On the discrete logarithm problem in elliptic curves

Claus Diem

April 7, 2009

Abstract

We study the elliptic curve discrete logarithm problem over finite extension fields. We show in particular that there exists a sequence of (non-prime) finite fields such that the elliptic curve discrete logarithm problem restricted to curves over these fields can be solved in subexponential expected time in the group size.

Contents

1 Introduction 2

2 The key algorithms 7
2.1 The decomposition algorithm 7
2.2 The index calculus algorithm 10
2.3 Computing a suitable covering 16

3 Some results on multihomogeneous polynomials 17
3.1 Intersection theory in $(\mathbb{P}^1_k)^n$ 18
3.2 Multigraded resultants 20
3.3 Computing resultants and solving systems 22
3.4 Interpolation 27

4 The summation polynomials 29

5 Geometric background on the algorithm and analysis 33
5.1 Weil restrictions 33
5.2 Background on the factor base 35
5.3 The role of the summation polynomials 38
5.4 Determination of non-zero-dimensional fibers 43

References 49

1 Introduction

The classical discrete logarithm problem in finite prime fields can be solved in an expected time which is subexponential in the group size via the so-called index calculus method. In contrast, it is not known if the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields (the *elliptic curve discrete logarithm problem* for short) can be solved in subexponential expected time in the group size. While some infinite classes of elliptic curves are known for which the problem can be solved in subexponential expected time (for example supersingular elliptic curves), it was up to now not known if there exists a sequence of finite fields of increasing size such that the problem restricted to curves over these fields can be solved in subexponential expected time.

We prove that such a sequence of finite fields exists. Indeed, we establish that there exists such a sequence such that the problem restricted to curves over these fields can be solved in an expected time of

$$e^{\mathcal{O}(\log(q)^{2/3})} ,$$

where $\mathbb{F}_q$ is the ground field.

In the following, q is always a prime power and n a natural number. Our main result is the following theorem.

Theorem *Let $c > 0$ be fixed. Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{q^n}$ with $n \leq c \cdot \sqrt{\log(q)}$ can be solved in an expected time which is polynomially bounded in q.*

The theorem has the following corollary, and the corollary shows that a sequence of finite fields as claimed above exists.

Corollary *Let now positive real numbers $a < b$ be fixed. Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{q^n}$ with $a \cdot \sqrt{\log(q)} \leq n \leq b \cdot \sqrt{\log(q)}$ can be solved in an expected time of*

$$e^{\mathcal{O}(\log(q^n)^{2/3})} .$$

Indeed, the theorem implies that restricted to instances as in the corollary, the elliptic curve discrete logarithm problem can be solved in an expected time which is polynomially bounded in

$$q = e^{\log(q)} = e^{(\log(q))^{(1+1/2)\cdot 2/3}} \leq e^{(\frac{1}{a}\cdot n \log_2(q))^{2/3}} .$$

The underlying model of computation for these results can be chosen to be a randomized Turing machine or a randomized Random Access Machine. We note that all results in this work hold for all specified instances; the averaging only takes place on the running times for a *fixed input*, and there is *no* averaging over input classes.

The method: Index calculus

Just as the algorithms leading to subexponentiality results for the discrete logarithm problem in the multiplicative groups of finite fields and in degree 0 class groups of curves, the algorithm leading to the Theorem above is based on the so-called *index calculus method.* In the classical case of multiplicative groups of prime fields, the method can very briefly be described as follows:

Let a prime p and $a, b \in \mathbb{F}_p^*$, where a is a generating element, be given. The task is to compute the discrete logarithm (or index in the classical terminology) of b with respect to a, that is, the smallest number $x \in \mathbb{N}_0$ with $a^x = b$. For this, one first fixes a so-called *smoothness bound* $S \in \mathbb{N}$ and considers the set of all prime numbers $\leq S$; this set is called the *factor base.* Then one searches for *relations* between input elements and classes mod p of factor base elements. After one has obtained enough relations, one derives the discrete logarithm by linear algebra.

If one instead considers finite fields of a fixed characteristic, one substitutes prime numbers by irreducible polynomials whose degree is below a certain bound; if one considers degree 0 class groups of curves over a fixed finite field, one considers prime divisors whose degree is below a certain bound instead.

In the present work, the factor base is defined in an *algebraic* rather than an *arithmetic* way (that is, there is no smoothness bound). Relations are derived by solving systems of multivariate polynomial equations over $\mathbb{F}_q$.

On the proof

We give here a very brief overview of the algorithm leading to the Theorem above.

Let $E/\mathbb{F}_{q^n}$ be an elliptic curve. Then we compute a covering $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$ of degree 2 which satisfies $\varphi \circ [-1] = \varphi$ as well as a certain additional condition. The factor base is then given by

$$\{P \in E(\mathbb{F}_{q^n}) \mid \varphi(P) \in \mathbb{P}^1(\mathbb{F}_q)\} \ .$$

The relation generation relies on an algorithm which we call *decomposition algorithm.* Given an elliptic curve $E/\mathbb{F}_{q^n}$ the extension degree n, a covering φ as above and some point $P \in E(\mathbb{F}_{q^n})$, this algorithm either fails or outputs a tuple $(P_1, \ldots, P_n) \in E(\mathbb{F}_{q^n})^n$ with $\varphi(P_i) \in \mathbb{P}^1(\mathbb{F}_q)$ for $i = 1, \ldots, n$ such that

$$P_1 + \cdots + P_n = P \; . \tag{1}$$

The decomposition algorithm is based on solving multivariate systems of polynomial equations over $\mathbb{F}_q$. Of course it fails if there is no such tuple $(P_1, \ldots, P_n)$. But it also fails if the algebraic set defined by the associated multivariate system is not *zero-dimensional*. We remark here that the most difficult part of the proof is to show that for a uniformly distributed point $P \in E(\mathbb{F}_{q^n})$ with a sufficiently high probability the algebraic set defined by the associated multivariate system is indeed zero-dimensional and contains an $\mathbb{F}_q$-valued point which gives rise to a relation (1). In order to prove this result, we pass to higher-dimensional schemes over $\mathbb{F}_q$ by using Weil restrictions. The proof then relies crucially on intersection theory in products of projective lines.

Some historical comments

In Feb. 2004 I. Semaev put a preprint on the archive of the International Association for Cryptographic Research (IACR) in which he discussed the possibility of index calculus in the groups of rational points on elliptic curves over prime fields ([Sem04]). In his work, Semaev defined the factor base via an upper bound on the x-coordinates of points, where the elliptic curve is given by a Weierstraß model.

He also introduced so-called *summation polynomials*: Let E be an elliptic curve over a field K, given by a Weierstraß model, and let $m \in \mathbb{N}$, $m \geq 2$. Then the m-th summation polynomial as defined by Semaev is an irreducible polynomial $f \in K[x_1, \ldots, x_m]$ such that for the following holds: Given $P_1, \ldots, P_m \in E(\overline{K}) - \{O\}$, we have

$$f(x(P_1), \ldots, x(P_m)) = 0 \longleftrightarrow \exists \epsilon_1, \ldots, \epsilon_m \in \{1, -1\} \, : \, \epsilon_1 P_1 + \cdots + \epsilon_m P_m = O \, ,$$

where we identify $\mathbb{A}^1(\overline{K}) = \mathbb{P}^1(\overline{K}) - \{\infty\}$ with $\overline{K}$, the algebraic closure of K. These summation polynomials have degree 2^{m-2} in each variable.

Now, any algorithm to determine solutions with "small coordinates" for multivariate equations of high degree would give rise to an algorithm for relation generation. However, no efficient algorithm for this task is known (except for very special equations), and therefore, Semaev's approach does (currently) not lead to an algorithm which is faster than generic algorithms to solve discrete logarithm problems.

Semaev's work lead however both P. Gaudry and the author to reflect on the question whether a similar approach over extension fields might not give algorithms which asymptotically are faster than generic algorithms for certain input classes.

In [Gau09] Gaudry argues on a heuristic basis that for any fixed extension degree $n \geq 2$ and $q \longrightarrow \infty$, the elliptic curve discrete logarithm problem over fields $\mathbb{F}_{q^n}$ can be solved in an expected time of

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

on a randomized random access machine.[1] The author on the other hand tried if a common variation of n and q would lead to a sequence of finite fields such that the elliptic curve discrete logarithm problem over these fields would becomes subexponential, and this study finally lead to the present work.

We note that all previous results on classes of elliptic curves for which the discrete logarithm problem can be solved in subexponential expected time rely on a *transfer*: First a homomorphism from the group under consideration to another group is applied and then the problem is solved in the second group. For example, one can solve the discrete logarithm problem in the groups of rational points of supersingular elliptic curves in an expected time of

$$e^{\mathcal{O}((\log(q)\cdot\log(\log(q)))^{1/2})}$$

via a transfer to the multiplicative group of an extension of degree at most 6 of the ground field $\mathbb{F}_q$ (see [MOV93], [FR94] together with [EG02]).

This contrasts to the direct application of index calculus in the groups of rational points of elliptic curves in [Gau09] and the present work. We note that one might argue that we implicitly use the isomorphism $E(\mathbb{F}_{q^n}) \simeq \mathrm{Res}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(E)(\mathbb{F}_q)$, where $\mathrm{Res}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(E)$ is the Weil restriction of the elliptic curve $E/\mathbb{F}_{q^n}$ with respect to $\mathbb{F}_{q^n}|\mathbb{F}_q$. The important aspect is here nonetheless that *no computation* is performed in doing so. Weil restrictions are of crucial importance for the analysis of the algorithm, but the algorithm itself can be formulated without even mentioning Weil restrictions, and we do so.

An outline

Let us give an outline of the rest of this article:

In the next section, we give the algorithm for the Theorem above. For this we start off with an overview of the "decomposition algorithm", followed by the index calculus algorithm and finally the subalgorithm for the computation of a suitable covering φ. In Section 3 we give some background information on systems of multihomogeneous polynomials. In particular we discuss intersection theory in $(\mathbb{P}^1_k)^n$, k a field, and multigraded resultants,

[1] Using a suitable variant of Gaudry's algorithm and techniques of the present work, a proof of this result is given in [Die09].

including computational aspects. In the next section we introduce homogeneous summation polynomials via an abstract approach. Finally, the last section contains the analysis of the algorithm.

An interesting aspect about the algorithm and its analysis is that the algorithm can be stated with substantially less theoretical background than the analysis, and our exposition reflects this fact. In particular, as already mentioned, it is not necessary to speak about Weil restrictions when describing the algorithm, and consequently we only introduce Weil restrictions at the beginning of the analysis.

Notation and Terminology

The algebraic closure of a field k is denoted by $\overline{k}$. If R is a ring with an ideal I and $a \in R$, the residue class of a in R/I is denoted by $[a]_I$. If $I = (r)$, we also use the notation $[a]_r$.

If X and Y are two subschemes of a scheme Z, then we set $X \cap Y := X \times_Z Y$, the scheme theoretic intersection.

