} r_{i2}X^{4-i}\right) \tag{15}$$

is separable of degree 8 *and such that the following relations hold:*

$$\begin{aligned} r_{02} &= 1 - r_{01} & (16)\\ r_{22} &= \alpha^2 + 4\alpha + 1 - r_{20} - r_{21} & (17)\\ r_{31} &= -\alpha^2 - \alpha - \tfrac{1}{16}a_1\Delta & (18)\\ r_{32} &= -\alpha^2 - \alpha + \tfrac{1}{16}a_1\Delta & (19)\\ r_{41} &= \tfrac{1}{2}\alpha^2 - \tfrac{1}{128}a_0\Delta^2 & (20)\\ r_{42} &= \tfrac{1}{2}\alpha^2 + \tfrac{1}{128}a_0\Delta^2 & (21)\end{aligned}$$

in which $\alpha = -\frac{1}{2}(r_{11} + r_{12} + 2) \neq 1$, $a_0 = 1 - 2r_{01} \neq 0$, $a_1 = r_{12} - r_{11}$ *and*

$$\Delta = \Delta(r_{01}, r_{11}, r_{12}, r_{21}) := (4a_0(\alpha^2 + 4\alpha + 1 - 2r_{21}) - a_1^2)/a_0^2. \qquad (22)$$

In addition, we have that

$$a_1^2 \neq 2a_0^2\Delta. \qquad (23)$$

A Weierstraß Normal Form for C *is given by*

$$\begin{aligned} Y^2 \;=\; & (r_{01}X^4 + r_{11}X^3 + r_{21}X^2 - (\alpha^2 + \alpha + \tfrac{1}{16}a_1\Delta)X + \tfrac{1}{2}\alpha^2 - \tfrac{1}{128}a_0\Delta^2)^2 \\ & -4r_{20}X^2((1 - r_{01})X^4 + r_{12}X^3 + (\alpha^2 + 4\alpha + 1 - r_{20} - r_{21})X^2 \\ & +(-\alpha^2 - \alpha + \tfrac{1}{16}a_1\Delta)X + \tfrac{1}{2}\alpha^2 + \tfrac{1}{128}a_0\Delta^2).\end{aligned}$$

Conversely, if $C \subset \mathbb{P}^1_K \times \mathbb{P}^1_K$ *is a curve given by an equation satisfying the above relations, then the isomorphism class of* (C, f_C, π_C) *is in* $\tilde{\mathcal{H}}^*_{3,4,3}(K)$.

It remains to prove the "converse" part of the proposition.

If $F(T,X) \in K[T,X]$ satisfies the conditions above, then $D^h_F(X_0, X_1) = X_0^8 D_F(X_1/X_0)$ has 8 distinct linear factors, and so by Proposition 8 we see that the equation $F(T,X) = 0$ defines a smooth curve $C \in |D_{2,4}|^{sm}$. Moreover, we know that $P_{-1,\infty} \notin C$ because $r_{02} - r_{01} = 1 - 2r_{01} = a_0 \neq 0$.

It remains to show that C satisfies conditions (5) – (7). Now if we substitute $T = 0, 1, -1$ in $F(T,X)$, then we obtain that

$$\begin{aligned} F(0,X) &= r_{20}X^2 & (24)\\ F(1,X) &= (X-1)^2(X-\alpha)^2 & (25)\\ F(-1,X) &= a_0\left(X^2 + \frac{a_1}{2a_0}X + \frac{\Delta}{8}\right)^2, & (26)\end{aligned}$$

as a quick computation (using MAPLE) shows. Since $a_0 \neq 0$, $a_1^2 \neq 2a_0^2\Delta$ and $r_{20} \neq 0$ (else D_F would be a square), it follows that (5) – (7) hold, and so (C, f_C, π_C) lies in a class of $\tilde{\mathcal{H}}^*_{3,4,3}(K)$.

In the following Example 15, we give, for all fields K of odd characteristic, examples of curves C/K for which (C, f_C, π_C) is a representative of a class in $\tilde{\mathcal{H}}^*_{3,4,3}(K)$. In particular, it follows that $\tilde{\mathcal{H}}^*_{3,4,3}(K) \neq \emptyset$.

Example 15 (a) Choose $r_{01} = r_{20} = 1$ and $r_{11} = r_{12} = r_{21} = 0$. Then $a_0 = \alpha = -1$, and so we can define $r_{02}, r_{22}, \ldots, r_{42}$ by (16) – (22). This gives the polynomial

$$F_{01}(T,X) \;=\; X^4T - X^2(3T^2 - 1) + T$$

Here $D_{F_{01}}(X) = X^8 + 14X^4 + 1$ and $\Delta = 8$. Using a computer algebra program (such as MAPLE) we see that the discriminant of $D_{F_{01}}$ is $2^{40}3^4$, and so it follows that $D_{F_{01}}$

is separable of degree 8 whenever $\mathrm{char}(K) \neq 3$. Thus $F_{01}(T,X)$ defines a smooth genus 3 curve $C \in \tilde{\mathcal{H}}_{3,4,3}(K)$ whenever $\mathrm{char}(K) \neq 3$.

(b) Choose $r_{01} = r_{21} = 1$, $r_{20} = 2$ and $r_{11} = r_{12} = 0$. Then as before $a_0 = \alpha = -1$, and so we can define $r_{02}, r_{22}, \ldots, r_{42}$ by (16) – (22). This gives the polynomial

$$F_{02}(T,X) \;=\; X^4T - X^2(5T^2 - T - 2) - \frac{3}{2}T^2 + \frac{5}{2}T$$

Here $\Delta = 16$ and $D_{F_{02}}(X) = X^8 + 2X^6 + 46X^4 + 17X^2 + \frac{25}{4}$, which (by MAPLE) has discriminant $2^{20}5^{10}13^2 17^4$. Thus $F_{02}(T,X)$ defines a smooth genus 3 curve $C \in \tilde{\mathcal{H}}_{3,4,3}(K)$ whenever $\mathrm{char}(K) \neq 5, 13, 17$.

4.1.2 Scheme Structures

By using Proposition 13, one can show that $\tilde{\mathcal{H}}'_{3,4,k}(K)$ can be identified (via $\kappa_{3,K}$) with the set of K-rational points of a locally closed subset $\tilde{H}'_{3,4,k}$ of $\tilde{H}_{3,4}$; cf. [K2]. More precisely, one can show (by considering $(\mathbb{P}^1_K)^k \times \tilde{H}_{3,4}$) that $\tilde{H}'_{3,4,k} = V \cap U$, where V (respectively, U) is a closed (respectively, open) subscheme of $\tilde{H}_{3,4}$ which is invariant under the $G \times G$-action. It thus follows that $\overline{H}_{3,4,k} = \pi_3(\tilde{H}'_{3,4,k})$ is also locally closed. Thus, both $\tilde{H}'_{3,4,k}$ and $\overline{H}_{3,4,k}$ have an induced scheme structure.

In a similar way one can interpret $\tilde{\mathcal{H}}_{3,4,3}(K)$, $\tilde{\mathcal{H}}^*_{3,4,3}(K)$, and $\tilde{\mathcal{H}}^{**}_{3,4,3}(K)$ as the sets of K-rational points of locally closed subschemes $\tilde{H}_{3,4,3}$, $\tilde{H}^*_{3,4,3}$, and $\tilde{H}^{**}_{3,4,3}$ of $H'_{3,4,3}$, respectively. It is then immediate that $\tilde{H}^*_{3,4,3}$ and $\tilde{H}^{**}_{3,4,3}$ are open subschemes of $\tilde{H}_{3,4,3}$.

With the explicit description for $\tilde{H}^*_{3,4,3}$ one is not far away from a geometrical description of $\tilde{H}_{3,4,3}$, though some work still has to be done; cf. [K2] for the details. One gets:

Proposition 16 *The Hurwitz space $\tilde{H}_{3,4,3}$ is a smooth rational variety of dimension* 5 *containing $\tilde{H}^*_{3,4,3}$ as open subscheme which is isomorphic to an open subscheme of $\mathbb{A}^5_K$.*

An explicit parametrization of $\tilde{H}^*_{3,4,3}$ is given by Proposition 14.

Remark 17 The equations $F(X,T)$ for the curves in $\tilde{\mathcal{H}}^*_{3,4,3}(K)$ are of degree 5 if $r_{01} = 1$ (with the normalization made above). This is the case in our examples.

Hence we find a hyperplane of $\tilde{H}^*_{3,4,3}$ for which the corresponding hyperelliptic curves C are described by plane equations of degree 5.

