Ordinary plane models and completely split divisors

Claus Diem and Sebastian Kochinke

March 21, 2019

Abstract

Let $\mathcal{C}$ be a smooth, non-hyperelliptic curve over an algebraically closed field of genus $g \geq 4$. We show that the projection from the canonical model of $\mathcal{C}$ through $(g-3)$ generic points on $\mathcal{C}$ is a birational morphism to a plane curve which has only finitely many non-ordinary tangents, that is, flex- or bitangents. For smooth, non-hyperelliptic curves of a fixed genus $g \geq 4$ over finite fields, we show that the probability that an effective divisor of degree $(g-3)$ defines such an "ordinary (birational) plane model" converges to 1.

This result has an application to the solution of the discrete logarithm problem for smooth, non-hyperelliptic curves curves of a fixed genus g over finite fields $\mathbb{F}_q$: By first changing the representation to such an ordinary plane model and then using an algorithm by the first author, the problem can be solved in an expected time of $\tilde{O}(q^{2-\frac{2}{g-1}})$.

Another consequence is that for smooth, non-hyperelliptic curves of a fixed genus g over finite fields $\mathbb{F}_q$, the number of completely split divisors in the canonical system is $\sim \frac{1}{(2g+2)!} \cdot q^{q-1}$.

1 Introduction

Let us consider the discrete logarithm problem in the degree-0 Picard groups of smooth curves of a fixed genus g. In [Die11] it is shown that this problem can be solved in an expected time of

$$\tilde{O}\big(q^{2-\frac{2}{g}}\big)\,;$$

here and in the following the phrase "expected time" refers to an internal randomization of the algorithm. In [Die12a] it is shown that this can be improved if $\mathcal{C}$ is represented in an appropriate way by what we call a *(birational) plane model*; this is a possibly singular plane curve which is birational to the curve in question. The basic idea of the algorithm in [Die12a] (and the previous algorithm in [Die06]) is to generate relations by intersecting the plane model with lines.

More specifically, consider the discrete logarithm problem for smooth curves $\mathcal{C}$ of genus g over finite fields $\mathbb{F}_q$ given by plane models of a fixed

degree $d \geq 4$. This means that the input consists of: First a plane curve $\mathcal{C}_{pm}$ of degree d over a finite field, say $\mathbb{F}_q$. To this curve the normalization $\mathcal{C}_{pm}$, which consists of a smooth curve $\mathcal{C}$ over $\mathbb{F}_q$ together with a birational morphism $\pi : \mathcal{C} \to \mathcal{C}_{pm}$, can be associated. A second part of the input is then an instance of the discrete logarithm problem in $\mathrm{Pic}^0(\mathcal{C})$.

Just as in [Die11] and in other algorithms for the discrete logarithm problem for curves of small genus, the factor base is a subset of the set of $\mathbb{F}_q$-rational points of $\mathcal{C}$. Then the linear system

$$\mathfrak{g}_d^2(\pi) := \{\pi^*((W)_0) \mid W \in \mathbb{F}_q[X, Y, Z]_1\}$$

that is given by the pullback of lines in $\mathbf{P}^2_{\mathbb{F}_q}$ is considered. Relations are generated by considering effective divisors containing two points of the factor base. As here the divisors on which conditions are imposed have degree $d-2$ instead of degree g in the algorithm for the result in [Die11], a first heuristic analysis suggests that one can obtain an expected running time of

$$\tilde{O}(q^{2-\frac{2}{d-2}})$$

in this way.

It is show in [Die11] that in this is indeed the case for two kind of curves given by plane models: First for non-hyperelliptic curves of genus 3 and second provided that there is of *at least one divisor in* $\mathfrak{g}_d^2(\pi)$ *that is completely and distinctly split*, by which we mean that it splits completely into distinct $\mathbb{F}_q$-rational points. A possibility to fulfill the latter condition is via a nonsingular point p of the plane model through which only ordinary tangents, that is, tangents which are neither bitangents nor flex tangents, run. Indeed, in this case, the number of completely and distinctly split divisors that contain p is $\sim \frac{1}{(d-1)!} \cdot q$ (see Proposition 14).

We call a plane curve with only finitely many nonsingular points with non-ordinary tangents an *ordinary* plane curve. Note here that if the characteristic is not 2 a plane curve is ordinary if and only if it is reflexive, however in characteristic 2 there are no reflexive plane curves.

For smooth, non-hyperelliptic curves of a fixed genus $g \geq 4$, an idea to improve upon [Die06] is then to generate ordinary plane models of degree $(g+1)$ by projection through the hyperplane generated by the image of a divisor D of degree $(g-3)$. The corresponding linear system is then the residual system of D, that is, $|K - D|$. Here and in the following, K denotes a canonical divisor on the curve in question. We only consider base point free systems, which means that the plane model indeed has degree $(g+1)$. Let us note here that if we vary D, we obtain in this way all base point free complete $\mathfrak{g}^2_{g+1}$'s.

It remains now to show that one can indeed efficiently find in this way an appropriate plane model. As pointed out by Griffiths & Harris in the introduction to their work on Brill-Noether theory on special linear systems

in characteristic 0 ([GH80]), it follows from the theory that a general effective divisor D of degree $(g-3)$ on a *general* non-singular (non-hyperelliptic) curve of genus $g \geq 3$ leads to a plane model of degree $(g+1)$ via $|K-D|$. Since the relevant statements of Brill-Noether theory are valid in any characteristic by Gieseker's work [Gie82], so is this statement.

We show that the obvious generalization of this result to arbitrary non-singular, non-hyperelliptic curves over algebraically closed fields holds and the resulting plane model is ordinary:

Theorem 1. *Let $\mathcal{C}$ be a non-singular, non-hyperelliptic curve over an algebraically closed field of genus $g \geq 4$. Then the residual system of a general effective divisor of degree $(g-3)$ on $\mathcal{C}$ defines an ordinary plane model of $\mathcal{C}$, which then has degree $(g+1)$.*

For linear systems over curves over finite fields, we cannot even formulate this result, but we can ask if a probabilistic variant holds. We show that this is indeed the case for curves of a fixed genus:

Theorem 2. *Let a natural number $g \geq 4$ be fixed. Then there exists a constant $C > 0$ such that for every smooth, non-hyperelliptic curve $\mathcal{C}/\mathbb{F}_q$ of genus g the following holds. Let $\mathcal{P}_\mathcal{C}$ be the probability that a divisor D chosen uniformly at random from the effective divisors of degree $(g-3)$ does not lead to an ordinary plane model of degree $(g+1)$ via $|K-D|$. Then*

$$\mathcal{P}_\mathcal{C} \leq \frac{C}{q}\,.$$

Again for smooth, non-hyperelliptic curves of a fixed genus, it is then not difficult to efficiently construct appropriate plane models and to transfer instances of the discrete logarithm problem in an efficient way. With Theorems 1 and 2 of [Die12a] we then obtain:

Theorem 3. *Let a natural number $g \geq 3$ be fixed. Then the discrete logarithm problem for non-hyperelliptic curves of genus g over finite fields $\mathbb{F}_q$ can be solved in an expected time of*

$$\tilde{O}\big(q^{2-\frac{2}{g-1}}\big)\,.$$

With the close connection between ordinary plane models coming from some $|K-D|$ with an effective divisor D of degree $(g-3)$ and the canonical linear system itself we also show:

Theorem 4. *Consider smooth, non-hyperelliptic curves of a fixed genus g over finite fields $\mathbb{F}_q$. Then the number of completely and distinctly split divisors in the canonical system of such a curve is in*

$$\frac{1}{(2g-2)!}\cdot q^{g-1} + O\big(q^{g-\frac{3}{2}}\big).$$

Outline

To obtain our probabilistic results over finite fields, we need estimates of the cardinalities of sets of $\mathbb{F}_q$-rational points of schemes and varieties. In Section 2 we introduce two key ingredients for such an approach: In the first subsection, we give upper and lower bounds on the number of rational points in schemes and varieties over finite fields and derive from these bounds on the number of rational points of fibers of relative schemes. We then recall that there is a fine moduli space parameterizing curves of fixed genus with a three-canonical embedding and analyze certain properties of this space. This enables us to parameterize various schemes linked to curves of fixed genus and to apply the results on the bounds.

Subsection 2.1 contains some results which are not necessary for the derivation of Theorem 2 and which we regard to be of independent interest. These results are also preparatory for our forthcoming work [DK], but also then we will not need the results in full generality.

In Section 3 we then prove the four theorems given. To prove Theorem 1 and Theorem 2, we closely study hyperplane divisors and tangents of canonical models of curves. We give motivations and some definitions in the first subsection and prove the theorems in the second. In order to prove Theorem 2 we formulate the properties for relative curves in such a way that we can successfully apply the techniques of Section 2.

We then show the number of completely and distinctly split divisors in the canonical linear system of $\mathcal{C}$ is as claimed in Theorem 4. Briefly, is due to the fact that line sections on a plane model as considered by us correspond to certain hyperplane sections on the canonical model.

Finally, we discuss how one can efficiently construct ordinary plane models and birational morphisms to them both from a theoretic as well as from a practical point of view and we prove Theorem 3.

Notation and Terminology

Most of the terminology in this work agrees with the generally accepted one in [Har77] complemented by [ACGH85] and [ACG11].

Let Y be an S-scheme. If $h : T \to Y$ is a morphism of S-schemes we call h a *T-valued point* of Y and denote the set of all T-valued points on Y by $Y(T)$. In the case $T = \mathrm{Spec}(\mathbb{F})$ for some field $\mathbb{F}$ we denote $Y(\mathrm{Spec}(\mathbb{F}))$ by $Y(\mathbb{F})$. Generally, $\mathbb{F}$ will always denote an arbitrary field and k an algebraically closed field.

A *variety* over some field $\mathbb{F}$ is a geometrically integral and separated scheme of finite type over $\mathbb{F}$. A *curve* over $\mathbb{F}$ is a one-dimensional variety that is proper over $\mathbb{F}$. In particular, a curve does not have to be smooth. If a smooth curve $\mathcal{C}$ is under consideration, K always denote a canonical

divisor on $\mathcal{C}$. If T is an S-scheme we denote the (scheme theoretic) fiber on T over $s \in S$ by T_s.

Let S be a scheme. If we want to emphasize the relative point of view or wish to introduce the base S, we denote an S-scheme T by T/S, otherwise we just write T. A *smooth relative curve over* S is an S-scheme $\mathcal{C}$ that is proper and smooth over S and whose fibers are curves of a fixed genus, which is then called the genus of the relative curve.

Let $\mathcal{C}$ be a smooth curve over a field $\mathbb{F}$. Following [Die12a], we say that a divisor D on $\mathcal{C}$ is *completely split* if it splits into $\mathbb{F}$-rational points. Furthermore, we say that it is *distinctly split* if it splits into distinct (closed) points. Thus, as already stated above, D is completely and distinctly split if and only if it splits into distinct $\mathbb{F}$-rational points.