Let now X and Y be locally noetherian schemes. Then a finite and flat morphism $X \longrightarrow Y$ is also called a *flat covering.*

Products of projective planes play an important role in this work. We set $\mathbb{P}^1 := \mathrm{Proj}(\mathbb{Z}[X,Y])$ and $x := \frac{X}{Y}$. We identify $(\mathbb{P}^1)^n$ componentwise with $\mathrm{Proj}(\mathbb{Z}[X_1, Y_1]) \times \cdots \times \mathrm{Proj}(\mathbb{Z}[X_n, Y_n])$. Therefore we have bases $X_i, Y_i \in \Gamma((\mathbb{P}^1)^n, \mathcal{O}(0, \ldots, 0, 1, 0, \ldots, 0))$, where the 1 is at the i^{th} position. For any commutative ring A we have the multigraded homogeneous coordinate ring $A[X_1, Y_1, \ldots, X_n, Y_n]$ of $(\mathbb{P}^1_A)^n$. In the following by a *multihomogeneous* polynomial in $A[X_1, Y_1, \ldots, X_n, Y_n]$ we mean a polynomial which is homogeneous with respect to the multigrading. A *multihomogeneous* ideal in $A[X_1, Y_1, \ldots, X_n, Y_n]$ is then an ideal in $A[X_1, Y_1, \ldots, X_n, Y_n]$ which is generated by multihomogeneous polynomials. Now for some multihomogeneous ideal I, we denote the *subscheme* defined by I in $(\mathbb{P}^1_k)^n$ by $V(I)$. Moreover, we set $x_i := \frac{X_i}{Y_i}$ and $\mathbb{A}^n := \mathrm{Spec}(\mathbb{Z}[x_1, \ldots, x_n])$.

Additionally, we set $\mathbb{P}^2 := \mathrm{Proj}(\mathbb{Z}[X,Y,Z])$ and $x := \frac{X}{Z}$, $y := \frac{Y}{Z}$. The elliptic curve $E/\mathbb{F}_{q^n}$ under consideration is always given by a Weierstraß model in $\mathbb{P}^2_{\mathbb{F}_{q^n}}$.

Finally, let f be a partial function from $\mathbb{N}$ to $\mathbb{R}$ which is defined on an infinite subset S of $\mathbb{N}$ such that f is eventually positive. Then we define the usual classes $\mathcal{O}(f)$ and $\tilde{\mathcal{O}}(f)$ of functions $S \longrightarrow \mathbb{R}$. Additionally, we define the class of functions which are polynomially bounded in f as

$$\begin{aligned}&\mathcal{P}oly(f) := \\ &\{g : S \longrightarrow \mathbb{R} \ : \exists c > 0, N \in \mathbb{N} : |g(n)| \leq f(n)^c \text{ for all } n \in S \text{ with } n \geq N\} \ .\end{aligned}$$

We do not use the usual "Landau-style notation" $g = \mathcal{O}(f)$ etc. but $g \in \mathcal{O}(f)$ instead.

Sets $\mathcal{O}(f)$ etc. occur frequently in statements on (expected) running times. We then implicitly fix a (reasonable) representation of the mathematical objects in question (e.g. elliptic curves etc.) by bit-strings, as usual.

2 The key algorithms

In this section we outline the algorithm for the Theorem.

As mentioned in the introduction, the relation generation algorithm relies on a *decomposition algorithm.* Before we come to the algorithm for the Theorem, we give an overview over this algorithm.

2.1 The decomposition algorithm

The decomposition algorithm relies on "homogeneous summation polynomials". These polynomials can be obtained by homogenizing the summation polynomials introduced by Semaev in [Sem04] in an appropriate way. A more systematic point of view is however to regard Semaev's summation polynomials as being obtained by dehomogenization of the homogeneous summation polynomials. The homogeneous summation polynomials are studied in detail in Section 4; here we merely mention the key results which are needed to describe the decomposition algorithm.

In Section 4 we show the following two propositions.

Proposition 2.1 *Let E be an elliptic curve over a field k, and let us fix a covering $\varphi : E \longrightarrow \mathbb{P}^1_k$ of degree 2 with $\varphi \circ [-1] = \varphi$. Let $m \in \mathbb{N}$ with $m \geq 2$. Then there exists an up to multiplication by a non-trivial constant unique irreducible multihomogeneous polynomial $S_{\varphi,m} \in k[X_1, Y_1, X_2, Y_2, \ldots, X_m, Y_m]$ such that for all $P_1, \ldots, P_m \in E(\overline{k})$ we have $S_{\varphi,m}(\varphi(P_1), \ldots, \varphi(P_m)) = 0 \longleftrightarrow \exists \epsilon_1, \ldots, \epsilon_m \in \{1, -1\}$ such that $\epsilon_1 P_1 + \cdots \epsilon_m P_m = O$. The polynomial $S_{\varphi,m}$ has multidegree $(2^{m-2}, \ldots, 2^{m-2})$.*

Definition 2.2 We call a *multihomogeneous* polynomial $S_{\varphi,m}$ as in the proposition an m^{th} *summation polynomial of E with respect to φ.*

Proposition 2.3 *Given an elliptic curve in Weierstraß form over a finite field $\mathbb{F}_q$ $m \in \mathbb{N}$ with $m \geq 2$ and $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$ of degree 2 with $\varphi \circ [-1] = \varphi$, the m^{th} summation polynomial with respect to the covering $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$ can be computed with a randomized algorithm in an expected time of $\mathcal{P}oly(e^{m^2} \cdot \log(q))$.*

Now let $K|k$ be a finite field extension of degree n with basis $b_1, \ldots, b_n$, let E be an elliptic curve over K (rather than over k!), and let $\varphi : E \longrightarrow \mathbb{P}^1_K$ be a covering of degree 2 with $\varphi \circ [-1] = \varphi$.

Now let $P \in E(K)$. Let $S_{\varphi,n+1}(X_1, Y_1, \ldots, X_n, Y_n, \varphi(P))$ be a polynomial obtained by inserting the coordinates of $\varphi(P)$ for the variables X_{n+1}, Y_{n+1} in an $(n+1)^{\text{th}}$ summation polynomial of E with respect to φ; note that this polynomial is unique up to multiplication with a non-trivial constant.

Let $S^{(1)}, \ldots, S^{(n)} \in k[X_1, Y_1, \ldots, X_n, Y_n]$ be defined by

$$\sum_{j=1}^{n} b_j S^{(j)} = S_{\varphi,n+1}(X_1, Y_1, \ldots, X_n, Y_n, \varphi(P)) \ . \tag{2}$$

Clearly, if $S^{(j)}$ is non-zero, just as $S_{\varphi,n+1}$ it is multigraded of multidegree $(2^{n-1}, \ldots, 2^{n-1})$. Note also that a different basis of $K|k$ would give rise to a system of polynomials over k which generate the same k-vector space. The same holds if the summation polynomial is multiplied by a non-trivial constant or if the coordinates of $\varphi(P)$ are simultaneously multiplied by a non-trivial constant. In particular, the subscheme $V(S^{(1)}, \ldots, S^{(n)})$ of $(\mathbb{P}^1_k)^n$ does not depend on these choices.

For $Q_1, \ldots, Q_n \in \mathbb{P}^1(k)$, the following conditions are equivalent:

- There exist $P_1, \ldots, P_n \in E(\overline{K})$ such that $P_1 + \cdots + P_n = P$ and $x(P_i) = Q_i$ for all $i = 1, \ldots, n$.
- $S_{\varphi,n+1}(Q_1, \ldots, Q_n, \varphi(P)) = 0$.
- For all $j = 1, \ldots, n$, $S^{(j)}(Q_1, \ldots, Q_n) = 0$, that is, $(Q_1, \ldots, Q_n)$ is a k-rational point of $V(S^{(1)}, \ldots, S^{(n)})$.

By a "decomposition algorithm" we mean an algorithm for the following computational problem: Given a prime power q, $n \in \mathbb{N}$, an $\mathbb{F}_q$-basis $b_1, \ldots, b_n$ of $\mathbb{F}_{q^n}|\mathbb{F}_q$, an elliptic curve E over $\mathbb{F}_{q^n}$ (given by a Weierstraß model), $\varphi : E \longrightarrow \mathbb{P}^1_k$ as well as $P \in E(\mathbb{F}_{q^n})$, determine if the subscheme $V(S^{(1)}, \ldots, S^{(n)})$ of $(\mathbb{P}^1_{\mathbb{F}_q})^n$ defined by $S^{(1)}, \ldots, S^{(n)}$ is zero-dimensional, and if this is the case, determine all tuples $(P_1, \ldots, P_n) \in E(\mathbb{F}_{q^n})^n$ with $\varphi(P_i) \in \mathbb{P}^1(\mathbb{F}_q)$ for all $i = 1, \ldots, n$ and $P_1 + \cdots + P_n = P$.

In Section 3 we show the following proposition (see subsection 3.1 and Proposition 3.17 in subsection 3.3).

Proposition 2.4

a) Let k be a field, and let $F_1, \ldots, F_n \in k[X_1, Y_1, \ldots, X_n, Y_n]$ be multigraded polynomials of multidegree $(d, d, \ldots, d)$ for some $d \in \mathbb{N}$. If then

$V(F_1, \ldots, F_n)$ is zero-dimensional, its degree is $n! \cdot d^n$ (that is, the number of solutions over $\overline{k}$ "with multiplicities" is $n! \cdot d^n$).

b) Given a system of multihomogeneous polynomials $F_1, \ldots, F_n \in \mathbb{F}_q[X_1, Y_1, \ldots, X_n, Y_n]$ of multidegree $(d, d, \ldots, d)$ for some $d \in \mathbb{N}$ and prime power q, one can determine if the system defines a zero-dimensional scheme and if this is the case compute all solutions over $\mathbb{F}_q$ in an expected time of $\mathcal{P}oly(n! \cdot d^n \cdot \log(q))$.

Based on the previously mentioned computational results, we have the following decomposition algorithm.

We have already remarked that one can compute the polynomial $S_{\varphi,n+1}$ in an expected time of $\mathcal{P}oly(e^{n^2} \cdot \log(q))$. Thus one can also determine the polynomials $S^{(1)}, \ldots, S^{(n)}$ in an expected time of $\mathcal{P}oly(e^{n^2} \cdot \log(q))$. By the previous proposition one can then determine if the subscheme $V(S^{(1)}, \ldots, S^{(n)})$ of $(\mathbb{P}^1_{\mathbb{F}_q})^n$ is zero-dimensional and if this is the case compute all its $\mathbb{F}_q$-rational points in an expected time of $\mathcal{P}oly(n! \cdot 2^{n^2} \cdot \log(q)) = \mathcal{P}oly(e^{n^2} \cdot \log(q))$.