4.1.3 From Hurwitz Spaces to Moduli Spaces

Recall from Subsection 3.2 that we have the morphism

$$\overline{\mu}_3 : \overline{H}_{3,4} \;\to\; M_3^h,$$

which is not (generically) finite, as we have already seen. But by Lemma 11 and Proposition 16 we know that we have a surjective map from the 5-dimensional irreducible scheme $\tilde{H}_{3,4,3}$ to $\overline{H}_{3,4,3}$ and from Proposition 14 we get a family of Weierstraß equations for the hyperelliptic curves which define points in this space.

We repeat their definition: Take s_1, s_2, s_3, t, u as algebraically independent elements over K. Put

$$\alpha := -\frac{1}{2}(s_2 + t + 2),$$

$$\Delta := (4(1-2s_1)(\alpha^2 + 4\alpha + 1 - 2s_3) - (t - s_2)^2)/(1-2s_1)^2,$$

and define the hyperelliptic curve $C(s_1, s_2, s_3, t, u) =: C$ by the Weierstraß equation

$$\begin{aligned} Y^2 \quad = \quad & (s_1X^4 + s_2X^3 + s_3X^2 - (\alpha^2 + \alpha + \tfrac{1}{16}(t - s_2)\Delta)X + \tfrac{1}{2}\alpha^2 - \tfrac{1}{128}(1 - 2s_1)\Delta^2)^2 \\ & -4uX^2((1 - s_1)X^4 + tX^3 + (\alpha^2 + 4\alpha + 1 - u - s_3)X^2 \\ & -(\alpha^2 + \alpha + \tfrac{1}{16}(s_2 - t)\Delta)X + \tfrac{1}{2}\alpha^2 + \tfrac{1}{128}(1 - 2s_1)\Delta^2). \end{aligned}$$

Theorem 18 (Hindry-Ritzenthaler) *The family of curves* $C(s_1, s_2, s_3, t, u)$ *is generic of dimension* 5.

The proof of this theorem ([HR]) is based on computational methods as developed in [LR] and crucially enhanced by ideas of Marc Hindry that enable to compute the dimension of the tangent space around an arbitrary point of the family.[5] We use Lemma 11 and get from Proposition 16 and Theorem 18:

Theorem 19 *The Hurwitz space* $\overline{H}_{3,4,3}$ *is an irreducible unirational variety of dimension* 5 *which is covered by the irreducible and rational variety* $\tilde{H}_{3,4,3}$ *of dimension* 5.

The restriction of the forget map $\overline{\mu}_3$ *to* $\overline{H}_{3,4,3}$ *is generically finite and dominant in the moduli space* M_3^h.

4.2 The Hurwitz space $\overline{H}_{3,4,4}$

The aim of this subsection is to describe $\overline{H}_{3,4,4}$. From the geometrical point of view, the main result is the following statement:

Theorem 20 *The Hurwitz space* $\overline{H}_{3,4,4}$ *is a scheme which has two irreducible components* V_1 *and* V_2, *both unirational of dimension* 4.

The proof of this theorem uses, in addition to the information we get in this paper, rather complicated constructions from algebraic geometry; cf. [K2] for the details.

In this paper we shall find equations for two 4-dimensional families of hyperelliptic curves C which define subsets $\mathcal{U}_1(K)$, $\mathcal{U}_2(K)$ of $\tilde{\mathcal{H}}_{3,4,3}(K)$. The cover maps f_C of these curves C have at least 4 ramification points of type $(2, 2)$, so $\mathcal{U}_i(K) \subset \tilde{\mathcal{H}}'_{3,4,4}$. Moreover, each $\mathcal{U}_i(K)$ is the set of K-rational points of a subscheme $U_i \subset \tilde{H}'_{3,4,4}$ whose image in $\overline{\mathcal{H}}_{3,4,4}$ is dense in V_i, for $i = 1, 2$.

4.2.1 Two Natural Subspaces of $\overline{H}_{3,4,4}$

Curves with elliptic differentials. First look at hyperelliptic curves C with cover map

$$\pi_E : C \to E$$

where E is an elliptic curve and $\deg(\pi_E) = 2$, i.e., C has an elliptic differential of degree 2. This implies that the Jacobian variety J_C of C has an elliptic subvariety $E^* = \pi_E^*(E)$ and a two-dimensional abelian subvariety A with $A \cap E^* = E^*[2]$. Such hyperelliptic curves are well-studied and it is known that over $\overline{K}$ they generate a 3-dimensional subspace of the moduli space of hyperelliptic curves of genus 3 ([GS]).

Assume that

$$\alpha : E \to \mathbb{P}^1_K$$

is a cover of degree 2, not induced by the hyperelliptic cover. Then

$$f_C : C \xrightarrow{\alpha\circ\pi_E} \mathbb{P}^1_K$$

[5] We are very thankful to Marc Hindry and Christophe Ritzenthaler for answering our question concerning the dimension of the above family very quickly.

is a cover of degree 4 which does not factor over the hyperelliptic cover, and hence the class $[C, f_C, \pi_C]$ satisfies the conditions imposed on elements in $\tilde{\mathcal{H}}_{3,4}(K)$.

We examine the ramification structure of f_C. By the Hurwitz genus formula there are 4 points $Q_1, \ldots, Q_4$ on $E(\overline{K})$ that are ramified under π_E, and α has four ramification points $P_1, \ldots, P_4$ on $\mathbb{P}^1_K(\overline{K})$.

Assume that α can be chosen such that the associated involution σ_α (with $\mathrm{Aut}(\alpha) = \langle \sigma_\alpha \rangle$) has no fixed points in common with $Q_1, \ldots, Q_4$. Then the points $\alpha^{-1}P_1, \ldots \alpha^{-1}P_4$ are unramified under π_E and hence have ramification type $(2,2)$ with respect to f_C. Thus, (C, f_C, π_C) represents an element in $\tilde{\mathcal{H}}'_{3,4,4}(K)$, and the equivalence class of f_C defines an element in $\overline{\mathcal{H}}_{3,4,4}(K)$.

Remark 21 (a) The assumptions made for α can be satisfied for K large enough (e.g., for $K = \overline{K}$).

(b) " Generically" the monodromy group of f_C is the dihedral group D_4.

(c) Again "generically" we have that $\alpha(Q_i) \neq \alpha(Q_j)$ for $i \neq j$ and so the ramification type of $\alpha(Q_i)$ is $(2,1,1)$.

Remark 22 The above covers $f_C = \alpha \circ \pi_E$ are clearly *imprimitive* in the sense that they factor over a nontrivial subcover. Now it turns out that *every* imprimitive cover $f_C : C \to \mathbb{P}^1_K$ in $\mathcal{H}_{3,4}(K)$ is of the above form.

Indeed, suppose that $f_C = \alpha \circ \pi$, for some subcover $\pi : C \to C'$ of degree 2. By Riemann-Hurwitz we have that $g_{C'} = 0, 1$, or 2. But if $g_{C'} = 0$, then π is equivalent to the hyperelliptic cover π_C, and so f_C factors over π_C, contradiction. Next, if $g_{C'} = 2$, then $\alpha = \pi_{C'}$ is (equivalent to) the hyperelliptic cover of C'. But then α is induced by the hyperelliptic cover of C, and so f_C factors over π_C, contradiction. Thus, we must have $g_{C'} = 1$, so $C' = E$ is an elliptic curve.

Covers with monodromy group equal to S_4. For more details of the following discussion see [FK].

Assume that

$$f_C : C \to \mathbb{P}^1_K$$

is primitive, and that there are exactly 4 points $P_1, \ldots, P_4$ of ramification type $(2,2)$ and 4 ramification points $Q_1, \ldots, Q_4$ of ramification type $(2,1,1)$. It follows that the discriminant divisor of f_C is equal to $\Delta_C = 2P_1 + \cdots + 2P_4 + Q_1 + \cdots + Q_4$ and that the monodromy group of f_C is equal to S_4. Let $\tilde{C}$ be the cover curve obtained as the Galois closure of f_C.

Let G_2 be a non-cyclic subgroup of S_4 of order 4 and different from the Klein group in A_4. Then $G_2 = N_{S_4}(\tau)$ is the normalizer of a transposition τ, and hence any two such groups are conjugate in S_4. By analyzing the ramification groups, we obtain that $C' := \tilde{C}/G_2$ is a curve of genus 3. Moreover, if P_2 denotes the unique 2-Sylow subgroup of S_4 which contains G_2, then $\tilde{C}/P_2$ has genus 0. Thus, C' has the following property:

There is a degree-2 cover $u_2 : C' \to \mathbb{P}^1_K$, and so C' is hyperelliptic, and a degree-3 cover $f_3 : \mathbb{P}^1_K \to \mathbb{P}^1_K$ such that the Galois closure of $f_6 := f_3 \circ u_2$ is $\tilde{C}$ and the monodromy group of f_6 is the symmetric group S_4. Hence $f_6 : C' \to \mathbb{P}^1$ is a trigonal cover in the sense of Donagi-Livné. The cover maps $\varphi_1 : \tilde{C} \to C'$ and $\varphi_2 : \tilde{C} \to C$ induce (via conorm respectively norm maps) a correspondence $\varphi_{2*} \circ \varphi_1^*$ and so a morphism from $\mathrm{Pic}^0_{C'}$ to Pic^0_C which is (essentially) as constructed by Smith [Sm].