For a natural number d, the effective divisors of degree d on the smooth curve $\mathcal{C}$ over $\mathbb{F}$ are in natural bijection with the $\mathbb{F}$-rational points of $\mathcal{C}_d$, the d-fold symmetric product of $\mathcal{C}$. We identify the two, and in particular, to say that D shall be an effective divisor of degree d on $\mathcal{C}$, we also write $D \in \mathcal{C}_d(\mathbb{F})$.

For asymptotic statements, for a function f on a countable set $\mathbb{X}$ with values in $\mathbb{R}_{\geq 0}$, we make use of the usual sets $O(f)$ and $\tilde{O}(f) = \bigcup_{a \geq 0} O(\max(\log^a(f), 1) \cdot f)$. As for example in [Die12a], our use of language reflects that $O(f)$ and $\tilde{O}(f)$ are in fact sets. As already mentioned, by the phrase "expected time" we always refer to an internal randomization of the corresponding algorithm and no input data.

Acknowledgement

The authors would like to thank the Deutsche Forschungsgemeinschaft, the State of Saxony and the University of Leipzig for their support. We would like to thank the referee for carefully reading the manuscript and for many suggestions.

2 Preliminaries

2.1 Bounds on the Cardinality of Varieties

For a property P on the points of a variety X over an algebraically closed field k, the statement "the k-rational points of an open subscheme of X fulfill P" might intuitively be expressed by saying that "almost all k-rational points of X fulfill P".

By contrast, if X is a variety over a finite field $\mathbb{F}$, from "the $\mathbb{F}$-rational points of an open subscheme of X fulfill P" one cannot conclude anything about the portion of points which fulfill P. By the following results established by Lang & Weil in [LW54], there is however a suitable probabilistic replacement of the result if one considers not just points with values of $\mathbb{F}$ but also in extensions of this field:

Proposition 1. *Let n, d be natural numbers.*

a) There exists a constant $C = C(n,d)$ such that for any closed subscheme A, pure of some dimension r and of degree d, of $\mathbf{P}^n_{\mathbb{F}_q}$, $\#A(\mathbb{F}_q) \leq C\ q^r$.

b) There exists a constant $C = C(n,d)$ such that for any closed subvariety V of some dimension r and degree d of $\mathbf{P}^n_{\mathbb{F}_q}$,

$$|\#V(\mathbb{F}_q) - q^r| \leq (d-1)(d-2)\ q^{r-\frac{1}{2}} + C\ q^{r-1}\ .$$

Here, the statement in a) is Lemma 1 and the statement in b) is Theorem 1 of [LW54]. This result was later reproven and improved with the use of étale cohomology. With these methods, it was shown in [GL02] that a) one in fact has $\#A(\mathbb{F}_q) \leq d \cdot \#\mathbf{P}^r(\mathbb{F}_q)$. Also, an explicit bound in b) is given.

We want to use these results to obtain a probabilistic result for families of schemes and closed subschemes in the spirit explained above. As a first step, we want to obtain bounds for subschemes of affine spaces in terms of the "complexity" of a defining system of equations. To make this precise, we use the following definitions which were essentially given by T. Tau in his blog (see e.g. the discussion for Theorem 4.4.17 in [Tao13]).

Definition 2. Let $\mathbb{F}$ be any field. and $M > 0$.

a) We say a closed subscheme $V \subseteq \mathbf{A}^n_{\mathbb{F}}$ is of *complexity at most M* if there are polynomials $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ of maximal degree d such that $V = V(f_1, \ldots, f_m)$ and $n, m, d \leq M$.

b) Likewise we say that a closed subscheme $V \subseteq \mathbf{P}^n_{\mathbb{F}}$ is *complexity at most M* if there are homogeneous polynomials $F_1, \ldots, F_m \in \mathbb{F}[x_1, \ldots, x_n]$ of maximal degree d such that $V = V(F_1, \ldots, F_m)$ and $n, m, d \leq M$.

Note here that the surrounding space (the affine or projective space) is part of the definition. With the following lemma, we relate this definition to the results by Lang & Weil:

Lemma 3.

a) Let X be a closed subscheme of $\mathbf{P}^n_{\mathbb{F}}$ of complexity at most M and let for $i = 0, \ldots, n$ X_i be the union of irreducibility components of X of dimension i. (One might call $X = \bigcup_i X_i$ the dimension decomposition *of X.) Then $\sum_i \deg(X_i) \leq M^M$.*

b) Let X be a closed subscheme of $\mathbf{A}^n_{\mathbb{F}}$ of complexity at most M, let $\overline{X}$ be the closure of X in $\mathbf{P}^n_{\mathbb{F}}$. Then for $i = 0, \ldots, n$, the union of irreducibility components of $\overline{X}$ of dimension i is equal to the closure of X_i in $\mathbf{P}^n_{\mathbb{F}}$; let this be $\overline{X}_i$. Then $\sum_i \deg(\overline{X}_i) \leq M^M$.

Proof. a) We have the following more concrete statement: Let $X = V(F_1, \ldots, F_m)$ with $\deg(F_i) \leq d$. Then $\deg(X_i) \leq d^{n-i}$. This can be deduced easily from Krull's Hauptidealsatz and the so-called normalization axiom of intersection theory; this is Axiom A7 in [Har77, Appendix A]. Briefly, if V is an irreducible closed subscheme of $\mathbf{P}^n_{\mathbb{F}}$ and $F \in \mathbb{F}[X_0, \ldots, X_n]$ homogeneous then either $V \subseteq V(f)$ and thus $V \cap V(f) = V$ or alternatively $\dim(V \cap V(f)) = \dim(V) - 1$ and $\deg(V \cap V(f)) = \deg(V) \cdot \deg(F)$.

b) The closure $\overline{X}$ is equal to the union of the closures of the irreducibility components of X. This gives the first statement. Let now $X = V(f_1, \ldots, f_m)$ and let $\tilde{X}$ be the scheme obtained by homogenizing the polynomials f_i. Then $\overline{X} \subseteq \tilde{X}$. Also, every irreducibility component of $\overline{X}$ is an irreducibility component of $\tilde{X}$, thus $\overline{X}_i \subseteq \tilde{X}_i$. We can now apply the result in a) to get the desired statement on $\overline{X}$. □

Putting this together, we obtain:

Proposition 4. *For $M > 0$ there exists a $C = C(M) > 0$ such that for any V be a closed subscheme of $\mathbf{A}^n_{\mathbb{F}_q}$ or of $\mathbf{P}^n_{\mathbb{F}_q}$ of complexity at most M,*

a) $\#V(\mathbb{F}_q) \leq C \cdot q^{\deg(V)}$,

b) If V is a variety then $|\#V(\mathbb{F}_q) - q^{\dim(V)}| \leq C \cdot q^{\dim(V)-\frac{1}{2}}$.

This proposition was also proven by Tao in an entry called "The Lang-Weil bound" in his blog. In contrast to the proof here, Tao refers to a result which he has proven by model theoretic means, namely the already cited Theorem 4.4.17 in [Tao13].

We are now able to prove the following.

Proposition 5. *Let X be a scheme of finite type over a noetherian scheme S. Then there is a constant $C > 0$ such that*

a) for any finite field $\mathbb{F}_q$ and $s \in S(\mathbb{F}_q)$, $|X_s(\mathbb{F}_q)| \leq C \cdot q^{\dim(X_s)}$,

b) for any finite field $\mathbb{F}_q$ and $s \in S(\mathbb{F}_q)$ such that X_s is a variety, $|X_s(\mathbb{F}_q) - q^{\dim(X_s)}| \leq C \cdot q^{\dim(X_s)-\frac{1}{2}}$.

Proof. Since X is of finite type over S, we can immediately reduce to S being affine, say $S = \mathrm{Spec}(Z)$, and X is a finite union of affine Z-schemes given by finitely generated Z-algebras, say $X = U_1 \cup \cdots \cup U_k$ with $U_i = \mathrm{Spec}(R_i)$.

We prove a). Clearly, for $s \in S(\mathbb{F}_q)$, $\#X_s(\mathbb{F}_q) \leq \sum_i \#(U_i)_s(\mathbb{F}_q)$. We can thus reduce to $X = \mathrm{Spec}(R)$ with a finitely generated Z-algebra R over the noetherian ring Z. We can present R as $R = Z[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. Speaking geometrically, we have

$$X = V(f_1, \ldots, f_m) \subseteq \mathbf{A}^n_Z \,.$$

A point $s \in S(\mathbb{F}_q)$ corresponds to a homomorphism $\varphi : Z \to \mathbb{F}_q$, and then

$$X_s = V(\varphi(f_1), \ldots, \varphi(f_m)) \subseteq \mathbf{A}^n_{\mathbb{F}_q} .$$

The claim then follows with Proposition 4 a).

We come to b). If X is affine, we obtain the result just like a) with Proposition 4 b).

In general, we again use a decomposition $X = U_1 \cup \cdots \cup U_k$ with $U_i = \mathrm{Spec}(R_i)$. For each i, we let $A_i := X - U_i$. The result in a) now holds for each A_i and the result in b) holds for each U_i.

Let now $s \in S(\mathbb{F}_q)$ such that X_s is a variety. Then there is a U_i for which $(U_i)_s$ is dense in X_s and which is therefore a variety of the same dimension. Then $(A_i)_s$ is a proper subscheme of X_s and in particular of lower dimension. By the results a) for U_i and b) for A_i, the statement follows. □

This gives immediately the following corollary:

Corollary 6. *Let X be a scheme of finite type over a noetherian scheme S and let A be a constructible subset of X. Then there exists a constant $C > 0$ such that for any finite field $\mathbb{F}_q$ and any $s \in S(\mathbb{F}_q)$ for X_s is a variety and A_s does not contain the generic point of X_s we have*

$$\frac{\#A_s(\mathbb{F}_q)}{\#X_s(\mathbb{F}_q)} \leq \frac{C}{q}.$$

Indeed, a constructible subset is a finite union of locally closed subsets. Each of these can be given a scheme structure; let us call the resulting schemes A_i. The result then follows by applying the previous proposition to X and the A_i.

2.2 Moduli of Curves

In this and the forthcoming article [DK] we want to apply the results of the previous section to obtain probabilistic results on smooth curves of a fixed genus and divisors on such curves. For this, we need a smooth relative curve $\mathcal{C}/S$, such that every curve over every finite field $\mathbb{F}_q$ is isomorphic to a fiber $\mathcal{C}_s$ for some $s \in \mathbb{F}_q$.

The usual moduli space $\mathcal{M}_g$ is not suitable for this, but the so-called *universal tri-canonically embedded curve* used by Delingne & Mumford in their work [DM69] on moduli spaces is. Let us recall this:

Let $\mathcal{C}/S$ be a smooth relative curve of genus g with structure morphism $p : \mathcal{C} \to S$. Recall that by [DM69, Section 1], the relative ν-canonical sheaf $\Omega^{\otimes\nu}_{\mathcal{C}/S}$ is relatively very ample if $\nu \geq 3$. By [Gro67, II,Proposition 4.4.4] there is therefore a canonical immersion $\mathcal{C} \hookrightarrow \mathbf{P}(p_*(\omega^{\otimes\nu}_{\mathcal{C}/S}))$. As explained in [ACG11, Section XXI, §3], the sheaf $p_*(\omega^{\otimes\nu}_{\mathcal{C}/S})$ is locally free. Its degree is $(2\nu - 1)(g - 1)$, thus $\mathbf{P}(p_*(\omega^{\otimes\nu}_{\mathcal{C}/S}))$ is a locally trivial $\mathbf{P}^{(2\nu-1)(g-1)-1}$-bundle.