Assume now that the scheme is indeed zero-dimensional, and that all $\mathbb{F}_q$-rational points have been computed. We now want to find all tuples $(P_1, \ldots, P_n) \in E(\mathbb{F}_{q^n})^n$ with $\varphi(P_i) \in \mathbb{P}^1(\mathbb{F}_q)$ for all $i = 1, \ldots, n$ and $P_1 + \cdots + P_n = P$.

For this we iterate over all $\mathbb{F}_q$-rational points of $V(S^{(1)}, \ldots, S^{(n)})$. For each $(Q_1, \ldots, Q_n) \in V(S^{(1)}, \ldots, S^{(n)})(\mathbb{F}_q)$ we consider all possibles tuples $(P_1, \ldots, P_n) \in E(\mathbb{F}_{q^n})^n$ with $x(P_i) = Q_i$ for $i = 1, \ldots, n$ and check if $P_1 + \cdots + P_n = P$. We output all tuples $(P_1, \ldots, P_n)$ for which this is the case.

Now for each tuple $(P_1, \ldots, P_n) \in V(S^{(1)}, \ldots, S^{(n)})(\mathbb{F}_q)$ we need $\tilde{\mathcal{O}}(2^n) \cdot \mathcal{P}oly(\log(q))$ bit operations, and we have $\mathcal{P}oly(e^{n^2})$ such tuples $(P_1, \ldots, P_n)$. The expected total running time is then still in $\mathcal{P}oly(e^{n^2} \cdot \log(q))$.

We obtain:

Proposition 2.5 *Given q, $n \in \mathbb{N}$, E, φ and P as above, one can determine if the subscheme $V(S^{(1)}, \ldots, S^{(n)})$ of $(\mathbb{P}^1_{\mathbb{F}_q})^n$ is zero-dimensional, and if this is the case determine all tuples $(P_1, \ldots, P_n) \in E(\mathbb{F}_{q^n})^n$ with $\varphi(P_i) \in \mathbb{P}^1(\mathbb{F}_q)$ for $i = 1, \ldots, n$ in an expected time of $\mathcal{P}oly(e^{n^2} \cdot \log(q))$.*

Terminology 2.6 We say that "the decomposition algorithm succeeds" if applied to an instance as described above if the scheme $V(F_1, \ldots, F_n)$ is zero-dimensional and there exists a tuple $(P_1, \ldots, P_n) \in E(\mathbb{F}_{q^n})^n$ with $\varphi(P_i) \in \mathbb{P}^1(\mathbb{F}_q)$ and $P_1 + \cdots + P_n = P$. Otherwise we say that "the decomposition algorithm fails".

In order to analyze the index calculus algorithm we need a lower bound in the probability that the decomposition algorithm succeeds. Let us mention the key result for the analysis of the algorithm for the Theorem, which we prove in subsection 5.4 (Proposition 5.24):

Proposition 2.7 *Let $\epsilon > 0$. Then for n large enough*[2] *and $(2+\epsilon) \cdot n^2 \leq \log_2(q)$ the following holds: Let $E/\mathbb{F}_{q^n}$ be an elliptic curve, and let $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_{q^n}}$ be a covering of degree 2 with $\varphi \circ [-1] = \varphi$ such that the following condition holds:*

There exists a point $P \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ which is a ramification point of φ such that the points $P, \sigma(P), \ldots, \sigma^{n-1}(P)$ are all distinct and φ is not ramified at $\sigma(P), \ldots, \sigma^{n-1}(P)$.

Then the probability that the decomposition algorithm succeeds if applied to a uniformly randomly distributed element in $E(\mathbb{F}_{q^n})$ is $\geq q^{-\frac{1}{2}}$.

2.2 The index calculus algorithm

Below we give an algorithm which leads to the following result.

Proposition 2.8 *Let $\epsilon > 0$. Then there exists a randomized algorithm such that the following holds: Given a prime power q, a natural number n with $(2+\epsilon) \cdot n^2 \leq \log_2(q)$, an elliptic curve over $\mathbb{F}_{q^n}$ (in Weierstraß form) and two points $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$ as well as a system of elements $C_1, \ldots, C_u$ of $E(\mathbb{F}_{q^n})$ whose size is polynomially bounded in $\log(q^n)$, if the algorithm terminates, it outputs the discrete logarithm of B with respect to A. Moreover, if $C_1, \ldots, C_u$ is a generating system, the expected running time is polynomially bounded in q.*

Let us see how one can with this proposition obtain the Theorem.

First, Proposition 2.8 implies:

Proposition 2.9 *Let $\epsilon > 0$. Then there exists a randomized algorithm such that the following holds: Given a prime power q, a natural number n with $(2+\epsilon) \cdot n^2 \leq \log_2(q)$, an elliptic curve over $\mathbb{F}_{q^n}$ (in Weierstraß form) and two points $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$ as well as a system of elements $C_1, \ldots, C_u$ of $E(\mathbb{F}_{q^n})$ whose size is polynomially bounded in $\log(q^n)$, the algorithm outputs the discrete logarithm of B with respect to A or "failure". Moreover, the running time of the algorithm is polynomially bounded in q, and if $C_1, \ldots, C_u$ is a generating system, the probability of failure is $\leq \frac{1}{2}$.*

Proof. We choose some polynomial $P(x)$ such that for q^n large enough the expected running time in the previous proposition is $\leq P(\log(q^n))$. Then we terminate the previous algorithm if time $2P(\log(q^n))$ is reached. The result follows with Markov's bound. □

[2] As usual, by the phrase "for n large enough" we mean that there exists a constant $C > 0$ such that the statement holds for $n \geq C$.

Lemma 2.10 *Let E be an elliptic curve over $\mathbb{F}_q$, and let C_1, C_2 be two uniformly randomly distributed points from $E(\mathbb{F}_q)$. Then with a probability of $\Omega(\frac{1}{(\log\log(q))^2})$, C_1 and C_2 generate $E(\mathbb{F}_q)$.*

Proof. As the Tate modules have rank 1 or 2, there exist, by the elementary divisor theorem, two uniquely determined natural numbers a, b with $b|a$ and $E(\mathbb{F}_q) \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Let us fix such an isomorphism. Now C_i corresponds to $(m_{1,i}, m_{2,i}) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. With a probability of $\Omega(\frac{1}{\log\log(a)})$, $m_{1,1}$ is invertible (cf. [RS62]). This proves the statement if $b = 1$.

Let now $b > 1$. Then conditionally to a being invertible, $m_{2,2} - [m_{1,1}^{-1}]_b\, m_{2,1} m_{1,2}$ is still uniformly distributed and therefore invertible with a probability of $\Omega(\frac{1}{\log\log(b)})$. With a probability of $\Omega(\frac{1}{\log\log(a)\cdot\log\log(b)}) \subseteq \Omega(\frac{1}{(\log\log(q))^2})$ both conditions are satisfied, and then C_1, C_2 is a generating system. □

We do however not know how to efficiently test if two points from $E(\mathbb{F}_{q^n})$ do indeed form a generating system. As a work around, we proceed as follows:

```
Repeat
    1. Choose uniformly and independently randomly points $C_1, C_2 \in E(\mathbb{F}_{q^n})$.
    2. Apply an algorithm satisfying Proposition 2.9.
Until the discrete logarithm has been found.
```

Note that Step 1 can easily be performed in an expected time which is polynomial in $\log(q^n)$.

Like this, we obtain:

Proposition 2.11 *Let $\epsilon > 0$. Then there exists a randomized algorithm such that the following holds: Given a prime power q, a natural number n with $(2+\epsilon)\cdot n^2 \leq \log_2(q)$, an elliptic curve over $\mathbb{F}_{q^n}$ (in Weierstraß form) and two points $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$, the algorithm outputs the discrete logarithm of B in an expected time which is polynomially bounded in q.*

This implies:

Proposition 2.12 *Let $c > 0$. Then there exists a randomized algorithm such that the following holds: Given a prime power q, a natural number n with $n \leq c \cdot \sqrt{\log(q)}$, an elliptic curve over $\mathbb{F}_{q^n}$ (in Weierstraß form) and two points $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$, the algorithm outputs the discrete logarithm of B in an expected time which is polynomially bounded in q.*

Proof. Let $d := \lfloor 2c^2 \log(2) \rfloor + 1$. Then the instances satisfy $\frac{d}{c^2 \log(2)} n^2 \leq \log_2(q^d)$ with $\frac{d}{c^2 \log(2)} > 2$. Now given an instance as in the theorem, we apply an algorithm satisfying the previous proposition to the corresponding instance in the group $E(\mathbb{F}_{q^{dn}})$ and the extension degree n. The expected running time is then polynomially bounded in q^d and therefore also polynomially bounded in q. □

Note now that in Proposition 2.12 in particular the extension degree n is part of the input whereas in the Theorem this is not the case. To obtain the Theorem we apply an algorithm for Proposition 2.12 with all possible extension degrees "in parallel".

We are now coming to the algorithm for Proposition 2.8. For this we outline – as already mentioned – an index calculus algorithm, where the relation generation is based on the "decomposition algorithm" given in the previous subsection.

The algorithm

Input: A prime power q, a natural number n, an elliptic curve E over $\mathbb{F}_{q^n}$ in Weierstraß form, $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$, $C_1, \ldots, C_u \in E(\mathbb{F}_{q^n})$.

Output: The discrete logarithm of B with respect to A.

```
1. Compute $N \longleftarrow \#E(\mathbb{F}_{q^n})$.

2. Apply the procedure for generation of a factor base given below.
   Let $\mathcal{F} = \{F_1, P_2, \ldots, F_k\} \subseteq E(\mathbb{F}_{q^n})$ be the chosen enumerated factor base.

3. Construct matrices $R \in (\mathbb{Z}/N\mathbb{Z})^{(k+u+1)\times k}$ and $S \in (\mathbb{Z}/N\mathbb{Z})^{(k+u+1)\times u}$ as well as vectors $\underline{\alpha}, \underline{\beta} \in (\mathbb{Z}/N\mathbb{Z})^{k+u+1}$ as follows:
   For $i = 1, \ldots, k+u+1$ do
       Repeat
           Choose uniformly and independently randomly $\alpha, \beta, s_1, \ldots, s_u \in \mathbb{Z}/N\mathbb{Z}$ and apply the decomposition algorithm to $\sum_j s_j C_j + \alpha A + \beta B$.
       Until this leads to a relation.
       Let
           $$\sum_j r_{i,j} F_j = \sum_j s_{i,j} C_j + \alpha_i A + \beta_i B$$
       be the relation generated.

4. Compute a lower row echelon form $H$ of $(R|S)$ (over $\mathbb{Z}/N\mathbb{Z}$); apply the row transformations also to $\underline{\alpha}, \underline{\beta}$; let $\underline{\alpha}', \underline{\beta}'$ be the resulting vectors.
```

5. If $\beta_1' \in (\mathbb{Z}/N\mathbb{Z})^*$, let $\xi := -\frac{\alpha_1'}{\beta_1'}$, otherwise go back to Step 3.

6. Compute the factorization of N.

7. Compute $\mathrm{ord}(a)$, using the factorization of N.

8. Output the unique non-negative number $x \in \{0, \ldots, \mathrm{ord}(a) - 1\}$ with $[x]_{\mathrm{ord}(a)} = [\xi]_{\mathrm{ord}(a)} \in \mathbb{Z}/\mathrm{ord}(a)\mathbb{Z}$.