In other words, C is the curve obtained from C' by Smith's construction. The *special property* here is that C is hyperelliptic.

4.2.2 Equations for $\tilde{H}^*_{3,4,4}$

We use the assumptions and results from Subsection 4.1 and add the condition that for fixed $t \in K \cup \{\infty\} \setminus \{0, 1, -1\}$, the point $P_t \in \mathbb{P}^1_K$ is ramified under f_C with ramification type $(2, 2)$, i.e. $f_C^*(P_t) = 2D_t$, for some $D_t \in \mathrm{Div}(C)$, $D_t \neq 2P$ for any $P \in C(K)$.

The subset of isomorphism classes $[C, f_C, \pi_C] \in \tilde{\mathcal{H}}^*_{3,4,3}(K)$ for which C satisfies this additional condition is denoted by $\tilde{\mathcal{H}}^*_{3,4,4,t}(K)$.

Moreover, define $\tilde{\mathcal{H}}^*_{3,4,4}(K) = \bigcup_t \tilde{\mathcal{H}}^*_{3,4,4,t}(K)$, where the union is over all $t \in K \cup \{\infty\} \setminus \{0, 1, -1\}$. It is not difficult to see (cf. [K2]) that $\tilde{\mathcal{H}}^*_{3,4,4}(\overline{K})$ is the set of $\overline{K}$-rational points of the scheme $\tilde{H}^*_{3,4,4} := \tilde{H}^*_{3,4,3} \cap \tilde{H}'_{3,4,4}$; cf. Subsection 4.1.2.

We will find equations for two rational families of triples (C, f_C, π_C) with $[C, f_C, \pi_C] \in \tilde{H}^*_{3,4,4}$; these will then also give equations for two *open subschemes* U_i of $\tilde{H}^*_{3,4,4}$ whose union $U = U_1 \cup U_2$ is dense in $\tilde{H}^*_{3,4,4}$.

We use the notation introduced in Subsection 4.1. Our aim is to show that we can find (Zariski-)open conditions for the parameter set $r_{01}, r_{11}, r_{12}, t$ such that for the resulting subset $U(K) \subset \mathbb{A}^4_K(K) = K^4$ we get: There is exactly one triple (C, f_C, π_C) with $[C, f_C, \pi_C] \in \tilde{\mathcal{H}}_{3,4,4,t}(K)$ with coefficients r_{01}, r_{11}, r_{12} in its normal form, and the other coefficients in the normal form are given by rational expressions in these parameters.

It is not surprising that the formulas become a bit involved, and to write them down it is useful to introduce some additional notation.

Notation. For $r_{01}, r_{11}, r_{12}, t \in K$, put

$$\begin{array}{lllllllll} a_0 & = & 1 - 2r_{01} & a_3 & = & r_{01}r_{11} + r_{01}r_{12} - r_{11} & a_5 & = & (1 - r_{01})t + r_{01} \\ a_1 & = & r_{12} - r_{11} & \alpha & = & -\frac{1}{2}(r_{11} + r_{12} + 2) & a_6 & = & r_{12}t + r_{11}. \\ a_2 & = & r_{12} + r_{11} & & & & & & \end{array}$$

$$\begin{aligned} A(T) &= r_{01}T + (1 - r_{01})T^2, && (27) \\ B(T) &= r_{11}T + r_{12}T^2, && (28) \\ C(T) &= r_{20} + r_{21}T + (\alpha^2 + 4\alpha + 1 - r_{20} - r_{21})T^2, && (29) \end{aligned}$$

where r_{20} and r_{21} have to be determined as functions of $r_{01}, r_{11}, r_{12}, t$.
For later use define

$$r_{201} := \frac{ta_3^2}{4a_0a_5} \quad \text{and} \quad r_{211} := \frac{4a_0(4\alpha r_{01} + (\alpha + 1)^2) - a_1^2}{8a_0}. \qquad (30)$$

We add open conditions for the parameter set:

Condition $\mathcal{U}$. We assume that $r_{01}, r_{11}, r_{12}, t \in K$ are such that

- $a_0 \neq 0$, i.e., $r_{01} \neq \frac{1}{2}$,
- $a_5 \neq 0$, i.e., either $r_{01} = 1$ or $r_{01} \neq 1$ and $t \neq \frac{r_{01}}{-1 + r_{01}}$
- $a_6 \neq 0$,
- $\alpha a_3 \neq 0$ and so $d := 4\alpha a_0 a_3 \neq 0$.
- Moreover, assume that $q \neq 0$, where

$$q := (a_2(r_{11}t + r_{12} - 3a_6)a_5 + 2a_6^2)/(t - 1).$$

Claim. If $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ is a curve with cover maps f_C and π_C such that the isomorphism class of (C, f_C, π_C) is in $\tilde{\mathcal{H}}^*_{3,4,4,t}(K)$ and the parameters $r_{01}, r_{11}, r_{12}, t \in K$ satisfy Condition $\mathcal{U}$, then C can be described by one of the following two types of equations (31) and (32), as will be explained presently. Define

$$F_1(T,X) = A(T)X^4 + B(T)X^3 + C(T)X^2 + \alpha B(T)X + \alpha^2 A(T), \tag{31}$$

where $A(T)$, $B(T)$ and $C(T)$ are as in (27) – (29) with $r_{20} = r_{201}$ and $r_{21} = r_{211}$, and

$$F_2(T,X) = F_1(T,X) + \frac{d}{q}G(T,X), \tag{32}$$

with

$$G(T,X) \ = \ (c_2(1-T^2) + a_6T(1-T))X^2 + c_3T(1-T)X + c_4T(1-T),$$

and

$$c_2 \ = \ \frac{ta_3}{a_0}, \quad c_3 \ = \ \frac{a_1a_6}{2a_0}, \quad c_4 \ = \ -\frac{\alpha a_1a_2a_5a_6}{q}.$$

Proof of the claim. C is a curve satisfying the hypotheses of Condition $\mathcal{U}$, so C belongs to a triple with isomorphism class in $\tilde{\mathcal{H}}^*_{3,4,3}(K)$, and hence by Proposition 14 we know that C is given by an equation $F(T,X) = 0$ of the form (14), where the coefficients r_{ij} satisfy the conditions (16) – (21) and are uniquely determined by C.

We thus have that $F(T,X) = \sum_{i=0}^4 A_i(T)X^{4-i}$, with $A_0(T) = A(T)$, $A_1(T) = B(T)$ and $A_2 = C(T)$, where A, B, C are as in (27) – (29). Moreover, by Proposition 14 we also know that D_F is separable of degree 8.

Since $f_C^*(P_t) = 2D_t$ and $P_{t,\infty} \notin C$ by hypothesis, we see that

$$F(t,X) = a(X^2 + bX + c)^2,$$

for some $b, c \in K$, where $a = A_0(t) = ta_5 \neq 0$ is the leading coefficient of $F(t,X)$. Thus, by Lemma 12(a) we obtain the relations (8) and (9), which can be written in the form $u_1 = u_2 = g = 0$, where

$$u_1 \ = \ 4a_5a_6c - 8ta_5^2a_7 - ta_6^3, \quad u_2 \ = \ 64t^2a_5^3a_8 - (4a_5c - ta_6^2)^2, \quad g \ = \ a_6^2a_8 - a_5a_7^2,$$

with

$$c = C(t) = (1-t^2)r_{20} + (t-t^2)r_{21} + t^2(\alpha^2 + 4\alpha + 1),$$

$$a_7 = A_4(t)/t = r_{32}t + r_{31} = -(t+1)(\alpha^2+\alpha) + \frac{1}{16}(t-1)a_1\Delta(r_{01}, r_{11}, r_{12}, r_{21}),$$

and

$$a_8 = A_5(t)/t = r_{42}t + r_{41} = \frac{1}{2}(t+1)\alpha^2 + \frac{1}{128}(t-1)a_0\Delta(r_{01}, r_{11}, r_{12}, r_{21})^2$$

with $\Delta(r_{01}, r_{11}, r_{12}, r_{21})$ as in (22). (Here we've used the relations (17) – (21).)