It is then natural to consider what might be called *coordinate systems* on $\mathbf{P}(p_*(\omega_{\mathcal{C}/S}^{\otimes\nu}))$: isomorphisms $\mathbf{P}(p_*(\omega_{\mathcal{C}/S}^{\otimes\nu})) \tilde{\to} \mathbf{P}_S^{(2\nu-1)(g-1)-1}$. With these one can then consider what is called *ν-canonically embedded curves*: tuples $(\mathcal{C}/S, \phi)$, where $\mathcal{C}/S$ is a smooth relative curve of genus g and ϕ is an isomorphism $\mathbf{P}(p_*(\omega_{\mathcal{C}/S}^{\otimes\nu})) \tilde{\to} \mathbf{P}_S^{(2\nu-1)(g-1)-1}$.

A key result for the construction of moduli spaces of curves is that for curves of a fixed genus g and for fixed ν the functor assigning to S the set of isomorphism classes of ν-canonically embedded curves is representable by a subscheme of a suitable Hilbert scheme. This was first stated in [DM69], a corresponding statement with proof is [MFK94, 5, §2].

Just as in [DM69] we apply this for $\nu = 3$. Let us fix this notation:

Notation 7. We denote the universal 3-canonically embedded curve of genus g by $\mathcal{Z}_g/\mathcal{H}_g$.

And furthermore:

Remark and Definition 8. Let $\mathcal{C}/S$ be any smooth relative curve. Then there is a unique closed subscheme whose geometric points are exactly those geometric points of S whose fibers are hyperelliptic. We denote this scheme by S^h and the complement of S^h by S^{nh}. The (geometric) points of S^{nh} are thus exactly those (geometric) points of S whose fibers are non-hyperelliptic.

In this work, we only need that every smooth curve of genus g over every finite field, say $\mathbb{F}_q$, can be obtained via an $\mathbb{F}_q$-rational point of $\mathcal{H}_g$. In addition to this, we have the following nice statement of which we will make use in our subsequent paper [DK].

Lemma 9. *Let q be a prime power. Then a uniformly chosen point in $\mathcal{H}_g(\mathbb{F}_q)$ leads to a uniformly chosen isomorphism classes of smooth curves over $\mathbb{F}_q$. Similarly, a uniformly chosen point in $\mathcal{H}_g^h(\mathbb{F}_q)$ leads to a uniformly chosen isomorphism classes of smooth hyperelliptic curves over $\mathbb{F}_q$ and a uniformly chosen point in $\mathcal{H}_g^{nh}(\mathbb{F}_q)$ leads to a uniformly chosen isomorphism classes of smooth, non-hyperelliptic curves over $\mathbb{F}_q$.*

Indeed, let $\mathcal{C}$ be a curve over $\mathbb{F}_q$ with structure morphism $p : \mathcal{C} \to \mathrm{Spec}(\mathbb{F}_q)$. Then $\mathbf{P}(p_*(\omega_{\mathcal{C}}^{\otimes 3})) = \mathbf{P}(\Gamma(\mathcal{C}, \omega_{\mathcal{C}}^{\otimes 3}))$ is a $(5g-6)$-dimensional projective space. There are $\#\,\mathrm{PGL}_{5g-6}(\mathbb{F}_q)$ coordinate systems on this projective space, thus the isomorphism class of $\mathcal{C}$ is given by $\#\,\mathrm{PGL}_{5g-6}(\mathbb{F}_q)$ $\mathbb{F}_q$-valued points of $\mathcal{H}_g$, a number which only depends on q.

The latter two statements then follow immediately.

3 Ordinary Plane Models

In this section, we first give some definitions and preliminary results, particularly on what we call ordinary plane curves. Then we prove Theorems 1

and 2. After this, we prove Theorem 4. In the last subsection, we give an algorithm to compute ordinary plane models given by complete $\mathfrak{g}^2_{g+1}$'s, starting from an arbitrary plane model, and to transfer divisors accordingly. With this, we prove Theorem 3.

3.1 Motivation and definitions

Let us now fix some interrelated definitions. We start with the definition of a tangent of a point on a smooth curve with respect to a birational morphism to a plane model which was already used in [Die12a] (for more information see [Die12a, Section 2]):

Remark and Definition 10. Let $\mathcal{C}$ be a nonsingular curve over an algebraically closed field k and let $\pi : \mathcal{C} \to \mathcal{C}_{pm}$ be a birational morphism to a plane model of $\mathcal{C}$. Now for a point $P \in \mathcal{C}(k)$ there is exactly one line $T \subset \mathbf{P}^2_k$ such that the multiplicity of the divisor $\pi^{-1}(T)$ at P is larger than the multiplicity of the divisor $\pi^{-1}(\pi(P))$ at P. We call this line the *plane tangent* at P (with respect to π).

A plane tangent T at P is called a *plane bitangent* at P if $\pi^{-1}(T) = 2P + 2P_1 + D$ for some $P_1 \in \mathcal{C}(k)$ and some effective divisor D on $\mathcal{C}$. It is called a *plane flex tangent* at P if $\pi^{-1}(T) = 3P + D$ for some effective divisor D on $\mathcal{C}$. A plane tangent T at P is called *ordinary* if it is neither a plane bitangent nor a plane flex tangent.

We now introduce two new related notions:

Definition 11. A plane curve $\mathcal{C}_{pm}$ over a field $\mathbb{F}$ is called *ordinary* if $(\mathcal{C}_{pm})_{\overline{\mathbb{F}}} := \mathcal{C}_{pm} \times \mathrm{Spec}(\overline{\mathbb{F}})$ only has only finitely many non-ordinary tangents. Likewise, if $\pi : \mathcal{C} \to \mathcal{C}_{pm}$ be a birational morphism from a smooth curve to a plane model of it, then π is called *ordinary* if $\mathcal{C}_{pm}$ is.

Definition 12. Let again $\mathcal{C}$ be a smooth curve over a field $\mathbb{F}$ and let $f : \mathcal{C} \to \mathbf{P}^1_{\mathbb{F}}$ be a non-constant function of degree n. Then f is called *ordinary* if f has only finitely many branch points (equivalently: if the corresponding extension of function fields $\mathbb{F}(\mathcal{C})|\mathbb{F}(\mathbf{P}^1)$ is separable) and if the preimage of every branch point of $f : \mathcal{C}_{\overline{\mathbb{F}}} \to \mathbf{P}^1_{\overline{\mathbb{F}}}$ is of the form $2P_1 + P_2 + \cdots + P_{n-1}$ for distinct points P_i.

Let us make some remarks about these definitions:

Remarks.

a) In Definition 11 we used the "elementary" definition of tangent of a plane curve. We could also first define that $\pi : \mathcal{C} \to \mathcal{C}_{pm}$ as in the definition is ordinary if $\mathcal{C}$ has only finitely many non-ordinary tangents with respect to π and then define a plane curve $\mathcal{C}_{pm}$ to be ordinary if the canonical morphism from the normalization of $\mathcal{C}_{pm}$ to $\mathcal{C}_{pm}$ is.

b) If in the context of Definition 11 the characteristic is $\neq 2$ then $\mathcal{C}_{pm}$ is ordinary if and only if it is reflexive.

c) If in the context of Definition 12 the characteristic is $\neq 2$ then the function is ordinary if and only if it is simple as defined for example in [Ful69].

d) In the context of Definition 11, $\pi : \mathcal{C} \to \mathcal{C}_{pm}$ is ordinary if and only if for nearly all $\overline{\mathbb{F}}$-rational points of $\mathcal{C}_{pm}$, the corresponding central projection is ordinary.

The essential statement is now:

Proposition 13. *Let us consider smooth curves of a fixed genus with ordinary non-constant functions $\mathcal{C} \to \mathbf{P}^1_{\mathbb{F}_q}$ of a fixed degree n over finite fields $\mathbb{F}_q$. Then the number of completely and distinctly split divisors in the corresponding pencil is in*

$$\frac{1}{n!} \cdot q + O\big(q^{\frac{1}{2}}\big) .$$

A *proof* was essentially already given in the course of the proof of [Die12a, Proposition 10]. Let us briefly recall the argument: Let M be a Galois closure of $\overline{\mathbb{F}}_q(C)|\overline{\mathbb{F}}_q(\mathbf{P}^1)$. A place of $\mathbb{F}_q(\mathbf{P}^1)$ is completely split in $\mathbf{F}_q(\mathcal{C})$ (which includes by definition that it is unramified) if and only if it is completely split in $M|\mathbb{F}_q(\mathbf{P}^1)$. By [Die12a, Proposition 6] the Galois group of $M\overline{\mathbb{F}}_q|\overline{\mathbb{F}}_q(\mathbf{P}^1)$ is isomorphic to S_n, and then so is the Galois group of $M|\mathbb{F}_q(\mathbf{P}^1)$. In particular, $\mathbb{F}_q$ is the exact constant field of M. One can now apply the effective Chebotaryov bound in [MS94] to obtain the result. There is also the following alternative: The Galois group $\mathrm{Gal}(M|\mathbf{P}^1_{\mathbb{F}_q})$ operates transitively on the places of M over a fixed place of $\mathbb{F}_q(\mathbf{P}^1)$. The number of completely split places of $\mathbb{F}_q(\mathbf{P}^1)$ of degree 1 is therefore given by the number of places of degree 1 of M which are unramified over $\mathbb{F}_q(\mathbf{P}^1)$ divided by $n!$. One can then obtain the estimate (and one with an explicit error term) by the bounds of Hasse & Weil. □

An application of Proposition 13 is the following proposition.

Proposition 14. *Let an integer d be fixed. We consider smooth curves $\mathcal{C}$ over finite fields $\mathbb{F}_q$ together with a birational morphism to a plane model $\pi : \mathcal{C} \to \mathcal{C}_{pm}$ of degree d. Let $P \in \mathcal{C}_{pm}(\mathbb{F}_q)$ such that only finitely many plane tangents $T \subseteq \mathbf{P}^2_{\mathbb{F}_q}$ pass through P and such that these plane tangents are all ordinary. Then the number of divisors in the corresponding $\mathfrak{g}^2_d(\pi)$ that contain P and split completely and distinctly is in*

$$\frac{1}{(d-1)!} \cdot q + O\big(q^{\frac{1}{2}}\big).$$

As already said, if the characteristic is not 2, a plane curve is ordinary if and only if it is reflexive. These curves were already considered in [Die12a].

It was proven that the number of non-ordinary tangents to a reflexive plane curve of a fixed degree is bounded. From this it then follows Theorem 3 of [Die12a] which states:

Proposition 15. *Let an integer d be fixed. We consider smooth curves $\mathcal{C}$ over finite fields $\mathbb{F}_q$ together with a birational morphism to a reflexive plane model $\pi : \mathcal{C} \to \mathcal{C}_{pm}$ of degree d. Then the number of completely and distinctly split divisors in $\mathfrak{g}^2_d(\pi)$ is in*

$$\frac{1}{d!} \cdot q + O\big(q^{\frac{1}{2}}\big).$$

For curves with morphisms to ordinary plane models given by complete base point free $\mathfrak{g}^2_{g+1}$'s, a corresponding proposition will be proven later; see Proposition 25.