For the *correctness* of the algorithm note that as $(R|S)$ is a $(k+u+1) \times (k+u)$-matrix, the first row of H is trivial. Therefore we have the relation $\alpha_1'A + \beta_1'B = 0$.

We now give some additional information on subroutines for the various steps of the algorithm and their complexity.

Step 1 can be performed in polynomial time with Schoof's algorithm ([Sch85]).

Step 6 can be performed in an expected time of time of $\mathcal{P}oly(e^{(\log(N)\cdot\log(\log(N)))^{1/2}})$, for example with the algorithm by Lenstra and Pomerance ([LP92]).

Step 7 can be performed in polynomial time along the following lines:

As in the algorithm, let $N = \prod_{i=1}^{v} \ell_i^{e_i}$ with $e_i \in \mathbb{N}$ and pairwise distinct prime numbers ℓ_i. Now let $L_i := \frac{N}{\ell_i^{e_i}}$, and let $o_i := \min\{j \in 0, \ldots, e_i \mid \ell_i^j L_i \cdot a = 0\}$ for $i = 1, \ldots, v$. Then $\prod_{i=1}^{v} \ell_i^{o_i}$ is the order of a.

We now discuss the crucial steps 2,3, 4 and 5.

Step 2 – Construction of the factor base

We have already mentioned that the factor base is a set

$$\{P \in E(\mathbb{F}_{q^n}) \mid \varphi(P) \in \mathbb{P}^1(\mathbb{F}_q)\}$$

for a suitable covering of degree 2 $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_{q^n}}$ with $\varphi \circ [-1] = \varphi$.

Let σ be the relative Frobenius automorphism of $\overline{\mathbb{F}}_q|\mathbb{F}_q$. Now the condition on φ we impose is the following condition, already mentioned in Proposition 2.7.

Condition 2.13 There exists a point $P \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ which is a ramification point of φ such that the points $P, \sigma(P), \ldots, \sigma^{n-1}(P)$ are all distinct and φ is not ramified at $\sigma(P), \ldots, \sigma^{n-1}(P)$.

This condition might seem strange for the moment. The reasons for this condition will be discussed in subsection 5.2. Very briefly, the factor base is in a certain sense defined by a 1-dimensional $\mathbb{F}_q$-scheme, and the condition ensures that this scheme is birational to a curve over $\mathbb{F}_q$.

In the next subsection we prove:

Proposition 2.14 *Given a prime power q, $n \in \mathbb{N}$ and an elliptic curve over $\mathbb{F}_{q^n}$ in Weierstraß form such that $(q, n) \neq (3, 2)$ one can compute a covering $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_{q^n}}$ of degree 2 with $\varphi \circ [-1] = \varphi$ satisfying Condition 2.13 in an expected time of $\mathcal{P}oly(n \cdot \log(q))$.*

The factor base clearly has $\leq 2(q+1)$ elements and can therefore clearly be constructed in an expected time which is polynomially bounded in $n \cdot \log(q) + q$.

Step 3 – Relation generation

As stated, we choose $\alpha, \beta, s_1, \ldots, s_u \in \{0, \ldots, \#E(\mathbb{F}_{q^n}) - 1\}$ uniformly at random and compute $\sum_j s_j C_j + \alpha A + \beta B$. Then we apply the decomposition algorithm as described in the previous subsection to this element and the covering φ. If the procedure does not fail, we have obtained at least one relation between factor base elements, $C_1, \ldots, C_u$ and the input elements A, B; we store such a relation. (It does not matter which one we store as long as the distribution of the output only depends on the element $\sum_j s_j C_j + \alpha A + \beta B$ (and not on the further internal state of the algorithm).) We repeat this procedure until we have obtained such a relation.

Let us assume that u is polynomially bounded in $\log(q^n)$ and $C_1, \ldots, C_u$ is a generating system. Then the time to compute $\sum_j s_j C_j + \alpha A + \beta B$ is polynomial in $\log(q^n)$. By Proposition 2.5, the expected running time of one iteration in the Repeat-loop is then in $\mathcal{P}oly(e^{n^2} \cdot \log(q))$. Note that for each iteration of the Repeat-loop the element $\sum_j s_j C_j + \alpha A + \beta B$ is uniformly randomly distributed (and independent of previous choices). Therefore by Proposition 2.7 (Proposition 5.24) for instances with $(2 + \epsilon) \cdot n^2 \leq \log_2(q)$ and n large enough the expected number of iterations in the Repeat-loop is in $\mathcal{O}(q^{1/2})$.

We conclude that for instances with $(2 + \epsilon) \cdot n^2 \leq \log_2(q)$ and n large enough and for u polynomially bounded in $\log(q^n)$ such that $C_1, \ldots, C_u$ is a generating system, the expected running time of Step 3 is in $\mathcal{P}oly(e^{n^2} \cdot \log(q)) \cdot \mathcal{O}(q^{1/2}) \cdot \mathcal{O}(q) \subseteq \mathcal{P}oly(q)$.

Step 4 – Linear algebra

The computation of a lower row echelon form can be performed with an easy modification of the usual Gaußian reduction algorithm with gcd computations. Given a matrix of size $m \times n$ over $\mathbb{Z}/N\mathbb{Z}$, the computation can be performed in a time which is polynomially bounded in $m \cdot n \cdot \log(N)$.

By the definition of the factor base, we have $k + u \in \mathcal{O}(q)$. We therefore have a running time which is polynomially bounded in $q \cdot \log(N)$.

Step 5 – Invertibility

We need to estimate the probability that β_1' is invertible. The key result is:

Proposition 2.15 *The random element β_1' is uniformly randomly distributed in $\mathbb{Z}/N\mathbb{Z}$.*

For $N \longrightarrow \infty$, we have $\frac{\varphi(N)}{N} \in \Omega(\frac{1}{\log\log(N)})$ (cf. [RS62, Formula 3.41]). Therefore, the expected number of iterations of steps 3,4,5 is in $\mathcal{O}(\log\log(N)) = \mathcal{O}(\log\log(q))$.

Proof of Proposition 2.15. For each i, β_i is stochastically independent of $\alpha_i A + \beta_i B$. Therefore β_i is stochastically independent of the i^{th} row of $(R|S)$. It follows that $\underline{\beta}$ is independent of $(R|S)$. Let U be the transformation matrix such that $H = U(R|S)$; this is also a random variable. Now U is stochastically independent of $\underline{\beta}$. Let $\underline{u}$ be the first row of U and note that $[\underline{u}]_\ell \neq 0$ for all prime divisors ℓ of N. Then $\beta_1' = \underline{u}\underline{\beta}$. Now the statement follows with the following well known lemma. □

Lemma 2.16 *Let N be a natural number, and let $\underline{u} \in (\mathbb{Z}/N\mathbb{Z})^m$ with $[\underline{u}]_\ell \neq \underline{0}$ for all prime divisors ℓ of N. Furthermore, let $\underline{v}$ be a uniformly distributed random element in $(\mathbb{Z}/N\mathbb{Z})^m$. Then $\sum_i u_i v_i$ is uniformly distributed in $\mathbb{Z}/N\mathbb{Z}$.*

Proof. Let us first consider the case that N is a prime power. Then at least one entry of $\underline{u}$ is invertible. This implies the statement. The general case follows then easily with the Chinese Remainder Theorem. □

The overall running time

Altogether we conclude:

We again restrict ourselves to instances with $(2 + \epsilon) \cdot n^2 \leq \log_2(q)$ and u polynomially bounded in $\log(q^n)$ such that $C_1, \ldots, C_u$ is a generating system. As the factor base has a size of $\mathcal{O}(q)$, it is now clear that for

n large enough the expected running time of the whole algorithm is then polynomially bounded in q.

We have proven the following statement:

Let $\epsilon > 0$. Then given a prime power q, a *large enough* natural number n with $(2+\epsilon)\cdot 2^n \leq \log_2(q)$, an elliptic curve over $\mathbb{F}_{q^n}$ (in Weierstraß form) and two points $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$ as well as a generating system of $E(\mathbb{F}_{q^n})$ whose size is polynomially bounded in $\log(q^n)$, the algorithm outputs the discrete logarithm of B with respect to A. Moreover, the expected running time is then polynomially bounded in q.

Proposition 2.8 can then be obtained by applying this algorithm "in parallel" with a brute force computation.

2.3 Computing a suitable covering

We discuss how a covering $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_{q^n}}$ as required in the construction of the factor base can be computed efficiently.

We make some case distinctions. In each case we start off with a specific Weierstraß model and determine some automorphism α of $\mathbb{P}^1_{\mathbb{F}_{q^n}}$. Then we set $\varphi := \alpha \circ x_{|E}$.

2.3.1 Even characteristic

Let first $j(E) = 0$. Then E by an easy coordinate change the "affine part" of E is defined by a polynomial

$$y^2 + a_3 y + x^3 + a_4 x + a_6 \ .$$

(see [Sil86, Appendix A]) (with $a_3 \neq 0$). Now $x_{|E}$ is ramified exactly over ∞. We set $\alpha := \frac{ax-1}{x}$ for some $a \in \mathbb{F}_{q^n}$ which is not contained in any proper subfield of $\mathbb{F}_{q^n}|\mathbb{F}_q$.[3] Then α maps ∞ to a, and thus φ is ramified exactly at a. Clearly the condition is satisfied.

Let now $j(E) \neq 0$. Then wlog. E the "affine part" of E is defined by the polynomial

$$y^2 + xy + x^3 + a_2 x^2 + a_6 \ .$$

Then $x_{|E}$ is ramified exactly over 0 and ∞. We set $\alpha := x + a$ with a as above. Then φ is ramified at a and ∞, and again the condition is satisfied.

[3] By a "proper subfield" we mean here a subfield of a field extension $K|k$ which is not equal to K.

2.3.2 Odd characteristic

Now wlog. E is defined by

$$y^2 - f(x) \, ,$$

where $f(x) \in \mathbb{F}_q[x]$ is monic of degree 3. The conditions which have to be satisfied are now more subtle but the algorithm is very simple:

We choose $\lambda \in \mathbb{F}_{q^n}$ uniformly at random and with $\alpha := x - \lambda$ we check if the condition is satisfied. We repeat this until the condition is satisfied.

Note here that if $f(x) = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$ (with $\lambda_i \in \mathbb{F}_{q^{6n}}$), then the ramification points of $\varphi = \alpha \circ x_{|E}$ in $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ are $\lambda_i - \lambda$ for $i = 1, 2, 3$. So it is easy to check the condition.