To analyze these relations, we first observe (by using MAPLE) that g factors as

$$64a_0^4g = (1-t^2)(4a_0r_{21} - c_{211})(4a_0qr_{21} - c_{212}) = (1-t^2)g_1g_2, \tag{33}$$

in which $g_1 = 4a_0(r_{21} - r_{211}) = 4a_0r_{21} - c_{211}$ and $g_2 = 4a_0qr_{21} - c_{212}$ with $c_{211} := 4a_0r_{211}$ and $c_{212} := qc_{211} + 4a_0a_6d$.

Since $(1-t^2) \neq 0$ we have to discuss two cases.

Case 1. $g_1 = 0$. This implies that

$$r_{21} = r_{211} = \frac{4a_0(4\alpha r_{01} + (\alpha+1)^2) - a_1^2}{8a_0}.$$

Substituting this into (22) and simplifying (with MAPLE's help) yields that

$$\Delta(r_{01}, r_{11}, r_{12}, r_{21}) = \Delta(r_{01}, r_{11}, r_{12}, \frac{4a_0(4\alpha r_{01} + (\alpha+1)^2) - a_1^2}{8a_0}) = 8\alpha.$$

Thus, by (18) we obtain that $r_{31} = \alpha r_{11}$ and similarly (19) yields $r_{32} = \alpha r_{12}$. Moreover, from (20) and (21) we obtain that $r_{41} = r_{01}\alpha^2$ and $r_{42} = (1 - r_{01})\alpha^2$. It remains to determine r_{20}.

Substituting the values for r_{21}, r_{31}, r_{32} and r_{42} into the equation $u_1 = 0$, we obtain

$$(1 - t^2)a_6 h_1 / a_0 = 0$$

with

$$h_1 = 4a_0 a_5 r_{20} - t a_3^2.$$

Hence by our assumptions we get that $h_1 = 0$ and so

$$r_{20} = r_{201} = \frac{t a_3^2}{4 a_0 a_5}.$$

By (23) we have that $a_1^2 \neq 2a_0^2 \Delta_1 = 16 a_0^2 \alpha$. Moreover, since

$$F_1(t, X) = a_5 t \left(X^2 + \frac{a_6}{2a_5} X + \alpha \right)^2,$$

we see that $F_1(t, X)$ has two distinct roots if and only if $a_6^2 \neq 16 a_5^2 \alpha$. We note this inequality and will find it in Theorem 23 below as a part of Inequality (35).

Case 2. $g_2 = 0$. Since $a_0 \neq 0$ and $q \neq 0$ it is clear that $g_2 = 0$ is equivalent to

$$r_{21} = r_{212} := \frac{c_{212}}{4a_0 q} = r_{211} + \frac{d a_6}{q}.$$

From the relation between r_{211} and r_{212} we see immediately from (22) that

$$\Delta(r_{01}, r_{11}, r_{12}, r_{21}) = \Delta(r_{01},\, r_{11},\, r_{12},\, r_{212}) = \Delta(r_{01}, r_{11}, r_{12}, r_{211}) - \left(\frac{d a_6}{q}\right)\left(\frac{8}{a_0}\right).$$

Define

$$\begin{array}{rcl} r_{311} & := & -\alpha^2 - \alpha - \frac{1}{16} a_1 \Delta(r_{01}, r_{11}, r_{12}, r_{211}), \\ r_{321} & := & -\alpha^2 - \alpha + \frac{1}{16} a_1 \Delta(r_{01}, r_{11}, r_{12}, r_{211}), \\ r_{411} & := & \frac{1}{2}\alpha^2 - \frac{1}{128} a_0 \Delta^2(r_{01}, r_{11}, r_{12}, r_{211}), \\ r_{421} & := & \frac{1}{2}\alpha^2 + \frac{1}{128} a_0 \Delta^2(r_{01}, r_{11}, r_{12}, r_{211}). \end{array}$$

By (18) – (19) it follows that $r_{31} = r_{311} + (\frac{d}{q})c_3$ and $r_{32} = r_{321} - (\frac{d}{q})c_3$, with $c_3 = \frac{a_1 a_6}{2a_0}$. Similarly, from (20) – (21) we see that $r_{41} = r_{411} + \frac{d}{q}c_4$, and $r_{42} = r_{421} - \frac{d}{q}c_4$, with $c_4 = -\frac{\alpha a_1 a_2 a_5 a_6}{q}$. In addition, since the condition $u_1 = 0$ means that $r_{20} = r_{202} := \frac{c_{202}}{4a_0 a_5 q} = r_{201} + \frac{d}{q}c_2$, where $c_2 = \frac{t a_3}{a_0}$, we obtain that

$$F(T, X) = F_1(T, X) + \frac{d}{q} G(T, X) = F_2(T, X).$$

Moreover, by (23) we have that $a_1^2 \neq 16 a_0^2 \frac{\Delta(r_{01}, r_{11}, r_{12}, r_{21})}{8} = 16 a_0^2 (\alpha - \frac{d a_6}{a_0 q})$, and since

$$F_2(t, X) = a_5 t \left(X^2 + \frac{a_6}{2a_5} X + (\alpha - \frac{(t-1) d a_1}{2 a_0 q}) \right)^2, \tag{34}$$

we see that $F_2(t, X)$ has two distinct roots if and only if $a_6^2 \neq 16 a_5^2 (\alpha + (1 - t)\frac{d a_1}{2 a_0 q})$.

We summarize and get the following result:

Theorem 23 *Fix $t \in K \setminus \{0, \pm 1\}$, and let $U_{3,4,4,t}$ denote the open subscheme of $\tilde{H}^*_{3,4,4,t}$ where Condition $\mathcal{U}$ holds.*

Then $U_{3,4,4,t}$ is the union of the two three-dimensional varieties $U_{1,t}$ and $U_{2,t}$ which are given as follows:
There exist unique elements $r_{01}, r_{11}, r_{12} \in K$ such that a curve C representing an element in $U_{i,t}(K)$ is given by the equation

$$F_i(T, X) = 0,$$

where $F_i(T, X)$ is defined as above by equation (31) or (32).

Moreover, we have that $D_{F_i}(X)$ is separable of degree 8 and that

$$a_1^2 \neq 16 a_0^2 \, \Delta_i' \quad \text{and} \quad a_6^2 \neq 16 a_5^2 \Delta_i'' \tag{35}$$

where $\Delta_1' = \Delta_1'' = \alpha$, $\Delta_2' = \alpha - \frac{da_6}{a_0 q}$, $\Delta_2'' = \alpha + (1-t)\frac{da_1}{2a_0 q}$.

Conversely, every equation of the above form with $\alpha a_0 a_3 a_5 q \neq 0$ defines a curve C which corresponds to a point in $U_{3,4,4,t}(K)$.

After our discussion, one only has to prove the converse part of the theorem and this is, in principle, an easy check (with the help of MAPLE).

Let us emphasize that a lot more work has to be invested if one wants to remove the restrictions given by Condition $\mathcal{U}$; cf. [K2] for the details. The result is the following:

Theorem 24 ([K2]) *For each $t \in K \cup \{\infty\}$, $t \neq 0, \pm 1$, the Hurwitz space $\tilde{H}^*_{3,4,4,t}$ consists of two irreducible, rational components $\tilde{H}^*_{3,4,4,t,1}$ and $\tilde{H}^*_{3,4,4,t,2}$ of dimension 3.*

We now use this result to study the Hurwitz space $\tilde{H}^*_{3,4,4}$. Taking $t = \tau$ as a variable over K and replacing K by $K(\tau)$, we obtain the 3-dimensional rational scheme $\tilde{H}^*_{3,4,4,\tau}$ over $K(\tau)$. We would like to interpret $\tilde{H}^*_{3,4,4,\tau}$ as the generic fibre of $\tilde{H}^*_{3,4,4}$ with respect to the "morphism" from $\tilde{H}^*_{3,4,4}$ to $\mathbb{P}^1_K$ which takes a point corresponding to C to t.

But this does not lead to a morphism because the $(2,2)$-ramification point t is not uniquely determined by (C, f_C, π_C) since f_C may have more than 4 ramification points of type $(2,2)$.