3.2 Proof of Theorems 1 and 2

We are now going to prove Theorems 1 and 2 at the same time. For the latter theorem, we wish to apply the techniques of Section 2. For this reason, we consider smooth relative curves. But we also give definitions and derive results for just curves over fields or algebraically closed fields. For the proof of Theorem 2 these statements are then applied to the fibers of relative curves.

Let $\mathcal{C}$ be a smooth, non-hyperelliptic curve of genus $g \geq 4$ over a field $\mathbb{F}$. For an effective divisor D of degree $(g-3)$ on $\mathcal{C}$, the residual linear system $|K-D|$ has degree $(g+1)$ and dimension at least 2, moreover, every complete linear system with these properties can be obtained in this way. We recall here that K always denotes a canonical divisor on the curve under consideration. A first – we known – result is that for every curve over an algebraically closed field, for a general divisor D, $|K-D|$ is base point free of dimension 2. The following statement is a suitable variant of this for relative curves.

Lemma 16. *Let $\mathcal{C}/S$ be a smooth relative curve of genus $g \geq 4$. Then there is a unique open subscheme $\mathcal{M}$ of $\mathcal{C}_{g-3}$ such that for every $s \in S(\mathbb{F})$, where $\mathbb{F}$ is any field, for a $D \in (\mathcal{C}_s)_{g-3}(\mathbb{F})$, $|K-D|$ is base point free of dimension 2 if and only if $D \in \mathcal{M}(\mathbb{F})$. For this scheme $\mathcal{M}$ it holds that for $s \in S$, the fiber $\mathcal{M}_s \subseteq (\mathcal{C}_s)_{g-3}$ is non-empty.*

Proof. Consider the diagram

$$\begin{array}{ccc} \mathcal{C}_{g-3} \times \mathcal{C} & \xrightarrow{\pi} & \mathcal{C}_{g-2} \supset \mathcal{C}^1_{g-2}\,, \\ \big\downarrow{\scriptstyle \tau} & & \\ \mathcal{C}_{g-3} & & \end{array}$$

where the morphisms π and τ are given by summation and projection, respectively. The morphism τ being proper, $\tau(\pi^{-1}(\mathcal{C}^1_{g-2}))$ is a closed set. We define

$$\mathcal{A} := \tau(\pi^{-1}(\mathcal{C}^1_{g-2})) .$$

Note that $\mathcal{C}^1_{g-3}$ is contained in $\mathcal{A}$. For $s \in S(k)$ for an algebraically closed field k and a divisor $D \in (\mathcal{C}_{g-3})_s(k)$, D being contained in $\mathcal{A}_s(k)$ means that

- either $D \in (\mathcal{C}_s)^1_{g-3}(k)$, so by Riemann-Roch $|K-D|$ is of dimension ≥ 3
- or $D \in \mathcal{A}_s(k) - (\mathcal{C}^1_s)_{g-3}(k)$, so $\dim(|K-D|) = 2$ but $|K-D|$ is not base point free.

With $\mathcal{M} := \mathcal{C}_{g-3} - \mathcal{A}$ the divisors in $\mathcal{M}_s(k)$ (for $s \in S(k)$, k an algebraically close field) are exactly the divisors D on $\mathcal{C}_s$ of degree $(g-3)$ for which $|K-D|$ is base point free and of dimension 2.

As the dimension of a linear system and being base point free are stable under base change, this also holds for $s \in S(\mathbb{F})$ for arbitrary fields $\mathbb{F}$.

The scheme $\mathcal{A}$ is closed in $\mathcal{C}_{g-3}$, and for each $s \in S$, the fiber $\mathcal{M}_s$ is non-empty. For the latter we note that for k algebraically closed, there is an effective divisor D of degree $(g-3)$ on $\mathcal{C}_s$ for which $|K-D|$ is base point free of dimension 2: One chooses, starting with the canonical model, successively non-singular points and considers the images under the central projections through these points. □

Consider now some nonsingular, non-hyperelliptic curve $\mathcal{C}$ of genus $g \geq 4$ over an algebraically closed field k. We are interested in effective divisors D of degree $(g-3)$ on $\mathcal{C}$ such that $|K-D|$ is base point free of dimension 2 defining a birational morphism to an ordinary plane curve (which is then a plane model of $\mathcal{C}$ of degree $(g+1)$). Now, if any birational morphism $\pi : \mathcal{C} \to \mathcal{C}_{pm} \subseteq \mathbf{P}^2_k$ is given, corresponding to a base point free linear system $\mathfrak{d}$, then the plane bitangents of $\mathcal{C}_{pm}$ correspond to the divisors of the form $2P + 2P' + D$ of $\mathfrak{d}$ and the plane flex tangents of $\mathcal{C}_{pm}$ correspond to the divisors of the form $3p + D$ of $\mathfrak{d}$. So, in particular we want $|K-D|$ to contain only finitely many such divisors. A first simplification of our task is now:

Lemma 17. *Let $\mathfrak{d}$ be a base point free linear system on $\mathcal{C}$ of dimension 2 such that there is a point $P \in \mathcal{C}(k)$ for which no divisor of the form $2P + 2P' + D$ with $P' \in \mathcal{C}(k)$ and $D \geq 0$ is contained in $\mathfrak{d}$. Then $\mathfrak{d}$ defines a birational morphism to a plane model of $\mathcal{C}$ with only finitely many bitangents. If furthermore there is no divisor of the form $3P + D$ with $D \geq 0$ contained in $\mathfrak{d}$, the plane model is ordinary.*

Proof. Let $\pi : \mathcal{C} \twoheadrightarrow \mathcal{D} \subset \mathbf{P}^2_k$ be a morphism defined by $\mathfrak{d}$. We first show that π is birational: Let $\tilde{\mathcal{D}}$ be the normalization of $\mathcal{D}$. The morphism π factors over $\tilde{\mathcal{D}}$; let $\tilde{\pi} : \mathcal{C} \longrightarrow \tilde{\mathcal{D}}$ be the induced morphism. Let the effective divisor D on $\mathcal{C}$ be defined by $\tilde{\pi}^{-1}(\tilde{\pi}(P)) = P + D$. For the tangent T at $\tilde{\pi}(p)$ (with

respect to $\tilde{\mathcal{D}} \to \mathcal{D}$) we have $2P+2D \leq \pi^{-1}(T) \in \mathfrak{d}$. The premise in the lemma now implies that $D = 0$, and this in turn means that $\tilde{\pi}$ and π are birational.

The further statements follow from the fact that the set of points $P \in \mathcal{C}(k)$ for which there is a point $P' \in \mathcal{C}(k)$ and an effective divisor D with $2P + 2P' + D \in \mathfrak{d}$ is closed and the set of points $p \in \mathcal{C}$ for which there is an effective divisor D with $3P + D \in \mathfrak{d}$ is closed. This can be seen as follows for any linear system $\mathfrak{d}$:

Let the degree of $\mathfrak{d}$ be d. Let $\Delta \subset \mathcal{C}^2$ and $\Delta_3 \subset \mathcal{C}^3$ be the diagonals, which are closed as $\mathcal{C}$ is proper.

Let $\mathbf{P}$ be the projective subspace of $\mathcal{C}_d$ with $\mathbf{P}(k) = \mathfrak{d} \subseteq \mathcal{C}_d(k)$. Consider the commutative diagrams

$$\begin{array}{ccccc} \mathcal{C} \times \mathcal{C} \times \mathcal{C}_{d-2} & \xrightarrow{\tau_1} & \mathcal{C}_{d-2} \times \Delta \times \Delta \times \mathcal{C}_{d-2} & \xrightarrow{\tau_2} & \mathcal{C}_d \supset \mathbf{P} \\ \downarrow{\scriptstyle \pi_1} & & & \overset{\tau}{\searrow} & \\ \mathcal{C} & & & & \end{array}$$

and

$$\begin{array}{ccccc} \mathcal{C} \times \mathcal{C}_{d-2} & \xrightarrow{\tau_3} & \Delta_3 \times \mathcal{C}_{d-2} & \xrightarrow{\tau_4} & \mathcal{C}_d \supset \mathbf{P}\,, \\ \downarrow{\scriptstyle \pi_2} & & & \overset{\hat{\tau}}{\searrow} & \\ \mathcal{C} & & & & \end{array}$$

where τ_1 and τ_3 come from the diagonal morphisms, τ_2, τ_4 refer to the sum of divisors and π_1, π_2 are the projections. Here π_1, π_2 are proper morphisms and $\mathbf{P}$ is a closed in $\mathcal{C}_d$. The sets of points of $\mathcal{C}$ under consideration are $\pi_1(\tau^{-1}(\mathfrak{d}))$ and $\pi_2(\hat{\tau}^{-1}(\mathfrak{d}))$, and these sets are closed in $\mathcal{C}$. □

We now want to show: There is a point $P \in \mathcal{C}(k)$ such that there is a non-empty open subscheme of $\mathcal{C}_{g-3}$ whose k-rational points correspond to divisors D which define systems $|K - D|$ containing no divisor of the form $2P+2P'+D'$ or $3P+D''$ with $P, P' \in \mathcal{C}(k)$ and $D', D'' \geq 0$. In the next lemma, we introduce two open subschemes for each of the conditions separately. Here, first we do so with variable P in order to find an appropriate P later. Second, in order to apply the techniques of Section 2, we do so for relative curves.

Lemma 18. *Let $\mathcal{C}/S$ be a smooth relative curve of genus $g \geq 4$. Then there are open subschemes $\mathcal{M}_1, \mathcal{M}_2 \subseteq \mathcal{C}_{g-3} \times \mathcal{C}$ such that*

a) for $s \in S(k)$ for an algebraically closed field k, a tuple $(D, P) \in (\mathcal{C}_{g-3})_s(k) \times \mathcal{C}_s(k)$ lies in $(\mathcal{M}_1)_s(k)$ if and only if $|K - D - 2P|$ contains no divisor of the form $2P' + D$ for $P' \in \mathcal{C}_s(k)$ and $D \in (\mathcal{C}_{g-3})_s(k)$, where K is a canonical divisor on $\mathcal{C}_s$,

b) for $s \in S(k)$ for an algebraically closed field k, a tuple $(D, P) \in (\mathcal{C}_{g-3})_s(k) \times \mathcal{C}_s(k)$ lies in $(\mathcal{M}_2)_s(k)$ if and only if $|K - D - 3P|$ is empty.