Proposition 2.14 now follows from the following lemma. (Note that we only apply the lemma in the case that q is odd.)

Lemma 2.17 *There exists a constant $C \in (0, 1)$ such that the following holds:*

Let q be a prime power and n a natural number such that $(q, n) \neq \{(2, 2), (3, 2), (2, 3), (2, 4)\}$. Now let $\lambda_1, \lambda_2, \lambda_3 \in \overline{\mathbb{F}}_q$, and let λ be a uniformly distributed element in $\mathbb{F}_{q^n}$. Then with a probability $\geq C$ we have

$$(\lambda_1 - \lambda)^{q^i} \notin \{\lambda_1 - \lambda, \lambda_2 - \lambda, \lambda_3 - \lambda\}$$

for $i = 1, \ldots, n - 1$.

Proof. Let $\ell = 1, 2, 3$. We have $(\lambda_1 - \lambda)^{q^i} = \lambda_\ell - \lambda$ if and only if $\lambda^{q^i} - \lambda = \lambda_1^{q^i} - \lambda_\ell$. The map $\lambda \mapsto \lambda^{q^i} - \lambda$ is an $\mathbb{F}_q$-linear map with kernel $\mathbb{F}_{q^{\gcd(i,n)}}$. There are thus either no or $q^{\gcd(i,n)}$ such λ.

We obtain: In total there are at most $3 \sum_{i=1}^{n-1} q^{\gcd(i,n)}$ elements λ for which the condition in the lemma is not satisfied.

Now $3 \sum_{i=1}^{n-1} q^{\gcd(i,n)} \leq 3(n - 1) \cdot q^{n/2}$, and therefore the probability in question is

$$\geq 1 - \frac{3(n - 1)}{q^{n/2}} \geq 1 - \frac{3(n - 1)}{2^{n/2}} \, .$$

For $n \geq 10$ this is $\geq \frac{5}{32} > 0$.

One also easily sees that for $n \leq 9$ and $(q, n) \neq \{(2, 2), (3, 2), (2, 3), (2, 4)\}$ the probability is positive. □

3 Some results on multihomogeneous polynomials

In this section we are concerned with results related to multihomogeneous polynomials and systems of such polynomials. In particular, we give some information on aspects of intersection theory in the special case of $(\mathbb{P}^1_k)^n$

(k a field), including multigraded resultants, and we discuss computational aspects.

3.1 Intersection theory in $(\mathbb{P}^1_k)^n$

In this subsection we review some standard material on intersection theory in the special case of $(\mathbb{P}^1_k)^n$, where k is a field.

Lemma 3.1 *Let X be a closed subscheme of $(\mathbb{P}^1_k)^n$ of dimension at least 1, and let $F \in k[X_1, Y_1, \ldots, X_n, Y_n]$ be a multihomogeneous polynomial whose multidegree is componentwise positive. Then $V(F)$ and X intersect non-trivially.*

Proof. Let $\underline{d}$ be the multidegree of F. The invertible sheaf $\mathcal{O}(\underline{d})$ is very ample, and under the corresponding embedding into projective space F corresponds to a non-trivial linear form. The result thus follows from intersection theory in projective space. □

Definition 3.2 We define the dimension of the empty scheme as -1.

Lemma 3.3 *Let $k \leq n + 1$. Let $F_1, \ldots, F_k$ be multihomogeneous polynomials in $k[X_1, Y_1, \ldots, X_n, Y_n]$ such that all multidegrees are componentwise positive. Then $\dim(V(F_1, \ldots, F_k)) \geq n - k$. Moreover, we have equality if and only if for $\ell = 2, \ldots, k$ no irreducibility component of $V(F_1, \ldots, F_{\ell-1})$ is contained in $V(F_\ell)$.*

Proof. Let first $k \leq n$ (such that the first statement is non-trivial). Then by the previous lemma $V(F_1, \ldots, F_k)$ is non-empty. The first statement thus follows with Krull's Hauptidealsatz. The second statement also follows easily with the previous lemma and Krull's Hauptidealsatz. □

Notation 3.4 Let V be a fixed quasi-projective variety, and let X be a closed subscheme of V. Then we denote the class of V in the Chow ring of V by $[X]$. (We do not fix a notation for the cycle corresponding to a closed subscheme as we never perform operations with cycles but only with classes.)

Remark 3.5 Let X be a closed subscheme of $(\mathbb{P}^1_k)^n$ and let $F \in k[X_1, Y_1, \ldots, X_n, Y_n]$ be a multihomogeneous polynomial such that no irreducibility component of X is contained in $V(F)$. Then

$$[X \cap V(F)] = [X] \cdot [V(F)] ,$$

where $X \cap V(F)$ is the scheme-theoretic intersection. Indeed, this is a special case of Axiom A7 on intersection theory in [Har77, Appendix A]. In particular, if $F_1, \ldots, F_k$ are multihomogeneous polynomials such that for all $\ell = 2, \ldots, k$ no irreducibility component of $V(F_1, \ldots, F_{\ell-1})$ is contained in $V(F_\ell)$, then

$$[V(F_1, \ldots, F_k)] = [V(F_1)] \cdots [V(F_k)] \ .$$

Note that by the previous lemma this is in particular the case if the multidegrees of the polynomials are componentwise positive and $\dim(V(F_1, \ldots, F_k)) = n - k$.

We have the following explicit description of the Chow ring of $(\mathbb{P}^1_k)^n$:

Proposition 3.6 *Let h_i be the class of $V(X_i) \subseteq (\mathbb{P}^1_k)^n$ for $i = 1, \ldots, n$. Then the Chow ring of $(\mathbb{P}^1_k)^n$ is generated by $h_1, \ldots, h_n$, and we have an isomorphism $\mathbb{Z}[H_1, \ldots, H_n]/(H_1^2, \ldots, H_n^2) \longrightarrow \mathrm{CH}((\mathbb{P}^1_k)^n)$, $[H_i] \mapsto h_i$.*

This proposition can easily be derived from a general result on the Chow rings of toric varieties (cf. the proposition on page 106 of [Ful93, Section 5.2]). We remark here that the book [Ful93] is concerned with toric varieties over the complex number. However, analytic arguments play a minor role in the exposition, and the few such arguments can rather easily be replaced with algebraic arguments. In particular, the proposition just mentioned holds over arbitrary fields.

Example 3.7 The class of an effective Cartier divisor on $(\mathbb{P}^1_k)^n$ of multidegree $(d_1, \ldots, d_n)$ is $d_1 h_1 + \cdots + d_n h_n$.

Let us consider the pull-back and push-forward homomorphisms associated with the canonical projections between products of $\mathbb{P}^1_k$'s. The following considerations follow immediately from the axioms of intersection theory in [Har77, Appendix A].

Let for $n_1 > n_2$ $p : (\mathbb{P}^1_k)^{n_1} \longrightarrow (\mathbb{P}^1_k)^{n_2}$ be the projection to the first n_2 components. Let us denote by h_i for $i = 1, \ldots, n_2$ the class of $V(X_i)$ in any of the two Chow rings.

Then the pull-back $p^* : \mathrm{CH}((\mathbb{P}^1_k)^{n_2}) \longrightarrow \mathrm{CH}(\mathbb{P}^1_k)^{n_1})$, which is a ring homomorphism, is given by the homomorphism which corresponds to the obvious inclusion under the isomorphism in Proposition 3.6. This means that it is given by $p^*(h_i) = h_i$.

The push-forward, which is a group homomorphism, is given as follows:

Lemma 3.8 *Let $\underline{e} \in \{0, 1\}^{n_1}$. Then $p_*(h_1^{e_1} \cdots h_{n_1}^{e_{n_1}}) = 1$ if $e_{n_2+1} = \cdots = e_{n_1} = 1$ and $p_*(h_1^{e_1} \cdots h_{n_1}^{e_{n_1}}) = 0$ otherwise.*

Let now $F_1, \ldots, F_n$ be multihomogeneous polynomials whose multidegree is componentwise positive. Let the multidegree of F_i be $(d_{i,1}, \ldots, d_{i,n})$, and let $D := ((d_{i,j}))_{i,j}$. If now the scheme $V(F_1, \dots, F_n)$ is zero-dimensional we conclude with Proposition 3.6 and Remark 3.5 that the class of $V(F_1, \dots, F_n)$ in the Chow group has degree $\mathrm{Perm}(D)$, the permanent of D. With other words: If the scheme $V(F_1, \dots, F_n)$ is zero-dimensional, it has degree $\mathrm{Perm}(D)$. In particular, if additionally the multidegree of each F_i is $(d, \dots, d)$ for a common $d \in \mathbb{N}$, then the degree of $V(F_1, \dots, F_n)$ is $n! \cdot d^n$.

3.2 Multigraded resultants

We will make repeated use of resultants for systems of multihomogeneous polynomials in $k[X_1, Y_1, \dots, X_n, Y_n]$. Let us recall the definition and basic properties:

Let us fix some $n \in \mathbb{N}$. Let for $\underline{d} \in \mathbb{N}$ $M_{\underline{d}}$ be the set of monomials of multidegree $\underline{d}$ in $k[X_1, Y_1, \dots, X_n, Y_n]$.

Let for each $i = 1, \dots, n+1$ some $\underline{d}^{(i)} \in \mathbb{N}^n$ be given. (Note that all coefficients are positive). We want to define the generic resultant for multihomogeneous polynomials of multidegrees $\underline{d}^{(1)}, \dots, \underline{d}^{(n+1)}$. For this we consider a "universal coefficient ring", which is a multivariate polynomial ring over the integers which for each pair (i, m) with $m \in M_{\underline{d}^{(i)}}$ has one indeterminate $c_{i,m}$, that is, it is the ring $\mathbb{Z}[\{c_{i,m}\}_{i=1,\dots,n+1, m \in M_{\underline{d}^{(i)}}}]$. We define the *generic system of* $n+1$ *multihomogeneous polynomials with multidegrees* $\underline{d}^{(1)}, \dots, \underline{d}^{(n+1)}$ as $G_1, \dots, G_{n+1} \in \mathbb{Z}[\{c_{(i,m)}\}_{i,m}][X_1, Y_1, \dots, X_n, Y_n]$ with $G_i = \sum_{m \in M_{\underline{d}^{(i)}}} c_{i,m}\, m$.

The generic resultant under consideration is then an element of $\mathbb{Z}[\{c_{i,m}\}_{i,m}]$, and the resultant of a particular system of multihomogeneous polynomials is obtained by substituting the coefficients of the polynomials for the generic coefficients.