However, we can cover $\tilde{H}^*_{3,4,4}$ by a locally closed subscheme $\tilde{H}^\dagger_{3,4,4} \subset \mathbb{P}^1_K \times \tilde{H}^*_{3,4,3}$ such that the fibre at $t \in K$ of $p_1 := (pr_1)_{|\tilde{H}^\dagger_{3,4,4}} \to \mathbb{P}^1_K$ can be identified with $\tilde{H}^*_{3,4,4,t}$ and such that its generic fibre is $\tilde{H}^*_{3,4,4,\tau}$. From this it is not difficult to deduce the following result (cf. [K2]):

Corollary 25 *The Hurwitz space $\tilde{H}^*_{3,4,4}$ consists of two irreducible, rational components of dimension 4.*

From this corollary it is easy to deduce Theorem 20 by using the following fact (cf. [K2]) which is a partial analogue of Lemma 11:

Lemma 26 *The map $\tilde{\mathcal{H}}^*_{3,4,4}(\overline{K}) \to \overline{\mathcal{H}}_{3,4,4}(\overline{K})$ is surjective and has finite fibres.*

The following examples (as well as other examples) are used in the proof of Theorems 20 and 23 to show that the Hurwitz spaces $\tilde{H}^*_{3,4,4}$ and hence $\overline{H}_{3,4,4}$ are non-empty.

Example 27 (a) Substituting $r_{01} = 1$, $r_{11} = 0$, and $r_{12} = 4$ in $F_1(T, X)$ yields the polynomial

$$F_{11}(T, X) \;=\; TX^4 + 4T^2X^3 + (4tT^2 - 2T - 4t)X^2 - 12T^2X + 9T.$$

By MAPLE we find that the discriminant of $F_{11}(T,X)$ with respect to T is

$$D_{F_{11}}(X) \ = \ X^8 - 4X^6 + 64tX^5 + (64t^2+22)X^4 - 192tX^3 - 36X^2 + 81,$$

which in turn has discriminant $d_{F_{11}}(t) = 2^{64} \cdot 3^{12} \cdot (t^4+14t^2+1)t^4(t-1)^4(t+1)^4$. It thus follows from Proposition 8 that the equation $F_{11}(T,X) = 0$ defines a smooth genus 3 curve C_{11} on $\mathbb{P}^1_K \times \mathbb{P}^1_K$ whenever $\mathrm{char}(K) \nmid d^*_{F_{11}} = 3(t^4+14t^2+1)$. Moreover, since $a_0 = -a_5 = -1$, $\alpha - 1 = -4$ and $a_1^2 - 16a_0^2\Delta'_1 = 784 = 2^47^2$ and $a_6^2 - 16a_5^2\Delta''_1 = 784t^2$, it follows that $C_{11} \in \tilde{\mathcal{H}}_{3,4,3,t}$ whenever $\mathrm{char}(K) \nmid f_{11}(t) := 7d^*_{F_{11}} = 21(t^4+14t^2+1)$. To check the ramification behavior of the associated 4-cover $f_{11} : C_{11} \to \mathbb{P}^1_K$, we compute its discriminant divisor which is given by the discriminant $\mathrm{disc}(F_{11})$ of $F_{11}(T,X)$ with respect to X. By MAPLE we find that

$$\mathrm{disc}(F_{11}) = 2^{12}3^2T^2(T-1)^2(T+1)^2(T-t)^2\mathrm{disc}^*(F_{11}),$$

where

$$\mathrm{disc}^*(F_{11}) := (t^2+12)T^4 - 4tT^3 + (4-2t^2)T^2 + 4tT + t^2.$$

Since the discriminant of $\mathrm{disc}^*(F_{11})$ is (by MAPLE) $2^{12}3^2t^4(t^4+14t^2+1)$, we see that $\mathrm{disc}^*(F_{11})$ has four distinct roots (in $\overline{K}$) whenever $\mathrm{char}(K) \nmid 2^{12}3^2t^4(t^4+14t^2+1)$. Since this condition follows from the previous one involving $f_{11}(t)$, we see that whenever $\mathrm{char}(K) \nmid f_{11}(t) = 21(t^4+14t^2+1)$, then F_{11} is ramified of type $(2,2)$ at $T = 0, 1, -1, t$ and of type $(2,1,1)$ at the 4 distinct roots of $\mathrm{disc}^*(F_{11})$.

For example, if we specialize to the case $t = 2$, then $f_{11}(2) = 3^2 \cdot 5 \cdot 7$, so we see that whenever $\mathrm{char}(K) > 7$, then the equation

$$F_{112}(T,X) \ = \ TX^4 + 4T^2X^3 + (8T^2 - 2T - 8)X^2 - 12T^2X + 9T$$

defines a smooth curve C_{112} of genus 3 on $\mathbb{P}^1_K \times \mathbb{P}^1_K$ whose associated 4-cover $f_{112} : C_{112} \to \mathbb{P}^1_K$ is ramified of type $(2,2)$ at $T = 0, 1, -1, 2$ and of type $(2,1,1)$ at the roots of $4T^4 - 2T^3 - T^2 + 2T + 1$.

(b) Substituting $r_{01} = 1$, $r_{11} = -1$, $r_{12} = 2$ and $t = 2$ in $F_2(T,X)$ yields the polynomial

$$F_{21}(T,X) = TX^4 + (2T^2 - T)X^3 + (\tfrac{7}{3}T^2 + \tfrac{9}{4}T - \tfrac{22}{3})X^2 + (3T^2 - \tfrac{9}{2}T)X + \tfrac{17}{4}T - 2T^2.$$

By MAPLE, the discriminant $D_{F_{21}} \in K[X]$ has degree 8, and its discriminant is

$$d_{F_{21}} = (2)^{12}(5)^2(11)^4(13)^2(17)^6(19)^2(47)^2(191)^2(3)^{-14},$$

so F_{21} defines a smooth curve whenever $\mathrm{char}(K) > 19$ and $\neq 47, 191$. The discriminant of F_{21} (and of the cover) is

$$\mathrm{disc}(F_{21}) = 18^2T^2(T-1)^2(T+1)^2(T-2)^2\mathrm{disc}^*(F_{21}),$$

where $\mathrm{disc}^*(F_{21}) = 15929408 - 7986000T - 7592871T^2 + 6397864T^3 - 1297776T^4$. Since the discriminant of $\mathrm{disc}^*(F_{21})$ is $-(2)^{22}(3)^{17}(7)^6(11)^{12}(379)^3$, we see that the polynomial $\mathrm{disc}^*(F_{21})$ has distinct roots if, in addition, $\mathrm{char}(K) \neq 379$. Thus, for $\mathrm{char}(K) > 19$ and $\neq 47, 191, 379$, we obtain a cover which is ramified of type $(2,2)$ at $T = 0, 1, -1, 2$ and of type $(2,1,1)$ at the four roots of $\mathrm{disc}^*(F_{21})$.

4.2.3 The Lagrange Resolvent

If we compare the results of Theorem 23 (and/or Theorem 24) with the motivating discussion of Subsection 4.2.1, then the natural question arises: Which of the two families

U_1 and U_2 corresponds to the curves with elliptic differentials, and which corresponds to the S_4-covers?

To decide this, we have to look at the monodromy group of covers in more detail. A convenient tool for this is the associated *Lagrange Resolvent*, as we shall see.

Definition. The *Lagrange resolvent* of a general quartic polynomial

$$f(x) = ax^4 + bx^3 + cx^2 + dx + e \tag{36}$$

is the monic cubic polynomial $r_f(x)$ which is defined by

$$r_f(x) = x^3 - cx^2 + (bd - 4ae)x + a(4ce - d^2) - b^2e.$$

Remark 28 If f is monic, then this definition of r_f agrees with the usual definition; cf. Hungerford[Hu], p. 272. In general, however, we have that $r_f(ax) = a^3 r_{\tilde{f}}(x)$, where $\tilde{f}(x) = f(x)/a$ is the associated monic polynomial (when $a \neq 0$).

We can use the Lagrange resolvent to detect primitivity because of the following basic fact.

Lemma 29 *Let x be a root of an irreducible quartic $f(X) \in k[X]$. Then $k(x)/k$ is primitive if and only if $r_f(X)$ is irreducible.*

Proof. This follows from [Hu], Proposition V.4.11 (p. 273) because in the list of groups given there, $k(x)/k$ is primitive if and only if $\mathrm{Gal}_f \simeq A_4$ or S_4, as is easy to see.

The following type of polynomials will play an important role in analyzing the curves represented by the points in U_1.