Proof. The proof technique is the same as the one for Lemma 17. We now consider the commutative diagrams

$$\begin{array}{ccccccc} \mathcal{C}_{g-3}\times\mathcal{C}\times\mathcal{C}\times\mathcal{C}_{g-3} & \xrightarrow{\tau_1} & \mathcal{C}_{g-3}\times\Delta\times\Delta\times\mathcal{C}_{g-3} & \xrightarrow{\tau_2} & \mathcal{C}_{2g-2}\supset\mathcal{C}_{2g-2}^{g-1} \\ \downarrow{\scriptstyle \pi_1} & & & \overset{\tau}{\searrow} & \\ \mathcal{C}_{g-3}\times\mathcal{C} & & & & \end{array} \tag{1}$$

and

$$\begin{array}{ccccccc} \mathcal{C}_{g-3}\times\mathcal{C}\times\mathcal{C}_{g-2} & \xrightarrow{\tau_3} & \mathcal{C}_{g-3}\times\Delta_3\times\mathcal{C}_{g-2} & \xrightarrow{\tau_4} & \mathcal{C}_{2g-2}\supset\mathcal{C}_{2g-2}^{g-1}\,, \\ \downarrow{\scriptstyle \pi_2} & & & \overset{\hat{\tau}}{\searrow} & \\ \mathcal{C}_{g-3}\times\mathcal{C} & & & & \end{array} \tag{2}$$

where the notations are as in Lemma 17. Again π_1, π_2 are proper morphisms, and similarly to Lemma 17 $\mathcal{C}_{2g-2}^{g-1}$ is a closed subscheme of $\mathcal{C}_{2g-2}$ since it is given by the corresponding Fitting ideal (see [ACG11, XXI, §3]). In conclusion, the sets

$$\mathcal{A}_1 \coloneqq \pi_1\big(\tau^{-1}\left(\mathcal{C}_{2g-2}^{g-1}\right)\big)$$

and

$$\mathcal{A}_2 \coloneqq \pi_2\big(\hat{\tau}^{-1}\left(\mathcal{C}_{2g-2}^{g-1}\right)\big)$$

are closed in $\mathcal{C}_{g-3}\times\mathcal{C}$.

We set $\mathcal{M}_1 \coloneqq (\mathcal{C}_{g-3}\times\mathcal{C}) - \mathcal{A}_1$ and $\mathcal{M}_2 \coloneqq (\mathcal{C}_{g-3}\times\mathcal{C}) - \mathcal{A}_2$. These spaces clearly have the desired properties. □

So far, we have not shown that any of the spaces considered in Lemma 18 is nonempty. This is what we want to address now. More precisely, we want to show that for any smooth, non-hyperelliptic curve $\mathcal{C}$ over an algebraically closed field k these spaces are non-empty.

The divisors of the form $2P + 2P' + D'$ in $|K - D|$ correspond to the divisors of the form $2P + 2P' + D + D'$ of the canonical system $|K|$ and that the divisors of the form $3P + D + D''$ in $|K - D|$ correspond to the divisors of the form $3P + D''$ of $|K|$. (Here again P and P' are points of $\mathcal{C}$ and D, D', D'' are effective divisors on $\mathcal{C}$.)

This indicates that we should study tangent conditions of divisors on the canonical model of $\mathcal{C}$. For this we fix the following definitions.

Definition 19. Let $\mathcal{C} \subset \mathbf{P}_k^n$ be a curve of degree $d \geq 4$ over some algebraically closed field k and let $H \subset \mathbf{P}_k^n$ be a hyperplane. If the hyperplane divisor corresponding to H is given as

$$2P_1 + 2P_2 + P_3 + \ldots + P_{d-2}$$

for not necessarily distinct nonsingular points $P_1, \ldots, P_{d-2} \in \mathcal{C}(k)$ then H is called a *bitangent hyperplane* at P_1 (and P_2). If the hyperplane divisor corresponding to H is given as

$$3P_1 + P_2 + P_3 + \ldots + P_{d-2}$$

for not necessarily distinct nonsingular points $P_1, \ldots, P_{d-2} \in \mathcal{C}(k)$ then H is called a *flex tangent hyperplane* at P_1. If H is neither a bitangent nor a flex tangent hyperplane but still contains the tangent at a point $P_1 \in \mathcal{C}(k)$ then we call H an *ordinary tangent hyperplane* at P_1.

Let again a nonsingular non-hyperelliptic curve $\mathcal{C}$ over an algebraically closed field k be fixed. Let $\mathcal{M}_1, \mathcal{M}_2$ be as in Lemma 18. We want to show that there is a $P \in \mathcal{C}(k)$ such that the fibers $(\mathcal{M}_1)_P$, $(\mathcal{M}_2)_P \subseteq \mathcal{C}_{g-3}$ over some $p \in \mathcal{C}(k)$ are nonempty.

More generally, let $\mathcal{C} \subset \mathbf{P}^n_k$, $n \geq 3$, be a nonsingular curve over an algebraically closed field k embedded into $\mathbf{P}^n_k$ by some linear system $\mathfrak{g}^n_d$. For any $P \in \mathcal{C}(k)$ we define

$$A_{2P} = \{D \in \mathcal{C}_{n-2}(k) \mid D + 2P + 2P' + D' \in \mathfrak{g}^n_d \text{ for some } P' \in \mathcal{C}, D' \in \mathcal{C}_{d-n-2}(k)\},$$

$$A_{3p} = \{D \in \mathcal{C}_{n-2}(k) \mid D + 3P + D' \in \mathfrak{g}^n_d \text{ for some } D' \in \mathcal{C}_{d-n-1}(k)\}.$$

In the context of Lemma 18, we then apply these definitions for the canonical system. We then have for $p \in \mathcal{C}(k)$ the decompositions

$$\mathcal{C}_{g-3}(k) = (\mathcal{M}_1)_P(k) \dot\cup A_{2P} \quad , \quad \mathcal{C}_{g-3}(k) = (\mathcal{M}_2)_P(k) \dot\cup A_{3P} \, .$$

Lemma 20.

a) $A_{2P} = \mathcal{C}_{n-2}(k)$ if and only if each divisor in $\mathfrak{g}^n_d$ containing $2P$ is of the form $\tilde{D} + 2P + 2P'$ with $\tilde{D} \in \mathcal{C}_{n-4}(k)$.

b) $A_{3P} = \mathcal{C}_{n-2}(k)$ if and only if each divisor in $\mathfrak{g}^n_d$ containing $3P$ is of the form $\tilde{D} + 3P$ with $\tilde{D} \in \mathcal{C}_{n-3}(k)$.

Proof. The statements "from right to left" is quite easy: They follow from the general fact that any divisor of degree n is a subdivisor of a divisor of $\mathfrak{g}^n_d$.

Let now $A_{2P} = \mathcal{C}_{n-2}$. Let E be any divisor in $\mathfrak{g}^n_d$ containing $2P$, say $E = E' + 2P$. Furthermore, let T_p be the tangent through P. Then the divisor E is given by a hyperplane H, and the hyperplane is uniquely determined by E. This means that E generates H. Note that this means by definition that T_P and the points in E' with the appropriate tangent conditions generate the hyperplane. We therefore have a divisor D of degree $n-2$ such that $2P + D$ generates H. The divisor E is then uniquely determined by $2P + D$. Now D is contained in A_{2P}, and thus E is of the desired form.

Analogously one can prove the statement in b). □

We now come to A_{2P}:

Lemma 21. *Let $\mathcal{C} \subset \mathbf{P}^n_k$, $n \geq 3$, be a non-degenerate, non-singular curve over an algebraically closed field k. Then there are at most $(n-2)$ points P such that $A_{2P} = \mathcal{C}_{n-2}(k)$ and the tangent at P is not a bitangent.*

Proof. We prove the statement by induction on n.

For the induction base, let $n = 3$.

Let first P be a point with $A_{2P} = \mathcal{C}_{n-2}(k)$. Then by assumption any plane $H \subseteq \mathbf{P}^3_k$ containing the tangent T_P to $\mathcal{C} \subset \mathbf{P}^3_k$ at P contains the tangent T_Q at an additional point Q or meets $\mathcal{C}$ at P with at least order 4.

Now, if the second statement is satisfied for two planes containing T_P, T_P meets $\mathcal{C}$ with order 4 and thus is a bitangent. (For two planes H_1, H_2 with intersection T_P, we have $T_P \cap \mathcal{C} = (H_1 \cap H_2) \cap \mathcal{C} = (H_1 \cap \mathcal{C}) \cap (H_2 \cap \mathcal{C})$.)

This leads to two cases: T_P is a bitangent or there are infinitely many tangents to $\mathcal{C}$ that meet T_P. Now, for points q on the curve, the condition that T_q passes through T_P is a closed condition. Thus if T_P is not a bitangent, the tangents of all points of $\mathcal{C}$ pass through P.

We argue now by contradiction: Assume that there are two points P_1, P_2 with $A_{2P} = \mathcal{C}_{n-2}(k)$ such that the tangents T_{P_i} are not bitangents. Now the tangents of all points pass through both tangents T_{p_i}. In particular T_{P_1} and T_{P_2} intersect; let A be the intersection point. Now all tangents pass through A as otherwise $\mathcal{C}$ would be degenerate (which would contradict the assumption). This means that $\mathcal{C}$ is a strange curve in $\mathbf{P}^n_k$. But by [Hartshorne, IV, Theorem 3.9] there are no non-singular, non-degenerate, strange curves in $\mathbf{P}^n_k$ for $n \geq 3$. We thus have the desired contradiction.

Suppose now that the statement has been proven for some n. We want to prove it now for $n+1$.

We again argue by contradiction. So assume that there $(n+1)-2+1 = n$ points $P_1, \ldots, P_n$ with $A_{2P_i} = \mathcal{C}_{(n+1)-3}(k)$ such that the tangent T_{p_i} is not a bitangent.

Let $\mathcal{U}$ be the union of the tangent and secant variety of $\mathcal{C}$ in $\mathbf{P}^{n+1}_k$; by [Hartshorne, IV, Proposition 3.5 and Corollary 3.6] $\mathcal{U}$ is 3-dimensional.

Let Q be any point in $\mathbf{P}^{n+1}_k - \mathcal{U}$ and consider the central projection ϕ_Q through Q. Note that the image $\phi_Q(\mathcal{C})$ in $\mathbf{P}^{n+1}_k$ is now again non-singular.

We have $A_{2\phi_Q(P_i)} = \phi_Q(\mathcal{C}_{n-2})(k)$. By the induction hypothesis, the tangents to two of the points $\phi_Q(P_i)$ are bitangents. These bitangents, lines in $\mathbf{P}^n_k$, correspond to hyperplanes $H_{Q,i}$ in $\mathbf{P}^{n+1}_k$ containing Q and T_{P_i}. Now $H_{q,i}$ contains the tangent of another point or meets $\mathcal{C}$ at P_i with least order 4.

We now vary Q. For each Q we have two i (a priori depending on q) such that the stated condition holds. But then there is also a dense subset such that it holds for two single i, say $i = 1, 2$. As the condition is closed, we conclude: For $i = 1, 2$ every plane containing T_{P_i} contains the tangent of another point or meets $\mathcal{C}$ at P_i with least order 4.