Proposition 3.9

a) There is an irreducible polynomial $\mathrm{Res} \in \mathbb{Z}[\{c_{i,m}\}_{i=1,\dots,n+1, m \in M_{\underline{d}^{(i)}}}]$ *which for* $i = 1, \dots, n+1$ *is homogeneous in the coefficients of the* i^{th} *generic polynomial and which has the following property: For all fields* k *and all systems of multihomogeneous polynomials* $F_1, \dots, F_{n+1} \in k[X_1, Y_1, \dots, X_n, Y_n]$, *where* F_i *has multidegree* $\underline{d}^{(i)}$, *we have* $\mathrm{Res}(F_1, \dots, F_{n+1}) = 0$ *if and only if* $V(F_1, \dots, F_{n+1})$ *is non-empty. Here* $\mathrm{Res}(F_1, \dots, F_{n+1})$ *is obtained by substituting the coefficients of the polynomials for the generic coefficients.*

b) The polynomial Res *with the above properties unique up to sign.*

c) For every field k, *the induced polynomial in* $k[\{c_{i,m}\}_{i,m}]$ *is irreducible.*

d) For each $i = 1, \ldots, n+1$, Res *has degree* $\mathrm{Perm}(D_i)$ *in the coefficients of the i^{th} generic polynomial, where D_i is obtained from the matrix* $\begin{pmatrix} \underline{d}^{(1)} \\ \vdots \\ \underline{d}^{(n+1)} \end{pmatrix}$ *by deleting the i^{th} row.*

Sketch of a proof. A corresponding result over the complex numbers follows from the general results in [GKZ94]. (The polynomial Res is then unique up to multiplication by a non-trivial complex number.) Even though there are various other works on general resultants, we could not find this "universal" result in the literature. We explain now how it can be derived from the results on "mixed resultants" in [GKZ94, Section 3.3].

For every commutative ring R, the set $\mathrm{Spec}(\mathbb{Z}[\{c_{i,m}\}_{i,m}])(R) \simeq \prod_{i,m} R$ corresponds in an obvious way to the set of systems $F_1, \ldots, F_{n+1} \in R[X_1, Y_1, \ldots, X_n, Y_n]$, where F_i has multidegree $\underline{d}^{(i)}$. For such a system of polynomials over a field such that at least one polynomial is non-trivial, we denote by $\overline{(F_1, \ldots, F_{n+1})}$ the class of the coefficient vectors in projective space $\mathrm{Proj}(\mathbb{Z}[\{c_{i,m}\}_{i,m}])(R)$.

Let $p : (\mathbb{P}^1)^n \times_{\mathbb{Z}} \mathrm{Proj}(\mathbb{Z}[\{c_{i,m}\}_{i,m}]) \longrightarrow \mathrm{Proj}(\mathbb{Z}[\{c_{i,m}\}_{i,m}])$ be the projection to the second component. Let $V(G_1, \ldots, G_{n+1})$ be the closed subscheme of $(\mathbb{P}^1)^n \times_{\mathbb{Z}} \mathrm{Proj}(\mathbb{Z}[\{c_{i,m}\}_{i,m}])$ defined by the generic multihomogeneous polynomials $G_1, \ldots, G_{n+1}$ introduced above.

We consider $p(V(G_1, \ldots, G_{n+1}))$, which is a closed subscheme of $\mathrm{Proj}(\mathbb{Z}[\{c_{i,m}\}_{i,m}])$, with the induced reduced structure. Note that for a system $F_1, \ldots, F_{n+1}$ of polynomials as above over a field k, the fiber of $V(G_1, \ldots, G_{n+1})$ above $\overline{(F_1, \ldots, F_{n+1})}$ is $V(F_1, \ldots, F_{n+1})$, and thus the fiber of $p(V(G_1, \ldots, G_{n+1}))$ at $\overline{(F_1, \ldots, F_{n+1})}$ is set-theoretically equal to $p_k(V(F_1, \ldots, F_{n+1}))$. In particular, $\overline{(F_1, \ldots, F_{n+1})}$ is contained in $p_k(V(G_1, \ldots, G_{n+1})_k)$ if and only if $V(F_1, \ldots, F_{n+1})$ is non-empty.

Now the results in [GKZ94, subsection 3.3 A] immediately generalize to arbitrary fields, and therefore $V(G_1, \ldots, G_{n+1}))_{\overline{\mathbb{Q}}}$ as well as $V(G_1, \ldots, G_{n+1}))_{\overline{\mathbb{F}}_p}$ for every prime number p are irreducible of codimension 1. It follows that $V(G_1, \ldots, G_{n+1})$ is irreducible of codimension 1. As $\mathrm{Proj}(\mathbb{Z}[\{c_{i,m}\}_{i,m}])$ is regular, this implies that it is a Cartier divisor and thus given by a section of an invertible sheaf on $\mathrm{Proj}(\mathbb{Z}[\{c_{i,m}\}])$. But every invertible sheaf on a projective space over $\mathbb{Z}$ is isomorphic to $\mathcal{O}(a)$ for some $a \in \mathbb{N}$ (cf. [Mum65, §0, 5 b)]). Therefore $V(G_1, \ldots, G_{n+1})$ is defined by a homogeneous polynomial in $\mathbb{Z}[\{c_{i,m}\}_{i,m}]$; let Res be such a polynomial.

We already know that Res is irreducible. Moreover, for every prime number p, the residue class $[\mathrm{Res}]_{\mathbb{F}_p[\{c_{i,m}\}_{i,m}]}$ is non-trivial, and thus the gcd of the coefficients of Res is 1. It is immediate that Res is homogeneous in the coefficients of each generic polynomial.

We have established a) and b). Result d) follows from [GKZ94, Proposition 3.3] and the remarks at the end of the previous subsection.

It remains to prove c). So let k be a field. Let Res_k be the induced polynomial obtained from Res. Then Res_k defines (scheme-theoretically) the fiber $p(V(G_1, \ldots, G_{n+1}))_k$. The associated reduced subscheme is the image $p_k(V(G_1, \ldots, G_{n+1})_k)$ with the reduced structure, which is irreducible. Therefore Res_k is the product of a constant and a power of an irreducible polynomial. Now first, by d), Res_k is a polynomial of degree $\sum_i \mathrm{Perm}(D_i)$. Also, by applying the reasoning in [GKZ94] for k instead of $\mathbb{C}$, one obtains that $p_k(V(G_1, \ldots, G_{n+1})_k)$ with the reduced structure also has degree $\sum_i \mathrm{Perm}(D_i)$. As we already know that set-theoretically $p_k(V(G_1, \ldots, G_{n+1})_k)$ is defined by Res_k, we know now that this is also true scheme-theoretically. We conclude that Res_k is irreducible. □

We call the polynomial Res a *generic mixed multigraded resultant*. If the multidegrees of the generic polynomials are equal, we speak of a *multigraded resultant*. For some commutative ring R and multihomogeneous $F_1, \ldots, F_{n+1} \in R[X_1, Y_1, \ldots, X_n, Y_n]$ we call $\mathrm{Res}(F_1, \ldots, F_{n+1})$ (where Res is the generic mixed multihomogeneous resultant for polynomials of appropriate multidegree) the *multigraded resultant* of $F_1, \ldots, F_{n+1}$.

3.3 Computing resultants and solving systems

In this subsection we address computational problems related to multigraded resultants and the solution of zero-dimensional multihomogeneous polynomial systems. In particular, we give an algorithm to determine all solutions of a multihomogeneous polynomial system $F_1, \ldots, F_n$ over a finite field, where each F_i has multidegree $(d, d, \ldots, d)$ for some $d \in \mathbb{N}$ and the scheme $V(F_1, \ldots, F_n)$ is zero-dimensional. Our algorithm heavily relies on the computation of resultants. We have not explicitly found our approach in the literature, but the idea to use appropriate resultants to solve systems of multivariate polynomial equations is of course well known (see for example [CLO05] for an introduction).

In the following, all structural statements are made for systems over an arbitrary field k. Computational statements are then for systems over finite fields, and the cardinality of the ground field is then always q.

Let $F_1, \ldots, F_{n+1} \in k[X_1, Y_1, \ldots, X_n, Y_n]$ be non-constant multihomogeneous polynomials of equal multidegree $(d, d, \ldots, d)$ for some $d \in \mathbb{N}$, and let $\mathrm{Res}(F_1, \ldots, F_{n+1})$ be the multigraded resultant of these polynomials. Now just as the usual Sylvester resultant, this resultant can be expressed as the determinant of a matrix each of whose entries is 0 or a coefficient of one of the polynomials F_i.

Let us to state this result fix the following definition.

Definition 3.10 Let M be a multigraded $k[X_1, Y_1, \ldots, X_n, Y_n]$-module, and let $\underline{d} \in \mathbb{Z}^n$. Then the k-vector subspace of M consisting of elements of multidegree $\underline{d}$ is denoted by $M_{\underline{d}}$.

We now consider the linear map

$$\begin{aligned}\Phi \ : \ (k[X_1, Y_1, \ldots, X_n, Y_n]_{(d-1, 2d-1, \ldots, nd-1)})^{n+1} \longrightarrow \\ k[X_1, Y_1, \ldots, X_n, Y_n]_{(2d-1, 3d-1, \ldots, (n+1)d-1)} \ , \\ (A_1, \ldots, A_{n+1}) \mapsto \textstyle\sum_{i=1}^{n+1} F_i A_i \ .\end{aligned} \qquad (3)$$

Note that both the domain as well as the codomain have dimension $(n+1)! \cdot d^n$.

Proposition 3.11 *Let M be the matrix of Φ with respect to the monomial bases in the domain and the codomain with any ordering. Then*

$$\mathrm{Res}(F_1, \ldots, F_{n+1}) = \pm \det(M) \ .$$

Note here that the resultant is only defined up to a sign, and a change of the ordering of any of the two the bases changes a sign too.

This result is essentially proven in [SZ94]. (Note the important reference to the proof of [KSZ92, Theorem 4.7] in the proof of [SZ94, Proposition 6].) Note first that one only has to show the formula for the generic resultant. Now in [SZ94] (and [KSZ92]) it is proven that the formula holds in characteristic 0 up to a multiplicative rational constant. It therefore also holds for the generic resultant up to a multiplicative rational constant. Moreover, the proof in [SZ94] generalizes to fields of arbitrary characteristic, and therefore the formula holds for the generic resultant in characteristic $p > 0$ up to a non-trivial multiplicative constant in $\mathbb{F}_p$. But the multiplicative constant in characteristic 0 specializes to the constants in positive characteristic. Therefore the multiplicative constant is 1 or -1.