Lemma 30 *Let $f(X) \in k[X]$ be an irreducible quartic of the form*

$$f(X) \ = \ aX^4 + bX^3 + cX^2 + \alpha bX + \alpha^2 a. \tag{37}$$

(a) *We have that* $\mathrm{Gal}_f \simeq D_4$ *or* $\mathrm{Gal}_f \simeq \mathbb{Z}/4\mathbb{Z}$ *or* $\mathrm{Gal}_f \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*. Moreover, the latter case occurs if and only if the discriminant* $\mathrm{disc}(f)$ *of f is a square in k.*

(b) *If x is a root of $f(X)$, and if we put $y = (2ax^2 + bx + 2a\alpha)/x$, then $y^2 = b^2 - 4ac + 8a^2\alpha$, and so $k(y)$ is a quadratic subfield of $k(x)$.*

Proof. (a) It is easy to see that the Lagrange resolvent of $f(x)$ factors as

$$r_f(x) \ = \ (x - 2a\alpha)(x^2 + (2a\alpha - c)x + \alpha(b^2 - 2ac)).$$

Thus, $r_f(x)$ is reducible over k and so the first assertion follows from Proposition 4.11 of Hungerford[Hu], p. 273. Moreover, since

$$\mathrm{disc}(f) = \alpha^2(b^2 + 8a^2\alpha - 4ac)^2((2a\alpha + c)^2 - 4\alpha b^2),$$

we see that $\mathrm{disc}(f)$ is a square in k if and only if $(2a\alpha+c)^2 - 4\alpha b^2 = (2a\alpha - c)^2 - 4\alpha(b^2 - 2ac)$ is a square in k. Since the latter is the discriminant of $x^2 + (2a\alpha - c)x + \alpha(b^2 - 2ac)$, it follows that $\mathrm{disc}(f)$ is a square in k if and only if r_f splits in k. By Hungerford[Hu], Proposition 4.11, this is equivalent to the condition that $\mathrm{Gal}_f \simeq Z/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) The first assertion holds because

$$y^2 - (b^2 - 4ac + 8a^2\alpha) = 4a(ax^4 + bx^3 + cx^2 + \alpha bx + \alpha^2 a)/x^2 = 0.$$

Thus, $[k(y) : k] \leq 2$. On the other hand, since x is a root of the polynomial $2aX^2 + (b - y)X + 2a\alpha \in k(y)[X]$, we see that $[k(x) : k(y)] \leq 2$, and so $[k(x) : k(y)] = [k(y) : k] = 2$ because $[k(x) : k] = 4$.

4.2.4 Application to the Monodromy Group of Covers

Let the isomorphism class of (C, f_C, π_C) belong to $\tilde{\mathcal{H}}^*_{3,4,4}(K)$. We want to determine the monodromy group of the 4-cover $f_C : C \to \mathbb{P}^1_K$, which is the same as the Galois group of the associated polynomial $F(T, X)$ over $K(T)$.

Curves with Elliptic Differentials. Recall the definition of the open subscheme U_1 of $\tilde{H}^*_{3,4,4}$ given in Theorem 23: The curves representing elements in this set satisfy the equation (31), which has the form

$$F_1(T, X) = A(T)X^4 + B(T)X^3 + C(T)X^2 + \alpha B(T)X + \alpha^2 A(T).$$

We look at this polynomial over $K(T)$ and see that it satisfies the conditions of Lemma 30. Hence its resolvent is reducible and f_C factors through a quadratic subcover

$$g_2 : C \to E,$$

where E is given by the equation

$$Y^2 = B(T)^2 - 4A(T)C(T) + 8\alpha A(T)^2$$

with

$$\begin{aligned} A(T) &= r_{01}T + (1 - r_{01})T^2, \\ B(T) &= r_{11}T + r_{12}T^2, \\ C(T) &= r_{201} + r_{211}T + (\alpha^2 + 4\alpha + 1 - r_{201} - r_{211})T^2 \end{aligned}$$

where $\alpha = -\frac{1}{2}(r_{11} + r_{12} + 2)$ and r_{201} and r_{211} are defined in (30) and satisfy the relations described in Theorem 23. In particular, E is an elliptic curve.

Hence we get:

Theorem 31 *The members of the family U_1 in $\tilde{H}^*_{3,4,4}$ are attached to hyperelliptic curves C of genus 3 with an elliptic differential of degree 2.*

The elliptic curve covered by such curves C is given by the Weierstraß equation

$$Y^2 = B(T)^2 - 4A(T)C(T) + 8\alpha A(T)^2,$$

which is uniquely and explicitly determined by the parameters $r_{01}, r_{11}, r_{12}, t$.

Corollary 32 *The monodromy group Gal_{f_C} of f_C for (C, f_C, π_C) belonging to an isomorphism class in $\mathcal{U}_1(K)$ is either the dihedral group D_4 or the Klein 4-group $V \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Moreover, $\mathrm{Gal}_{f_C} \simeq D_4$ if and only if the discriminant $\mathrm{disc}(F_1)$ of its associated equation $F_1(T, X)$ is not a square in $K(T)$. Thus, the isomorphism classes of triples (C, f_C, π_C) that lie in $\mathcal{U}_1(K)$ with $\mathrm{Gal}_{f_C} \simeq D_4$ are K-rational points of an open non-empty subscheme of U_1 (the generic case).*

Proof. Since f_C is ramified of type $(2, 2)$ at some point, Gal_{f_C} contains a $(2, 2)$-cycle and hence cannot be cyclic. In view of this, the first and second assertions follow from Lemma 30(a). Since over $\overline{K}$ the condition of a being a square can be described by polynomial conditions (cf. Lemma 12), the last assertion follows.

Remark 33 It follows from Corollary 32 that the examples presented in Example 27(a) all have D_4 as their monodromy group. Indeed, it seems difficult to find examples in U_1 with monodromy group V.

The Primitive Case. We now come to the second family U_2 in $\tilde{H}^*_{3,4,4}$. Each curve $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ attached to elements in $\mathcal{U}_2(K)$ is given by an equation of the form

$$F_2(T,X) = F_1(T,X) + \frac{d}{q}G(T,X).$$

By the previous discussion we would expect that at least generically such curves should give primitive 4-covers $f_C : C \to \mathbb{P}^1_K$ with monodromy group S_4. The following result shows that this expectation is correct:

Theorem 34 *Take (C, f_C, π_C) such that its isomorphism class lies in $\mathcal{U}_2(K)$, and suppose that f_C has ramification type $(2,2)^4(2,1,1)^4$ or, equivalently, that the discriminant of its associated polynomial $F_2(T,X)$ has the form*

$$\operatorname{disc}(F_2) = T^2(X^2-1)^2(X-t)^2\operatorname{disc}^*(F_2),$$

and $\operatorname{disc}^*(F_2) \in K[T]$ is squarefree. If $r_{11} \neq r_{12}$, then f_C is a primitive cover and hence its monodromy group is S_4.

Proof. (Sketch) To show that f_C is primitive, it is enough to show that the Lagrange resolvent r_{F_2} is irreducible over $K(T)$; Lemma 29. Suppose the contrary, i.e., that

$$r_{F_2}(X) = (X-y)(X^2+aX+b)$$

for some $y, a, b \in K(T)$. Since $r_f(X) \in K[T,X]$, it follows from Gauss that $y, a, b \in K[T]$. Furthermore, a careful degree count shows that $\deg(y) \leq 2$; cf. [K2].

By specializing $f(X)$ modulo $T-1$, $T+1$ and $T-t$ and using (25), (26) and (34) and suitable properties of r_f, it follows that y satisfies the congruences

$$\begin{aligned} y &\equiv 2\alpha \,(\operatorname{mod} T-1) \\ y &\equiv 2a_0\alpha \,(\operatorname{mod} T+1) \\ y &\equiv 2a_5t\beta \,(\operatorname{mod} T-t), \end{aligned}$$

where $\beta = \alpha - \frac{da_1(t-1)}{2a_0q}$; cf. [K2] for the details. Since $\deg(y) \leq 2$, the Lagrange Interpolation Formula shows that

$$y = \alpha(T-t)\left(\frac{T+1}{1-t} + a_0\frac{T-1}{t+1}\right) + 2a_5t\beta\frac{T^2-1}{t^2-1}.$$

On the other hand, the fact (24) that $F_2(0,X) = r_{20}X^2$ implies that

$$r_{F_2}(X) \equiv X^3 - r_{20}X^2 \;(\operatorname{mod} T),$$

and from this one obtains that either $y \equiv 0 \,(\operatorname{mod} T)$ or that $y \equiv r_{20} \,(\operatorname{mod} T)$. Now if $y \equiv r_{20} \,(\operatorname{mod} T)$, then $b^2 - 4c \equiv 0 \,(\operatorname{mod} T)$, and this contradicts the fact that $\operatorname{disc}^*(F_2)$ is squarefree; cf. [K2]. We thus have that $y(0) = 0$. But from the above expression fro y we have (after simplification) that

$$y(0) = \frac{2ta_5}{t^2-1}(\alpha - \beta).$$

We thus have that $\alpha = \beta$, which is equivalent to $da_1 = 0$. Since $d \neq 0$ by the definition of U_2 and $a_1 \neq 0$ by hypothesis, it follows that no such y exists, and hence r_{F_2} is irreducible, as desired.