With the same arguments as for $n = 3$ we arrive at a contradiction. Indeed, revisiting this case, we see that all that is needed are two points with the stated property. In particular, the dimension of the projective space is irrelevant. □

We study the spaces A_{3P} only for the canonical system. For this we use tangents to the canonical model. This relies on yet another notion of tangency, namely that of the (usual) tangent of a curve $\mathcal{C}$ in some projective space $\mathbf{P}^n_k$:

Definition 22. Let $\mathcal{C} \subset \mathbf{P}^n_k$, $n \geq 2$, be a non-degenerate curve over some algebraically closed field k. Consider a tangent line $T \subset \mathbf{P}^n_k$ at some nonsingular $P \in \mathcal{C}(k)$. We call T a *bitangent* (at P) if it either is the tangent at two distinct nonsingular points on $\mathcal{C}$ or if it is a tangent of at least order 4 at P. We call T a *flex tangent* (at P) if it is a tangent of at least order 3 at P. Otherwise we call T an *ordinary tangent*.

Proposition 23. *Let $\mathcal{C}$ be a non-hyperelliptic, nonsingular curve of genus $g \geq 4$ over some algebraically closed field k.*

a) There are no bitangents of the canonical model of $\mathcal{C}$.

b) The number of flex tangents of the canonical model of $\mathcal{C}$ is bounded by 12 if $g = 4$ and by $(g + 2)$ otherwise.

Proof. We identify $\mathcal{C}$ with its canonical model in $\mathbf{P}^{g-1}_k$.

On a) Assume there is a bitangent at $P \in \mathcal{C}(k)$. Then by definition there is a point $P' \in \mathcal{C}(k)$ on this tangent such that

$$g - 3 = \dim(|K - 2P|) = \dim(|K - 2P - 2P'|).$$

So by Riemann-Roch we have

$$\begin{aligned}\dim(|2P + 2P'|) &= \deg(2P + 2P') - g + 1 + \dim(|K - (2P + 2P')|)\\ &= 4 - g + 1 + g - 3\\ &= 2.\end{aligned}$$

Thus $|2P + 2P'|$ defines a complete $\mathfrak{g}^2_4$ on $\mathcal{C}$. Since $\mathcal{C}$ is not hyperelliptic, this contradicts Clifford's Theorem (see for instance [Har77, IV], Theorem 5.4).

On b) Consider some $P \in \mathcal{C}(k)$ such that the tangent to $\mathcal{C}$ at P is a flex tangent. So we get

$$\dim(|K - 2P|) = \dim(|K - 3P|).$$

By a similar calculation to the one above this implies that $\dim(|3P|) = 1$ hence any flex tangent defines a $\mathfrak{g}^1_3$ on $\mathcal{C}$.

Since $\mathcal{C}$ is not hyperelliptic, any of its $\mathfrak{g}_3^1$'s is complete and base point free. Hence it defines a morphism $\Phi : \mathcal{C} \to \mathbf{P}_k^1$ of degree 3. The corresponding extension of function fields $k(\mathcal{C})|k(\mathbf{P}_k^1)$ is separable as otherwise it was purely inseparable and then the genus of $\mathcal{C}$ would be 0.

Any divisor $3P$ as above corresponds to a ramification point of Φ. By Hurwitz's Theorem we have

$$2g - 2 = 3 \cdot (-2) + \deg(R)$$

where R denotes the ramification divisor of Φ. So $\deg(R) = 2g + 4$; the number of ramification points of Φ of order 3 is then bounded by $(g + 2)$.

Hence any $\mathfrak{g}_3^1$ on $\mathcal{C}$ contains at most $(g + 2)$ divisors of the form $3p$. By the analysis following [ACGH85, V, Theorem 1.1] we distinguish two cases: Either $g = 4$ and there are at most two $\mathfrak{g}_3^1$'s on $\mathcal{C}$ or $g \geq 5$ and there is at most one such linear system. By the bound on the ramification points the result follows. □

Remark. We see from the proof that all tangents of the canonical model of a non-singular, non-hyperelliptic and non-trigonal curve are ordinary.

Now Proposition 23 and Lemma 21 yield a nice result about the number of those points $p \in \mathcal{C}(k)$ at which each effective divisor of degree $(g-3)$ leads to a non-ordinary tangent hyperplane on the canonical model of $\mathcal{C}$:

Proposition 24. *Let $\mathcal{C}$ be a non-hyperelliptic, nonsingular curve of genus $g \geq 4$ over some algebraically closed field k. Then there are at most*

$$n := \begin{cases} 13 & \text{if } g = 4 \\ 2g - 1 & \text{if } g \geq 5 \end{cases}$$

points $P \in \mathcal{C}(k)$ such that A_{2P} or A_{3P} are all of $\mathcal{C}_{g-3}(k)$.

Proof. Identify $\mathcal{C}$ with its canonical model.

Consider some $p \in \mathcal{C}(k)$ such that $A_{3p} = \mathcal{C}_{g-3}(k)$. Then each tangent hyperplane at p meets $\mathcal{C}$ with order at least 3 at P. We conclude that the tangent to $\mathcal{C}$ at P is a tangent of at least order 3. In particular, this tangent is a flex tangent. By Proposition 23 there are at most

$$12 \text{ if } g = 4 \text{ or}$$
$$g + 2 \text{ if } g \geq 5$$

such points P.

Moreover, as by Proposition 23 there are no bitangents of $\mathcal{C}$, by Lemma 21 there are at most $(g-1)-2 = (g-3)$ points $P \in \mathcal{C}(k)$ such that $A_{2P} = \mathcal{C}_{n-2}(k)$.

So overall there are at most

$$n := \begin{cases} 12 + 1 = 13 & \text{if } g = 4 \\ (g + 2) + (g - 3) = 2g - 1 & \text{if } g \geq 5 \end{cases}$$

points $P \in \mathcal{C}(k)$ such that A_{2P} or A_{3P} are all of $\mathcal{C}_{g-3}(k)$. □

Combining Lemma 16 and Lemma 18 with Lemma 17 and Proposition 24, we are now able to show that "many" divisors in $\mathcal{C}_{g-3}$ lead to an ordinary plane model of degree $(g+1)$ via their residual, as claimed in Theorem 1 and Theorem 2:

Proof of Theorem 1 and Theorem 2. Let $\mathcal{C}/S$ be a smooth relative curve of genus $g \geq 4$ whose (geometric) fibers are non-hyperelliptic.

We define open subschemes $\mathcal{M}_1, \mathcal{M}_2 \subseteq \mathcal{C}_{g-3} \times \mathcal{C}$ as in Lemma 18, denote the complement of $\mathcal{A} \subseteq \mathcal{C}_{g-3}$ by $\mathcal{M}_3$ and set

$$\mathcal{N} := \mathcal{M}_1 \cap \mathcal{M}_2 \cap (\mathcal{M} \times \mathcal{C}) .$$

For $s \in S(\mathbb{F})$ and $P \in \mathcal{C}_s(\mathbb{F})$, by Lemma 17 any divisor D in $(\mathcal{N}_s)_P(\mathbb{F})$ leads to an ordinary plane model of degree $(g+1)$ via $|K-D|$.

If we apply this to S the spectrum of an algebraically closed field k and $\mathbb{F} = k$, with Lemma 16, Lemma 17 and Proposition 24 we obtain Theorem 1.

To obtain Theorem 2, we now consider $\mathcal{C}^{g-3} - \mathcal{N}$ as a scheme over $\mathcal{C}$ and apply Proposition 5 a). We conclude: There exists a constant $C_0 > 0$ such that for any $s \in S(\mathbb{F}_q)$ and any $P \in \mathcal{C}_s(\mathbb{F}_q)$ for which the fiber $(\mathcal{N}_s)_P$ is nonempty (and therefore dense in $(\mathcal{C}_s)_{g-3}$) we have

$$\#(\mathcal{C}_{g-3} - (\mathcal{N}_s)_P)(\mathbb{F}_q) \leq C_0 \cdot q^{g-4} .$$

This implies that there is a $C > 0$ such that

$$\frac{\#(\mathcal{C}_s)_{g-3}(\mathbb{F}_q) - \#(\mathcal{N}_s)_p(\mathbb{F}_q)}{\#(\mathcal{C}_s)_{g-3}(\mathbb{F}_q)} \leq \frac{C}{q}$$

for any s and p as previously stated.

We know that for any $s \in S(\mathbb{F})$ there is a $P \in \mathcal{C}_s(\mathbb{F})$ such that $(\mathcal{N}_s)_P$ is non-empty. We can therefore conclude:

For every $s \in S(\mathbb{F}_q)$, the probability that a uniformly randomly chosen effective divisor D of degree $(g-3)$ on $\mathcal{C}_s$ leads to a linear system $|K-D|$ which does not define an ordinary plane model of degree $(g+1)$ is $\leq \frac{C}{q}$.

If we apply this now to the smooth relative curve $\mathcal{Z}_g^{nh}/\mathcal{H}_g$ introduced in 2.2, the result follows. □

3.3 Proof of Theorem 4

The following result was already announced after Proposition 15.

Proposition 25. *Let some natural number $g \geq 4$ be fixed. We consider smooth, non-hyperelliptic curves $\mathcal{C}/\mathbb{F}_q$ together with complete base point free $\mathfrak{g}^2_{g+1}$'s defining ordinary plane models. Then there are*

$$\frac{1}{(g+1)!} \cdot q^2 + O\big(q^{\frac{3}{2}}\big)$$

divisors in the $\mathfrak{g}^2_{g+1}$ that split completely and distinctly.

As already stated in and above Proposition 15, this statement has already been proven in [Die12a] provided that the characteristic is not 2, so we only have to prove it in characteristic 2. The following proof holds in any characteristic.

Proof. Pick a smooth, non-hyperelliptic curve $\mathcal{C}/\mathbb{F}_q$ and let $\pi : \mathcal{C} \to \mathcal{C}_{pm}$ be a birational morphism to an ordinary plane model of degree $(g+1)$. The number of non-ordinary tangents of $\mathcal{C}$ with respect to π is finite. Let us assume for the moment that it is in $O(1)$, that is, bounded. The number of singular points of $\mathcal{C}_{pm}$ is also bounded, namely by $\frac{g(g-1)}{2} - g$. By Hasse-Weil the number of points in $\mathcal{C}(\mathbb{F}_q)$ is in $q + O(q^{\frac{1}{2}})$.

If for a point $P \in \mathcal{C}_{pm}(\mathbb{F}_q)$ only ordinary tangents (of whatever points) run through p, by Proposition 14 the number of completely and distinctly split divisors in $\mathfrak{g}^2_d(\pi)$ containing P is in

$$\frac{1}{g!} \cdot q + O\big(q^{\frac{1}{2}}\big) ,$$

and so is the number of such divisors containing only non-singular points of $\mathcal{C}_{pm}$.

If we vary P, each such divisor is selected exactly g times, thus the number of divisors which split completely and distinctly into non-singular points of $\mathcal{C}_{pm}$ is in

$$\frac{1}{(g+1)!} \cdot q^2 + O\big(q^{\frac{1}{2}}\big).$$

By the first considerations, the number of completely and distinctly split divisors containing a non-singular point or a point which lies on a non-ordinary tangent is in $O(q)$. This gives the claim.