This description of the resultant immediately gives rise to the following result:

Proposition 3.12 *Given $F_1, \ldots, F_{n+1} \in \mathbb{F}_q$ of multidegree $(d, \ldots, d)$ one can compute $\mathrm{Res}(F_1, \ldots, F_{n+1})$ in a time of $\mathcal{P}oly((n+1)! \cdot d^n \cdot \log(q))$.*

Proposition 3.11 states in particular that $V(F_1, \ldots, F_{n+1})$ is empty if and only if Φ is surjective, that is, $(F_1, \ldots, F_{n+1})_{(2d-1, 3d-1, \ldots, (n+1)d-1)}$ is equal to the whole ambient space $k[X_1, Y_1, \ldots, X_n, Y_n]_{(2d-1, 3d-1, \ldots, (n+1)d-1)}$. This statement can be generalized:

Proposition 3.13 *Let $F_1, \ldots, F_m$ be multihomogeneous polynomials in $k[X_1, Y_1, \ldots, X_n, Y_n]$ of multidegree $(d, d, \ldots, d)$. Then $V(F_1, \ldots, F_m)$ is empty if and only if $(F_1, \ldots, F_m)_{(2d-1,3d-1,\ldots,(n+1)d-1)} = k[X_1, Y_1, \ldots, X_n, Y_n]_{(2d-1,3d-1,\ldots,(n+1)d-1)}$.*

Proof. It is obvious that the latter statement implies the former. So let $V(F_1, \ldots, F_m)$ be empty. To show the equality we can perform a base-change. So we consider the field extension $k((c_{i,j})_{i=1,\ldots,n+1,j=1,\ldots,m})|k$, where the $c_{i,j}$ are indeterminates, and let $G_i := \sum_{j=1}^m c_{i,j}F_j$ for $i = 1, \ldots, n+1$. By the following lemma, if $g_1, \ldots, g_{n+1}$ are obtained by any dehomogenization from $G_1, \ldots, G_{n+1}$, then $V(g_1, \ldots, g_{n+1})$ is empty. Thus $V(G_1, \ldots, G_{n+1})$ is empty too. Therefore $(G_1, \ldots, G_{n+1})_{(2d-1,3d-1,\ldots,(n+1)d-1)}$ is equal to the ambient space. This clearly implies that $(F_1, \ldots, F_m)_{(2d-1,3d-1,\ldots,(n+1)d-1)}$ is equal to the ambient space too. □

Lemma 3.14 *Let k be a field, and let R be a non-trivial commutative noetherian k-algebra of dimension n. Let $f_1, \ldots, f_m \in R$ with $(f_1, \ldots f_m) = R$. Now let $g_i := \sum_{j=1}^m c_{i,j}f_j$ in $R \otimes_k k((c_{i,j})_{i,j})$ for $i = 1, \ldots, n+1$. Then $g_1, \ldots, g_{n+1}$ generate the unit ideal of $R \otimes_k k((c_{i,j})_{i,j})$.*

Proof. This statement follows from the following statement by induction on n:

Let R be a non-trivial commutative noetherian k-algebra, and let $f_1, \ldots, f_m \in R$ with $(f_1, \ldots, f_m) = R$. Then $\dim((R \otimes_k k(c_1, \ldots, c_m))/(c_1 f_1 + \cdots + c_m c_m)) < \dim(R \otimes_k k(c_1, \ldots, c_m)) = \dim(R)$, where we define the dimension of the trivial algebra as -1.

We assume that this statement is well known to the experts in commutative algebra. Because we could not find a suitable reference we give here a proof.

We have to show that $c_1 f_1 + \cdots + c_m f_m$ is not contained in any minimal prime ideal of $R \otimes_k k(c_1, \ldots, c_m)$.

Now, the minimal prime ideals of $R \otimes_k k(c_1, \ldots, c_m)$ are exactly the ideals of the form $(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of R. (Let first $\mathfrak{p}$ be a prime ideal of R. Then $R/(\mathfrak{p}) \otimes_k k[c_1, \ldots, c_n] \simeq (R/\mathfrak{p})[c_1, \ldots, c_n]$ is a domain. Therefore $R/\mathfrak{p} \otimes_k k(c_1, \ldots, c_n) \simeq (R \otimes_k k(c_1, \ldots, c_n))/(\mathfrak{p})$, which is a localization of the previous ring, is a domain too. Thus $(\mathfrak{p})$ is prime. Let us assume that $\mathfrak{p}$ is minimal, and let $\mathfrak{P} \subseteq (\mathfrak{p})$ be a prime ideal of $R \otimes_k k(c_1, \ldots, c_m)$. Then $\mathfrak{P} \cap R = \mathfrak{p}$ by the minimality of $\mathfrak{p}$, thus $(\mathfrak{P} \cap R) = (\mathfrak{p})$. As $(\mathfrak{P} \cap R) \subseteq \mathfrak{P}$, we have $\mathfrak{P} = (\mathfrak{p})$. We conclude that $(\mathfrak{p})$ is a minimal prime ideal. Now let $\mathfrak{P}$ be any minimal prime ideal of $R \otimes_k k(c_1, \ldots, c_m)$. By what we just have shown $(\mathfrak{P} \cap R)$ is then a prime ideal of $R \otimes_k k(c_1, \ldots, c_m)$. Moreover, this ideal is obviously contained in $\mathfrak{P}$

and thus equal to $\mathfrak{P}$. Now $\mathfrak{P} \cap R$ is also minimal because otherwise $(\mathfrak{P} \cap P)$ was not minimal either.)

So let us fix a minimal prime ideal $\mathfrak{p}$ of R. By assumption the residue classes $[f_1]_{\mathfrak{p}}, \ldots, [f_m]_{\mathfrak{p}}$ generate $R/\mathfrak{p}$. This implies in particular that there exists some $i \in \{1, \ldots, m\}$ such that $[f_i]_{\mathfrak{p}} \neq 0$. Therefore $c_1[f_1]_{\mathfrak{p}} + \cdots + c_m[f_m]_{\mathfrak{p}} \neq 0 \in R/\mathfrak{p} \otimes_k k(c_1, \ldots, c_m) \simeq (R \otimes_k k(c_1, \ldots, c_m))/(\mathfrak{p})$. Thus $c_1 f_1 + \cdots + c_m f_m \notin (\mathfrak{p})$. □

Proposition 3.13 implies immediately:

Proposition 3.15 *Given $F_1, \ldots, F_m \in \mathbb{F}_q[X_1, Y_1, \ldots, X_n, Y_n]$ as above, one can determine if $V(F_1, \ldots, F_m)$ is empty in a time of $\mathcal{P}oly(m \cdot n! \cdot d^n \cdot \log(q))$.*

We now prove:

Proposition 3.16 *Given multihomogeneous polynomials $F_1, \ldots, F_n \in \mathbb{F}_q[X_1, Y_1, \ldots, X_n, Y_n]$ of multidegree $(d, d, \ldots, d)$, where $q \geq n! \cdot d^n$, one can determine in a time of $\mathcal{P}oly(n! \cdot d^n \cdot \log(q))$ if $V(F_1, \ldots, F_n)$ is zero-dimensional. If this is the case, one can compute in an expected time of $\mathcal{P}oly(n! \cdot d^n \cdot \log(q))$ all its $\mathbb{F}_q$-rational points.*

Proof. Let $k = \mathbb{F}_q$, and let for $i = 1, \ldots, n$ $p_i : (\mathbb{P}^1_k)^n \longrightarrow \mathbb{P}^1_k$ be the projection to i^{th} component. Then $V(F_1, \ldots, F_n)$ is not zero-dimensional if and only if there is some $i = 1, \ldots, n$ such that $p_i(V(F_1, \ldots, F_n))$ is equal to $\mathbb{P}^1_k$. (If $p_i(V(F_1, \ldots, F_n)) = \mathbb{P}^1_k$ for some i, then clearly $V(F_1, \ldots, F_n)$ is not zero-dimensional. Otherwise $V(F_1, \ldots, F_n)$ is contained in the finite set $\bigcap_{i=1}^n p_i^{-1}(p_i(V(F_1, \ldots, F_n)))$.)

For each $i = 1, \ldots, n$ we consider the multigraded resultant of $F_1, \ldots, F_n$ with respect to all coordinates except X_i, Y_i. Let us denote this resultant by $\operatorname{Res}_{\overset{\vee}{(X_i,Y_i)}}(F_1, \ldots, F_n)$. By definition $\operatorname{Res}_{\overset{\vee}{(X_i,Y_i)}}(F_1, \ldots, F_n)$ vanishes exactly on $p_i(V(F_1, \ldots, V_n))$, and one easily see with Proposition 3.9 c) that this is a homogeneous polynomial of degree $n! \cdot d^n$.

We thus see that $V(F_1, \ldots, F_n)$ is not zero-dimensional if and only if at least one of the resultants $\operatorname{Res}_{\overset{\vee}{(X_i,Y_i)}}(F_1, \ldots, F_n)$ vanishes. We can thus decide if $V(F_1, \ldots, F_n)$ is zero-dimensional or not by checking if all these resultants are non-trivial.

Each of these resultants is a homogeneous polynomial of degree $n! \cdot d^n$, thus it vanishes if and only if it vanishes on $n! \cdot d^n + 1$ distinct points in $\mathbb{P}^1(\overline{k})$.

By assumption we have $n! \cdot d^n$ distinct elements of k at our disposal. Including ∞ these give $n! \cdot d^n + 1$ elements of $\mathbb{P}^1(k)$. We can therefore check if the resultant $\operatorname{Res}_{\overset{\vee}{(X_i,Y_i)}}(F_1, \ldots, F_n)$ vanishes by computing all the resultants obtained by substituting X_i and Y_i with the $n! \cdot d^n + 1$ elements of $\mathbb{P}^1(k)$ and checking if the results are 0. By Proposition 3.12 each of these computations can be performed in a time which is polynomially bounded in $n! \cdot d^{n-1} \log(q)$, and there are $n \cdot (n! \cdot d^n + 1)$ resultants to be computed. The overall running time is thus polynomially bounded in $n! \cdot d^n \cdot \log(q)$. We have shown the first statement of the proposition.

We now come to the computation of the k-rational solutions, provided that the system is indeed zero-dimensional.

We start off in the same way as above, and from the "evaluated resultants" we compute the resultants $\operatorname{Res}_{\overset{\vee}{(X_i,Y_i)}}(F_1, \ldots, F_n)$ by interpolation. For this we again compute the "evaluated resultants" as determinants as in Proposition 3.11. Here for each i all the $n! \cdot d^n + 1$ matrices have to be computed with respect to the same ordering of monomials in order that the sign is consistent.

By assumption all these resultants are non-trivial. We factorize them and determine their roots in k; let L_i be a list of the roots of the i^{th} resultant, that is, of the k-rational points of $p_i(V(F_1, \ldots, F_n))$.

We now compute the solutions in an iterative manner, by successively imposing conditions of the coordinates. We start out with the k-rational points in $p_1(V(F_1, \ldots, F_n))$, that is, L_1. Suppose now that we know the k-rational points of $(p_1, \ldots, p_i)(V(F_1, \ldots, F_n))$, which we have stored in a list S_i. Then for each point of $P = (P_1, \ldots, P_i)$ in S_i and Q in L_{i+1}, we check if the system obtained by substituting P for $X_1, Y_1, \ldots, X_i, Y_i$ and Q for (X_{i+1}, Y_{i+1}) is consistent, that is if it has a solution over $\overline{k}$. Then all tuples (P, Q) are inserted into a new list S_{i+1} for later inspection. Note here the important point that the list S_i has $\leq n! \cdot d^n$ elements.