Thus, f_C is primitive and hence $\operatorname{Gal}_{f_C} \simeq S_4$ because Gal_{f_C} contains a transposition since we have points which are ramified of type $(2,1,1)$.

Notation. Let $U' \subset U$ denote the subfamily determined by the condition that the monodromy group of covers f_C attached to isomorphism classes of triples (C, f_C, π_C) corresponding to points in $U'(\overline{K})$ is equal to S_4 and that the ramification type is $(2,2)^4(2,1,1)^4$.

Corollary 35 *The family U' is open in U_2 and its K-rational elements coincide with the set of isomorphism classes of triples (C, f_C, π_C) satisfying the hypotheses of* Theorem 34. *Moreover, $U'(K)$ is non-empty provided that char$(K) > 5$.*

Proof. The fact that U' is a subscheme of U_2 follows from Corollary 32. Now if the class of (C, f_C, π_C) corresponds to a point in $U'(K)$, then by Proposition 36 below we see that C must satisfy the hypotheses of Theorem 34. Since triples attached to these curves clearly define an open subscheme of U_2, it follows that U' is open in U_2.

Since Example 27(b) satisfies the hypotheses of Theorem 34 whenever $\mathrm{char}(K) > 19$ and $\neq 47, 191, 379$, it follows that $U'(K) \neq \emptyset$ in these cases. By considering other curves (cf. [K2]) one concludes that $U'(K) \neq \emptyset$ whenever $\mathrm{char}(K) > 5$.

Note that we do have imprimitive covers in U_2, as the following simple criterion shows.

Proposition 36 *Let $C \in \mathcal{U}_2(K)$ be a curve defined by $F_2(T, X) = 0$ with parameters $(r_{01}, r_{11}, r_{12}, t)$. If $r_{11} = r_{12}$, or if $r_{11} = -tr_{12}$, then* $\mathrm{Gal}_{f_C} \simeq D_4$ *or V. Moreover, the latter case occurs if and only if* $\mathrm{disc}(F_2)$ *is a square in $K(T)$.*

Proof. The condition $r_{11} = r_{12}$ (respectively, $r_{11} = -tr_{12}$) means that $a_1 = 0$ (respectively, $a_6 = 0$), and so it follows that $c_3 = c_4 = 0$ in formula (32). Thus, $G(T, X) = C_1(T)X^2$, with $C_1(T) = c_2(1 - T^2) + a_6T(1 - T)$, and so $F_2(T, X)$ has the form of Lemma 30 (with $c = C(T) + \frac{d}{q}C_1(T)$). Thus, the result follows by the same argument as in the proof of Corollary 32.

4.2.5 The "Inverse" of the Donagi-Livné-Smith Construction

The basic strategy was already explained in Subsection 4.2.1:

Given a 4-cover $f : C \to \mathbb{P}^1_K$ with monodromy S_4 and ramification type $(2, 2)^4(2, 1, 1)^4$, we want to construct a hyperelliptic genus 3 curve C' with a degree 6 cover $f_6 : C' \to \mathbb{P}^1_K$ which factors over the hyperelliptic cover of C' in such a way that the Galois hull $\tilde{f} : \tilde{C} \to \mathbb{P}^1_K$ of f factors over f_6.

The following lemma makes this construction more explicit.

Lemma 37 *Let $f(X) \in k[X]$ be an irreducible quartic with* $\mathrm{Gal}_f \simeq S_4$, *and let L/k be a splitting field of f. Then the field L also splits the Lagrange resolvent $r_f(X)$. Let $x \in L$ be a root of f and $\xi \in L$ a root of r_f. Then:*

(a) $\mathrm{Gal}(L/k(\xi))$ *is a 2-Sylow subgroup of $G = \mathrm{Gal}_f$.*

(b) $[L : k(x, \xi)] = 2$.

(c) *There is an element $y \in k(x, \xi)$ such that $y^2 = \xi^2 - 4ae$, where a and e are the coefficients of f as in* (36), *and then $[k(\xi, y) : k(\xi)] = 2$.*

Proof. If $f(X) = a(X - x_1)(X - x_2)(X - x_3)(X - x_4)$ is the factorization of $f(X)$ in L, then

$$r_f(X) = (X - \xi_1)(X - \xi_2)(X - \xi_3),$$

where $\xi_1 = a(x_1x_2 + x_3x_4)$, $\xi_2 = a(x_1x_3 + x_2x_4)$ and $\xi_3 = a(x_1x_4 + x_2x_3)$; cf. [Hu], Lemma V.4.10 (together with Remark 28). Thus L also splits $r_f(X)$.

To prove the rest of the assertions, we may assume (after renumbering, if necessary) that $x = x_1$ and $\xi = \xi_1$. We identify an element $\sigma \in S_4$ with the elements of $\mathrm{Gal}(L/k)$ via the natural relation $\sigma(x_i) = x_{\sigma(i)}$.

(a) Since r_f is irreducible, we have $[k(\xi_i) : k] = 3$ and so $|\mathrm{Gal}(L/k(\xi_i))| = [L : k(\xi)] = \frac{24}{3} = 8$, which means that $\mathrm{Gal}(L/k(\xi))$ is a 2-Sylow subgroup of $\mathrm{Gal}(L/k)$.

(b) We have $\mathrm{Gal}(L/k(x_1)) = \langle(34), (234)\rangle =: H$ and $\mathrm{Gal}(L/k(\xi_1)) = \langle(34), (1324)\rangle =: P_2$. Thus, $\mathrm{Gal}(L/k(x_1, \xi_1)) = H \cap P_2 = \langle(34)\rangle$, and so $[L : k(x_1, \xi_1)] = |\langle(34)\rangle| = 2$.

(c) Let $y_1 = ax_1x_2$ and $y_2 = ax_3x_4$. Since $\mathrm{Gal}(L/k(x_1,\xi_1)) = \langle(34)\rangle$ by part (b), we see that $y_1, y_2 \in k(x_1,\xi_1)$. Clearly $y_1 + y_2 = \xi_1$ and $y_1y_2 = a^2x_1x_2x_3x_4 = ae$, so

$$(X - y_1)(X - y_2) = X^2 - \xi_1X + ae.$$

Put $y = y_1 - y_2$. By the quadratic formula we have that $y^2 = \xi_1^2 - 4ae \neq 0$. Since $(1324)y_1 = y_2$ and $(1324)y_2 = y_1$, we see that $(1324)y = -y$, and so $[k(\xi_1, y) : k(\xi_1)] = 2$, as desired.

By combining this lemma with what was said in Subsection 4.2.1, we obtain:

Proposition 38 *Let $F(T,X) \in K[T,X]$ be a polynomial with $\deg_X(F) = 4$ such that the associated quartic cover $f : C \to \mathbb{P}^1_K$ has monodromy group S_4 and ramification type $(2,2)^4(2,1,1)^4$. Then the Lagrange resolvent r_F defines a degree 3 cover $f_3 : C_0 \to \mathbb{P}^1_K$, and the curve $C_0 : r_F = 0$ has genus 0. Furthermore, if $(p(Z), q(Z))$ is a parametrization of C_0, and if $A(T)$ and $E(T)$ are the leading and constant terms of $F(T,X)$, respectively, then*

$$C' : \quad Y^2 = q(Z)^2 - 4A(p(Z))E(p(Z))$$

defines a hyperelliptic curve of genus 3, and the Galois hull $\tilde{f} : \tilde{C} \to \mathbb{P}^1_K$ of f factors over $f_3 \circ f_2$, where $f_2 : C' \to C_0 \simeq \mathbb{P}^1_K$ is the hyperelliptic subcover of C'.

We now show how this works in an example.

Example 39 Let $C = C_{21}$ be the curve defined by $F_{21}(T,X) = 0$, where F_{21} is as in Example 27(b). Thus, if $\mathrm{char}(K) > 19$ and $\neq 47, 191, 379$, then C is a smooth curve and $f_C : C \to \mathbb{P}^1_K$ is a cover of type $(2,2)^4(2,1,1)^4$. Since here $r_{11} = -1 \neq 2 = r_{12}$, we conclude from Theorem 34 that f_C has monodromy group S_4. We can thus apply the above proposition.