We still have to show that the number of non-ordinary tangents is bounded. For this we first consider a smooth relative curve $\mathcal{C}$ of genus g over a noetherian base S. Let $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$ and $\mathcal{M}$ be as in the proof of Theorem 2. We consider $\mathcal{M}$ as a scheme over $\mathcal{C}_{g-3}$. For $s \in S(\mathbb{F})$ and $D \in (\mathcal{M}_3)_s(\mathbb{F}) \subseteq (\mathcal{C}_{g-3})_s(\mathbb{F})$ the $\mathbb{F}$-rational points of the fiber of $\mathcal{M}$ over D correspond to the non-ordinary tangents with respect to the morphism to the plane model defined by $|K - D|$. The same holds for extensions of $\mathbb{F}$. In particular, such a fiber is finite if and only if the plane model is ordinary.

By Proposition 5 a) there is a constant $C > 0$ such that the number of $\mathbb{F}$-rational points in the zero-dimensional fibers is bounded by C. Thus whenever an ordinary curve is defined by a divisor as considered, the number of non-ordinary tangents is bounded by C.

As in the proof of Theorem 2 we apply this now to $\mathcal{Z}^{nh}_g/\mathcal{H}_g$. This gives the result. □

We can derive Theorem 4:

Proof of Theorem 4. The case $g = 3$ has already been treated in [Die12a] as a special case of Theorem 3, where it is labeled as "$d = 4$".

So we may assume that $g \geq 4$.

Let $\mathcal{C}/\mathbb{F}_q$ be as above. By Hasse-Weil, the number of points in $\mathcal{C}(\mathbb{F}_q)$ is in $q + O(q^{\frac{1}{2}})$. So the number of completely and distinctly split divisors in $\mathcal{C}_{g-3}(\mathbb{F}_q)$ is in

$$\binom{q + O(q^{\frac{1}{2}})}{g-3} = \frac{1}{(g-3)!} \cdot q^{g-3} + O(q^{g-\frac{7}{2}}).$$

By Theorem 2 the number of effective divisors D of degree $(g-3)$ on $\mathcal{C}$ for which $|K - D|$ does not define an ordinary plane model of degree $(g+1)$ is in $O(q^{g-4})$.

Combining this we obtain that the number of completely and distinctly split divisors $D \in \mathcal{C}_{g-3}(\mathbb{F}_q)$ that lead, via $|K - D|$, to a morphism to an ordinary plane model of degree $(g+1)$ is in

$$\frac{1}{(g-3)!} \cdot q^{g-3} + O\big(q^{g-\frac{7}{2}}\big)\,.$$

By Proposition 25 for each morphism π to an ordinary plane model the number of completely and distinctly split divisors in the corresponding linear system $\mathfrak{g}^2_{g+1}(\pi)$ is in

$$\frac{1}{(g+1)!} \cdot q^2 + O\big(q^{\frac{3}{2}}\big).$$

In conclusion, the number of pairs (D_1, D_2) where the completely and distinctly split divisor $D_1 \in \mathcal{C}_{g-3}(\mathbb{F}_q)$ defines an ordinary plane model of degree $(g+1)$ (and a morphism to it), say $\pi : \mathcal{C} \to \mathcal{C}_{pm}$, and D_2 is a completely and distinctly split divisor in the corresponding $\mathfrak{g}^2_{g+1}(\pi)$ is in

$$\begin{aligned}&\big(\frac{1}{(g-3)!} \cdot q^{g-3} + O(q^{g-\frac{7}{2}})\big)\big(\frac{1}{(g+1)!} \cdot q^2 + O(q^{\frac{3}{2}})\big)\\ &= \frac{1}{(g-3)!\,(g+1)!} \cdot q^{g-1} + O(q^{g-\frac{3}{2}}).\end{aligned}$$

So is also the number of pairs (D_1, D_2) with the given properties and the additional property that D_1 and D_2 have disjoint support, that is, define a completely and distinctly split divisor $D_1 + D_2$, which is then a completely and distinctly split divisor in K.

Now, as there are at most $O(q^{g-4})$ effective divisors of degree $(g-3)$ which do not lead to a morphism to an ordinary plane model, there are at most $O(q^{g-2})$ divisors in $|K|$ which have a subdivisor of degree $(g-3)$ which does not lead to a morphism to an ordinary plane model.

So there are $\frac{1}{(g-3)!\,(g+1)!} \cdot q^{g-1} + O(q^{g-\frac{3}{2}})$ pairs (D_1, D_2) as above such that with $D = D_1 + D_2$ every subdivisor of degree $(g-3)$ of D leads to a

morphism to an ordinary plane model. The number of pairs leading to the same element in $|K|$ is

$$\binom{2g-2}{g-3} = \frac{(2g-2)!}{(g+1)!\,(g-3)!}\,.$$

We thus have: There are

$$\frac{1}{(2g+2)!} \cdot q^{g-1} + O\big(q^{g-\frac{3}{2}}\big)$$

completely and distinctly split divisors D in $|K|$ such that every subdivisor of degree $(g-3)$ of D leads to a morphism to an ordinary plane model.

Moreover, as already explained the number of completely and distinctly split divisors in $|K|$ which have a subdivisor of degree $(g-3)$ not leading to a morphism to an ordinary plane model (which then has degree $(g+1)$) is in $O(q^{g-2})$.

So overall there are

$$\frac{1}{(2g-2)!} \cdot q^{g-1} + O\big(q^{g-\frac{3}{2}}\big)$$

completely and distinctly split divisors in $|K|$, as claimed. □

3.4 Algorithms and proof of Theorem 3

We now give an efficient algorithm to compute ordinary plane models given by a complete $\mathfrak{g}^2_{g+1}$ and morphisms to them. After this, we discuss how one can transfer divisors and how Theorem 3 can be obtained.

3.4.1 Computing an ordinary plane model

Recall that for a non-singular point P of a plane curve, the tangents of arbitrary points on the curve running through P are given by the intersection of the curve with the polar curve. This is used in the algorithm.

In the algorithm and afterwards we use the following notation: The input curve $\mathcal{C}$ is represented by a plane model $\mathcal{C}_{pm}$. The new plane model to be computed is denoted $\mathcal{C}'_{pm}$ and the morphism to the plane model by φ. As always, g is the genus of $\mathcal{C}$. Differently from the above and because of later considerations, we denote the effective divisor of degree $(g-3)$ considered in the construction by D_0.

Algorithm

Input. A smooth, non-hyperelliptic curve $\mathcal{C}$ of genus $g \geq 4$ over $\mathbb{F}_q$, represented by a plane model $\mathcal{C}_{pm}$.

Output. An ordinary plane model of $\mathcal{C}$ given by a complete base point free $\mathfrak{g}^2_{g+1}$ and a morphism to it.

1. Compute a canonical divisor K on $\mathcal{C}$.
2. Compute an effective completely and distinctly split divisor D_0 of degree $(g-3)$ uniformly at random.
3. Compute a basis f_0, f_2, f_3 of the space $L(K - D_0)$. If the dimension is not 3, go back to Step 2.

   (For notation, let $\varphi : \mathcal{C} \to \mathrm{Proj}(\mathbb{F}_q[X', Y', Z'])$ be the morphism given by the basis.)
4. Compute the image $\mathcal{C}'_{pm}$ of φ (via a homogeneous equation in $\mathbb{F}_q[X', Y', Z']$).
5. If $\deg(\mathcal{C}'_{pm}) < (g+1)$, go back to Step 2.
6. Compute a non-singular point P in $\mathcal{C}_{pm}(\mathbb{F}_q)$ uniformly at random.
7. Compute the polar curve for the point P.
8. Compute the $\mathbb{F}_q$-rational intersection points Q of the polar curve with $\mathcal{C}'_{pm}$ and then the lines through P and the points Q.
9. If these lines are non-ordinary tangents, go back to Step 2.
10. Output $\mathcal{C}'_{pm}$ and φ.

It is clear that if the algorithm terminates then the desired plane model and morphism to it have been computed.

A curve of genus g over a finite field can always be given by a plane model of degree $O(g)$, so we assume that this is the case. For computation with divisors and for the computation of the space $L(K - D_0)$, one can use ideal arithmetic for divisors and Heß' algorithm for the computation of Riemann-Roch spaces ([Heß01]). With this, these computations can be carried out in polynomial time. For more information on this, we refer also to [Die11, Section 2] and also to the considerations in subsection 3.4.3 below.

The computation of the intersection points of the curve with the polar curve can be performed in expected polynomial time with resultants.

In total, all the individual steps (without repetitions) can be performed in polynomial time (for curves of varying genus). Finally, for curves of a fixed genus, by Theorem 2 the number of repetitions converges to 0. Therefore for curves of a fixed genus the algorithm runs in polynomial time.

We note that in Step 1 we say that the divisor should be chosen uniformly among effective completely and distinctly split divisors of degree $(g-3)$ rather than that it should be chosen uniformly at random among all effective divisors of degree $(g-3)$. For the latter, by our knowledge it would be necessary to first compute the L-polynomial. This can be done in polynomial time for curves of a fixed genus but – by current knowledge – not in polynomial time uniformly for all curves. Moreover, the computation is in practice very difficult. By using completely and distinctly split divisors we have an algorithm which is theoretically more pleasing and more relevant in practice.

Let us state the theoretical algorithmic result in a brief way:

Proposition 26. *For curves of a fixed genus ≥ 4 over finite fields, an ordinary plane model of degree $(g+1)$ and a morphism to it, both given by a complete linear system, can be computed in polynomial time.*

3.4.2 Proof of Theorem 3

If $\varphi : \mathcal{C} \to \mathcal{C}'_{pm}$ is a birational morphism to an ordinary plane model of $\mathcal{C}$ as computed in the algorithm, by Proposition 25 there are $\sim \frac{1}{(g+1)!}\, q^2$ completely and distinctly split divisors in the linear system $\mathfrak{g}^2_{g+1}(\pi)$. This means in particular that by [Die12a, Theorem 2] the discrete logarithm problem for the curve in the representation by $\mathcal{C}'_{pm}$ can be solved in an expected time of $\tilde{O}(q^{2-\frac{2}{g-1}})$.

The evident way to prove Theorem 3 is now to show that one can transfer an instance of the discrete logarithm problem sufficiently efficiently. Actually, this is not necessary: The algorithm for Theorem 3 in [Die12a] relies on the consideration of divisors in the linear system given by a plane model, and for this, one can also consider the system $|K - D_0|$ with respect to the original representation. We note here the following aspect of the algorithm in [Die12a], which is the one which requires the most thought with this approach: The factor base is a subset of the $\mathbb{F}_q$-rational points of the non-singular part of $\mathcal{C}_{pm}$. Now, an $\mathbb{F}_q$-rational point P of $\mathcal{C}$ is a non-singular point of $\mathcal{C}_{pm}$ if and only if $|K - D_0 - P|$ is base point free, and this can be easily checked.

3.4.3 Transferring divisors

For completeness we now also discuss how one can efficiently map points and divisors of $\mathcal{C}$ with respect to the original plane model $\mathcal{C}_{pm}$ to the normalization of $\mathcal{C}'_{pm}$ via φ. These considerations will also be of relevance in [DK].

We consider first a smooth, non-hyperelliptic curve $\mathcal{C}$ of an arbitrary genus g given by a plane model $\mathcal{C}_{pm} \subseteq \mathrm{Proj}(\mathbb{F}_q[X,Y,Z])$ of degree $O(g)$. Let us denote the pull-back of a linear form W to $\mathcal{C}$ by $W_{|\mathcal{C}}$ and of a function f on $\mathbf{P}^2_{\mathbb{F}_q}$ (whose pole divisor does not contain $\mathcal{C}_{pm}$) to $\mathcal{C}$ by $f_{|\mathcal{C}}$.

Let us first briefly recall ways to represent divisors on $\mathcal{C}$: First, there is the representation via two ideals already mentioned: $\mathbb{F}_q(\mathcal{C})|\mathbb{F}_q(x_{|\mathcal{C}})$ or $\mathbb{F}_q(\mathcal{C})|\mathbb{F}_q(y_{|\mathcal{C}})$ is separable; let us assume that $\mathbb{F}_q(\mathcal{C})|\mathbb{F}_q(x_{|\mathcal{C}})$ is. Then a divisor is represented by tuples of two ideals, where one ideal is a $\mathbb{F}_q[x_{|\mathcal{C}}]$-module and one is a $\mathbb{F}_q[\frac{1}{x_{|\mathcal{C}}}]$-module. We call this *ideal theoretic representation.*

A divisor D defining a base point free complete linear system $|D|$ can be represented by a system of generating global sections of the sheaf $\mathcal{O}(D)$, in particular by a basis of the space $L(D) = \Gamma(\mathcal{C}, \mathcal{O}(D))$. Note that any divisor of degree at least $2g$ is base point free. A arbitrary divisor D of

positive degree can be represented as follows: One chooses any divisor D_1 of degree at least $2g+\deg(D)$ and represents D by systems of generating global sections of the two spaces $L(D_1)$ and $L(D_1 - D)$. Let us call this the *global section representation*. We assume in the following that D_1 is effective with a degree of $O(g + \deg(D))$ and the systems of global sections are linearly independent. If one is interested in representing effective divisors of bounded degree c, one can once and for all choose a divisor D_1 of degree at least $2g+a$ and a basis of $L(D_1)$ and then represent any divisor D in question by the coordinate matrix of an $\mathbb{F}_q$-basis of $L(D_1 - D)$ with respect to the chosen basis of $L(D_1)$. This might be called *subspace representation*.

In addition, rational points over non-singular points of $\mathcal{C}_{pm}$ can be represented by their coordinates, and this can be extended to all closed points over non-singular points of $\mathcal{C}_{pm}$ via a base extension; we speak here of *representation via coordinates*. Note that the representation of rational points via coordinates can be seen as an incomplete variant of the subspace representation. Here the fixed divisor D_1 is $(Z_{|\mathcal{C}})_0$ and the fixed system of generating global sections is $1, x, y$. The problem is that for a singular rational point p of $\mathcal{C}$, $|(Z_{|\mathcal{C}})_0 - P|$ is not base point free.

Besides representing divisors as described (with the ideal, the global section or the subspace representation), they can be represented in free representation, that is, in factored form, where the individual prime divisors can be represented in any of the described ways and also in coordinate representation if possible.

One can change between all the given representations (with the obvious restrictions for the coordinate representation) in an expected time of $g \cdot \log(q) \cdot \mathrm{ht}(D)$, where $\mathrm{ht}(D)$ is the height of D; cf. [Die12a, Definition 2.3]. Here randomization is only required to factor divisors when computing a free representation.

Let us now suppose we are given a birational morphism φ from $\mathcal{C}$ to a (new) plane model $\mathcal{C}'_{pm} \subset \mathrm{Proj}(\mathbb{F}_q[X', Y', Z'])$ of $\mathcal{C}$, where $\mathcal{C}'_{pm}$ has a degree of $O(g)$. Concretely, φ shall be given by three functions f_0, f_1, f_2. These functions might be a basis of $L(K - D_0)$ for an effective divisor D_0 of degree $(g-3)$, but need not be. For the following complexity theoretic statements, we suppose that the system f_0, f_1, f_2 is given via the following unique representation: f_i is given as $\frac{g_i(x_{|\mathcal{C}}, y_{|\mathcal{C}})}{h(x_{|\mathcal{C}})}$, where $g_i(x, y)$ and $h(x)$ are polynomials, the degree of $g_i(x, y)$ in y is minimal (that is, smaller than $\deg(x_{|\mathcal{C}})$) and with respect to this condition the degree of $h(x)$ is also minimal.

Let $x' := \frac{X'}{Z'}, y' := \frac{Y'}{Z'}$. We denote the normalization of $\mathcal{C}'_{pm}$ by $(\mathcal{C}', \pi')$. We thus have an isomorphism $\varphi : \mathcal{C} \tilde{\to} \mathcal{C}'$, or with other words, $(\mathcal{C}, \pi' \circ \varphi)$ is also a normalization of $\mathcal{C}'_{pm}$. Nonetheless, we keep the curves $\mathcal{C}$ and $\mathcal{C}'$ separate because we want to emphasize that a computation has to be performed via φ.

A first, one might say naive, approach is based on the coordinate representation. We can express φ also via $(g_1(x_{|\mathcal{C}}, y_{|\mathcal{C}}), g_2(x_{|\mathcal{C}}, y_{|\mathcal{C}}), g_3(x_{|\mathcal{C}}, y_{|\mathcal{C}}))$, and we wish to apply these functions to a point to obtain a point in $\mathcal{C}'$. This computation can fail for three reasons: The point "lies over infinity", the result is $(0,0,0)$ or the result is a singular point of $\mathcal{C}'_{pm}$. In the first two cases one might modify the computation, but in any case one sees that the number of "failures" is polynomially bounded in the genus.

Now, for arbitrary rational points, given in ideal representation, an approach to compute images under functions has been described in [Die12b, Section 5]. Briefly, if $\varphi(P)$ is not ∞, it is the unique scalar a such that $f - a$ lies in $L((f)_\infty - a)$. With this approach and the consideration of appropriate quotients of the f_i, one can also evaluate $\varphi(P) \in \mathbf{P}^2(\mathbb{F}_q)$ at any point of $\mathcal{C}$. However, also this approach does not give the desired point in $\mathcal{C}'$ if the image in $\mathcal{C}'_{pm}$ is a singular point. Just as the previous computation, this computation can also be performed in polynomial time in $g \cdot \log(q)$.

A very different approach which works on divisors in non-factored form is to consider a "transport of functions". This approach first goes in the opposite direction: We have $(x')_{|\mathcal{C}} \circ \varphi = \frac{f_0}{f_3}$ and $(y')_{|\mathcal{C}} \circ \varphi = \frac{f_1}{f_3}$. With this, one can easily and efficiently transfer, via φ^{-1}, a function on $\mathcal{C}'$ (given with respect to $\mathcal{C}'_{pm}$) to the corresponding function on $\mathcal{C}$ (given with respect to $\mathcal{C}_{pm}$). One can then also transfer Riemann-Roch spaces and thus also divisors in global section representation and thus in particular in subspace representation. The latter two computations can be performed in a time which is polynomial in $g \cdot \log(q) \cdot \mathrm{ht}(D)$. With the obvious limitations concerning singular points, this can also be applied to points in coordinate representation, where from the result one can compute for example an ideal representation.

We would like to apply this to φ instead of φ^{-1}. For this, we desire to compute φ^{-1}, which is given by the triple $(x_{|\mathcal{C}} \circ \varphi^{-1}, y_{|\mathcal{C}} \circ \varphi^{-1}, 1)$.

Now, the functions $x_{|\mathcal{C}}, y_{|\mathcal{C}}$ are given by their divisors and the value at one rational point. So, we want to transfer these divisors and a point to $\mathcal{C}'$. To transfer a point we can apply the naive approach (possibly over an extension field). The idea to transfer the divisors of the functions is to factor the divisors $\mathrm{div}(x_{|\mathcal{C}}), \mathrm{div}(y_{|\mathcal{C}})$ and to apply the naive approach to the points involved (possibly over an extension field). This approach can of course fail. If this is the case, we apply a coordinate transformation to $X_{|\mathcal{C}}, Y_{|\mathcal{C}}, Z_{|\mathcal{C}}$ (if the field is too small over an extension field) and try again. Then in the image we revert the coordinate transformation. If the base field has been extended, this can then be reverted as well. This computation can then be performed in polynomial time in $g \cdot \log(q)$.

All in all, the desired computations related to transfer of points and divisors can be performed as efficiently as one can realistically expect from a theoretical point of view (up to exponents at least) and can be performed efficiently in practice as well.

References

[ACG11] E. Arbarello, M. Cornalba, and P. Griffiths. *Geometry of Algebraic Curves: Volume II with a contribution by Joseph Daniel Harris.* Grundlehren der mathematischen Wissenschaften. Springer, 2011.

[ACGH85] E. Arbarello, M. Cornalba, P. Griffiths, and J. Harris. *Geometry of Algebraic Curves.* Springer, 1985.

[Die06] C. Diem. An index calculus algorithm for plane curves of small degree. In *Algorithmic Number Theory - ANTS VII*, 2006.

[Die11] C. Diem. On the discrete logarithm problem in class groups of curves. *Mathematics of Computation*, 80:443 – 475, 2011.

[Die12a] C. Diem. On the discrete logarithm problem for plane curves. *Journal de Théorie des Nombres de Bordeaux*, 2012.

[Die12b] C. Diem. On the use of expansion series for stream ciphers. *LMS Journal of Computation and Mathematics*, 15:326–340, 2012.

[DK] C. Diem and S. Kochinke. Computing discrete logarithms with pencils. To come, a preliminary version is available under `http://www.math.uni-leipzig.de/~diem`.

[DM69] P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 36(1):75–109, 1969.

[Ful69] W. Fulton. Hurwitz schemes and irreducibility of moduli of algebraic curves. *Annals of Mathematics*, 90(3):542–575, 1969.

[GH80] P. Griffiths and J. Harris. On the variety of special linear systems on a general algebraic curve. *Duke Mathematical Journal*, 1980.

[Gie82] D. Gieseker. Stable curves and special divisors: Petri's conjecture. *Inventiones mathematicae*, 66(2):251–275, 1982.

[GL02] S. Ghorpade and G. Lachaud. Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. *Mosc. Math. J.*, pages 589–631, 2002.

[Gro67] A. Grothendieck. Éléments de géométrie algébrique. *Publications mathématiques de l'IHÉS*, 4, 8, 11, 17, 20, 24, 28, 32, 1960–1967.

[Har77] R. Hartshorne. *Algebraic Geometry.* Springer-Verlag, 1977.

[Heß01] F. Heß. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symb. Comput.*, 11, 2001.

[LW54] S. Lang and A. Weil. Number of points of varieties in finite fields. *American Journal of Mathematics*, 76(4):pp. 819–827, 1954.

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric Invariant Theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1994.

[MS94] V. Murty and J. Scherk. Effective versions of the Chebotarev density theorem for funciton fields. *C. R. Acad. Sci.*, 319:523–528, 1994.

[Tao13] T. Tao. *Compactness and Contradiction*. American Mathematical Society, 2013.