The Lagrange resolvent of F_{21} is

$$\begin{aligned} R(T,X) \;=\; & X^3 - (\tfrac{7}{3}T^2 + \tfrac{9}{4}T - \tfrac{22}{3})X^2 + (6T^4 - 4T^3 - \tfrac{25}{2}T^2)X \\ & +8T^6 - \tfrac{158}{3}T^5 + \tfrac{203}{3}T^4 + \tfrac{869}{12}T^3 - \tfrac{374}{3}T^2 \end{aligned}$$

By Proposition 38, $R(T,X) = 0$ defines a curve C_0 of genus 0, MAPLE finds the following parametrization of C_0:

$$T = -484p_1(Z)/q(Z), \quad \text{and} \quad X = p_2(Z)/q(Z)^2,$$

where

$$\begin{aligned} p_1(Z) &= 162Z^2 - 99Z - 20812 \\ p_2(Z) &= -\tfrac{11}{3}p_1(Z)(26244Z^4 + 416988Z^3 - 21434787Z^2 - 298325016Z + 186702032) \\ q(Z) &= 9(162Z^3 - 99Z^2 + 18392Z + 574992). \end{aligned}$$

Note that since $484 = (2)^2(11)^2$, $162 = (2)(3)^4$ and $26244 = (2)^3(3)^8$, the indicated top coefficients of the numerator and denominator of $T(Z)$ and $X(Z)$ are non-zero in K. Following the recipe of Proposition 38, put $h(Z) = X(Z)^2 - 4A(T(Z))E(T(Z))$. Here $A(T) = T$ and $E(T) = \frac{17}{4}T - 2T^2$, and by MAPLE we find that $h(Z) = h_1(Z)h_2(Z)^2$, where

$$\begin{aligned} h_1(Z) \;=\; & (162Z^2 - 99Z - 20812)(162Z^2 - 5643Z - 86636) \\ & \cdot(162Z^2 + 3861Z + 6292)(162Z^2 + 7029Z - 55660) \\ h_2(Z) \;=\; & \frac{11(162Z^2 - 99Z - 20812)}{243(162Z^3 - 99Z^2 + 18392Z + 574992)^2} \end{aligned}$$

It thus follows from Proposition 38 that $C' : Y^2 = h_1(Z)$ is the desired hyperelliptic curve of genus 3.

Note that since $\mathrm{disc}(h_1) = (2)^{152}(3)^{165}(5)(11)^{62}(13)(17)^3(19)(47)(191) \neq 0$, the roots of $h_1(Z)$ are distinct over $\overline{K}$, and so C' is indeed a curve of genus 3.

Remark 40 One might be tempted to use the curves C attached to elements in $U_2(\mathbb{F}_q)$ to avoid Smith's attack. In fact, let C' be the curve obtained from C by the inverse of the Donagi-Livné-Smith construction. If there is *only one* $\mathbb{F}_q$-rational possibility for a correspondence η for C' (with resulting curve C necessarily), then the Smith attack cannot be applied to C' over $\mathbb{F}_q$. Whether C' satisfies this condition can be decided by looking at the Galois structure of the Weierstraß points of C' (see [Sm]) and this structure can be rediscovered by the Galois structure of the ramification points of type $(2,2)$ of f_C. For instance a "good" case is that these points form one Galois orbit. (This should be the "generic" case).

But then necessarily $[C, f_C, \pi_C] \notin U_2(\mathbb{F}_q)$ and so over $\mathbb{F}_q$ we cannot use the simple equations defining this family to find C. (Recall that a random choice of C will be not in $U'(\mathbb{F}_q)$.)

Of course, one could try to go to extensions $\mathbb{F}_{q^d}$ ($d \leq 4$ will be enough), find $[C, f_C, \pi_C] \in U_2(\mathbb{F}_{q^d})$ with the extra condition that C is defined over $\mathbb{F}_q$ and then try Galois descent to find a 4-cover of C over $\mathbb{F}_q$. But it is very doubtful that this strategy will lead to a computationally effective algorithm.

The image of U in M_3^h. We now consider the map

$$\phi := (\mu_3)_{|U} : U = U_1 \cup U_2 \ \rightarrow\ M_3^h$$

which is defined by the rule $\phi([C, f_C, \pi_C]) =$ isomorphism class of C. On the component U_1 of U this map cannot be generically finite because all fibres are infinite. However, we do have the following result:

Proposition 41 *The restriction of ϕ to the subscheme U' is quasi-finite, and hence the restriction of μ_3 to U_2 is generically finite. Thus, the image of U_2 in M_3^h is a 4-dimensional variety.*

Proof. To verify this, let $H^h_{3,6}(S_4)$ denote the Hurwitz space which classifies 6-covers $f_6 : C' \to \mathbb{P}^1_K$ with the property that C' is a hyperelliptic curve, f_6 factors over the hyperelliptic involution and that f_6 has monodromy group S_4 (with a special ramification structure as was explained in [FK], Theorem 3). Then the construction of Proposition 38 induces a (set) map from $U'(\overline{K})$ to $H^h_{3,6}(S_4)(\overline{K})$ with finite fibres.

Moreover, the existence of a correspondence between C and C' which induces a (polarized) isogeny of degree 8 between the Jacobians J_C and $J_{C'}$ implies (by Torelli) that the isomorphism class of C produces only finitely many isomorphism classes of curves C'.

Now since the forget map $H_{3,6}(S_4) \to M_3^h$ is quasi-finite (because for a given C' there are, up to equivalence, only finitely many trigonal maps $f_3 : \mathbb{P}^1_K \to \mathbb{P}^1_K$ such that $f_6 = f_3 \circ \pi_{C'}$ satisfies the required ramification conditions), it follows that the forget map $\phi : U' \to M_3^h$ is also quasi-finite.

Corollary 42 *The restriction of $\overline{\mu}_3$ to V_2 is generically finite.*

Finally, we are ready to present at least a sketch of the proof of the main result announced in Subsection 1.2.1.

Proof of Theorem 2 (sketch). We have that $\overline{H}_{3,4,4}(S_4) \subset \overline{H}_{3,4,4} = V_1 \cup V_2$, the latter by Theorem 20. By a similar argument as that of the proof of Theorem 31 we see that $\overline{H}_{3,4,4}(S_4) \subset V_2$; cf. [K2].

Next, by Theorem 34 and Corollary 35 we see that $\overline{H}_{3,4,4}(S_4)$ contains the non-empty open subscheme $\pi_3(U')$ when $\mathrm{char}(K) > 5$. Moreover, by an extension of the argument of Theorem 34 it follows that $\overline{H}_{3,4,4}(S_4)$ is open in V_2 (cf. [K2]), and so it follows from Theorem 20 that $\overline{H}_{3,4,4}(S_4)$ is an irreducible, unirational variety of Dimension 4.

The assertions about $\overline{\mu}_3$ follow by a similar argument as that of the proof of Proposition 41.

Acknowledgment. We would like to thank the referees for their extremely careful reading of the paper, for their numerous useful comments which greatly improved the exposition of this paper, and for providing a long list of typos, some of which required considerable ingenuity and insight to find.

References

[CF] H.Cohen, G. Frey, (eds.), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC, 2005.

[CM] M. Coppens, G. Martens, *Linear Series on 4–Gonal Curves*, Math. Nachr. **213** (2000), 35–55.

[D] C. Diem, *On the discrete logarithm problem for plane curves*, J. Th. des Nombres de Bordeaux **24** (2012), 639–667.

[DGTT] C. Diem, P. Gaudry, E. Thom, N. Thériault, *A double large prime variation for small genus hyperelliptic index calculus* , Math. Comp. **76** (2007), 475–492.

[FK] G. Frey, E. Kani, *Correspondences on hyperelliptic curves and applications to the discrete logarithm*, in: Security and Intelligent Information Systems (International Joint Conference, Warsaw, 2011), *Lecture Notes in Computer Science* **7053** (2012), pp. 1–19.

[GL] S. R. Ghorpade and G. Lachaud, *Etale cohomology, Lefschetz theorems and number of points on singular varieties over finite fields*, Mosc. Math. J. **2** (2002), 589–631.

[GS] J. Gutierrez, T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. of Comp. Math. **8** (2005), 102–115.

[Ha] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[HR] M. Hindry, Ch. Ritzenthaler, e-mail to the authors, 28.06.2014.

[Hu] T. Hungerford, *Algebra*, Springer, New York, 1974.

[K1] E. Kani, *Castelnuovo's equivalence defect*, J. reine angew. Math. **352** (1984), 24-70.

[K2] E. Kani, *Hurwitz spaces for hyperelliptic curves of genus 3*, Preprint, 2014.

[LR] R. Lercier, Ch. Ritzenthaler, *Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects*, J. Algebra **372** (2012), 595–636.

[Mu] D. Mumford, *Geometric Invariant Theory,* Springer-Verlag, Berlin, 1966.

[Sm] B. Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 2 hyperelliptic curves*, in: EUROCRYPT 2008, *Lecture Notes in Computer Science* **4965** (2008), pp. 163-180; revised version in: *J. Cryptology* **22** (2009), 505–529.

[St] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd edition. Springer-Verlag, Berlin, 2008.