Let us give the algorithm in a more formal way:

Algorithm for solving multihomogeneous zero-dimensional systems

Input: Multihomogeneous polynomials $F_1, \ldots, F_n \in \mathbb{F}_q[X_1, Y_1, \ldots, X_n, Y_n]$ of multidegree $(d, d, \ldots, d)$ where $q \geq n! \cdot d^n$ such that $V(F_1, \ldots, F_n)$ is zero-dimensional.

Output: All $\mathbb{F}_q$-rational points of $V(F_1, \ldots, F_n)$.

1. For each $i = 1, \ldots, n$, compute $\operatorname{Res}_{\overset{\vee}{(X_i,Y_i)}}(F_1, \ldots, F_n)$ by interpolation. (*Each of these resultants is non-trivial by assumption.*)

2. Factorize these resultants and compute their roots in $\mathbb{P}^1(\mathbb{F}_q)$. Let L_i be a list of roots of the i^{th} resultant.

3. Let $S_1 \longleftarrow L_1$.

4. For $i = 1, \ldots, n-1$ do
   Determine a list S_{i+1} consisting of elements of $(\mathbb{P}^1(\mathbb{F}_q))^{i+1}$ as follows: For each $P = (P_1, \ldots, P_i) \in S_i$ and $Q \in L_{i+1}$ check if the system obtained by substituting P for $X_1, Y_1, \ldots, X_i, Y_i$ and Q for X_{i+1}, Y_{i+1} is consistent. If this is the case, insert (P, Q) into S_{i+1}.

5. Output S_n.

It is obvious that each of the lists S_i contains exactly the k-rational points of $(p_1, \ldots, p_i)(V(F_1, \ldots, F_n))$. Thus the output of the algorithm consists of the k-rational points of $V(F_1, \ldots, F_n)$.

Let us analyze the complexity: Step 1 can clearly be performed in a time of $\mathcal{P}oly(n! \cdot d^n \log(q))$ (cf. Proposition 3.12). Step 2 can be performed in an expected time of $\mathcal{P}oly(n! \cdot d^n \log(q))$ with the algorithm by Cantor and Zassenhaus ([CZ81]). Each of the checks in Step 4 can be performed with a time of $\mathcal{P}oly(n! \cdot d^n \cdot \log(q))$ by Proposition 3.13. Now, as already remarked each list S_i contains at most $n! \cdot d^n$ elements. Therefore, there are at most $(n! \cdot d^n)^2$ tuples (P, Q) to be considered for each value of i. Thus Step 4 can also be performed in a time of $\mathcal{P}oly(n! \cdot d^n \log(q))$. □

One might have to pass to a field extension of degree $\leq \log_2(n! \cdot d^n)$ in order that enough field elements are available. To construct an appropriate field extension, one can choose a polynomial of appropriate degree uniformly at random and test for irreducibility. Like this, one obtains:

Proposition 3.17 *Given multihomogeneous polynomials $F_1, \ldots, F_n \in \mathbb{F}_q[X_1, Y_1, \ldots, X_n, Y_n]$ of multidegree $(d, d, \ldots, d)$, one can determine if $V(F_1, \ldots, F_{n+1})$ is zero-dimensional and if this is the case compute all its $\mathbb{F}_q$-rational points in an expected time of $\mathcal{P}oly(n! \cdot d^n \cdot \log(q))$.*

3.4 Interpolation

Similarly to the algorithm above, the computation of the summation polynomials will be based on an interpolation. In contrast to the computation above, the result is however a multihomogeneous polynomial. Here we consider the corresponding interpolation problem.

Let us first consider the classical 1-dimensional interpolation problem in the context of homogeneous polynomials: Let $d \in \mathbb{N}$ and $(a_j, b_j) \in k^2 - \{0\}$ for $j = 1, \ldots, d+1$ such that the induced elements in $\mathbb{P}^1(k)$ are pairwise distinct. Moreover, let $c_1, \ldots, c_{d+1} \in k$. Then there is exactly one homogeneous polynomial $F(X, Y) \in k[X, Y]$ of degree d with $F(a_j, b_j) = c_j$ for all

$j = 1, \ldots, d+1$. Moreover, with

$$L_j := \prod_{\ell \neq j} \frac{b_\ell X - a_\ell Y}{a_j b_\ell - a_\ell b_j} \tag{4}$$

we have

$$F = \sum_j c_j L_j \ . \tag{5}$$

Proposition 3.18 *Let $\underline{d} \in \mathbb{N}^n$, and let $S := \{1, \ldots, d_1 + 1\} \times \cdots \times \{1, \ldots, d_n + 1\}$. Let k be a field, let $(a_{i,j}, b_{,j}) \in k^2 - \{0\}$ for $i = 1, \ldots, n$ and $j = 1, \ldots, d_i + 1$ such that for each i, the elements $(a_{i,1} : b_{i,1}), \ldots, (a_{i,d_i+1} : b_{i,d_i+1}) \in \mathbb{P}^1(k)$ are pairwise distinct, and let $c_{\underline{j}} \in k$ for $\underline{j} \in S$.*

Then there is exactly one multihomogeneous polynomial $F \in k[X_1, Y_1, \ldots, X_n, Y_n]$ of multidegree $\underline{d}$ with $F(a_{1,j_1}, b_{1,j_2}, \ldots, a_{n,j_n}, b_{n,j_n}) = b_{\underline{j}}$ for all $\underline{j} \in S$.

Proof. The case $n = 1$ is treated above. For the general case we proceed by induction on n.

Let us first prove the uniqueness. For this, let $\underline{d}$, S, k, and $(a_{i,j}, b_{,j}) \in k^2 - \{0\}$ for $i = 1, \ldots, n$ and $j = 1, \ldots, d_i + 1$ be as in the proposition, and let $F \in k[X_1, Y_1, \ldots, X_n, Y_n]$ be of multidegree $\underline{d}$ with $F(a_{1,j_1}, b_{1,j_2}, \ldots, a_{n,j_n}, b_{n,j_n}) = 0$ for all $\underline{j} \in S$.

Then be induction hypothesis, for each $j = 1, \ldots, d_n + 1$, $F(X_1, Y_1, \ldots, X_{n-1}, Y_{n-1}, a_{n,j}, b_{n,j}) = 0 \in k[X_1, Y_1, \ldots, X_{n-1}, Y_{n-1}]$. We now regard $F(X_1, Y_1, \ldots, X_n, Y_n)$ as a bivariate homogeneous polynomial in the ring $k(X_1, Y_1, \ldots, X_{n-1}, Y_{n-1})[X_n, Y_n]$. Then by the uniqueness of the solution of the 1-dimensional interpolation problem, we conclude that $F = 0$.

We come to the existence. So let objects as in the proposition be given.

For each $j = 1, \ldots, d_n + 1$ there is by induction assumption exactly one multihomogeneous polynomial $C_j \in k[X_1, Y_1, \ldots, X_{n-1}, Y_{n-1}]$ of multidegree $(d_1, \ldots, d_{n-1})$ with $C_j(a_{1,j_1}, b_{1,j_2}, \ldots, a_{n-1,j_{n-1}}, b_{n-1,j_{n-1}}) = c_{\underline{j}}$ for all $\underline{j} \in S$ with $j_n = j$. Let $L_j := \prod_{\ell \neq j} \frac{b_\ell X_n - a_\ell Y_n}{a_j b_\ell - a_\ell b_j}$ for $j = 1, \ldots, d_n + 1$. Then the polynomial $F := \sum_j C_j L_j$ fulfills the requirements. □

We call the computation problem to determine the polynomial F, given the data in the proposition the *multihomogeneous interpolation problem.* One can solve this problem with an obvious linear algebra approach. We therefore obtain:

Proposition 3.19 *The multihomogeneous interpolation problem over finite fields can be solved in a time of $\mathcal{P}oly((d_1 + 1) \cdots (d_n + 1) \cdot \log(q))$, where as* *above* $\underline{d}$ *is the multidegree of the polynomial to be computed and* $\mathbb{F}_q$ *is the ground field.*

4 The summation polynomials

In this section we prove Propositions 2.1 and 2.3 on the summation polynomials. Let E be an elliptic curve over a field k, let $m \in \mathbb{N}, m \geq 2$, and let $\varphi : E \longrightarrow \mathbb{P}^1_k$ be a covering of degree 2 which satisfies $\varphi \circ [-1] = \varphi$.

Now let N_m (or N) be the kernel of the addition map $E^m \longrightarrow E$, $(P_1, \ldots, P_m) \mapsto P_1 + \cdots + P_m$. (Here the P_i are Z-valued points for some k-scheme Z.) Note that N is isomorphic to E^{m-1} via the projection $(P_1, \ldots, P_m) \mapsto (P_1, \ldots, P_{m-1})$.

We now consider the projection $E^m \longrightarrow (\mathbb{P}^1_k)^m$ induced by φ. Note that $[-1]$ operates on N, and the map $N \hookrightarrow E^m \longrightarrow (\mathbb{P}^1_k)^m$ factors through the quotient $N/[-1]$.

Definition 4.1 Let $H_{\varphi,m}$ (or H_m or H) be the image of N in $(\mathbb{P}^1_k)^m$ (with the induced subscheme structure).

Lemma 4.2

a) *The induced map* $N/[-1] \longrightarrow H$ *is finite and birational.*

b) H *is a hyperplane in* $(\mathbb{P}^1_k)^m$ *of multidegree* $(2^{m-2}, \ldots, 2^{m-2})$.

c) *The projections* $H \longrightarrow \mathbb{P}^{m-1}_K$ *to any* $m-1$ *of the* m *components are flat coverings of degree* 2^{m-2}.

Proof. The maps $N \hookrightarrow E^m \longrightarrow (\mathbb{P}^1_k)^m$ and $H \hookrightarrow (\mathbb{P}^1_k)^m$ are clearly finite. It follows immediately that the induced map $N \longrightarrow H$ is also finite. This in turn implies that the induced map $N/[-1] \longrightarrow H$ is finite too (by definition of the geometric quotient).

Let us now consider the commutative diagram

$$\begin{tikzcd}
 & N \arrow[r, hook] \arrow[d] \arrow[dl] & E^m \arrow[d] \arrow[dll] \\
E^{m-1} \arrow[d] & H \arrow[r, hook] \arrow[dl] & (\mathbb{P}^1_k)^m \arrow[dll] \; , \\
(\mathbb{P}^1_k)^{m-1} & &
\end{tikzcd}$$

where the morphisms $E^m \longrightarrow E^{m-1}$ and $(\mathbb{P}^1_k)^m \longrightarrow (\mathbb{P}^1_k)^{m-1}$ are the projections to the first $m-1$ coordinates. Then the induced morphism $N \longrightarrow$

E^{m-1} is an isomorphism, and the morphism $E^{m-1} \longrightarrow (\mathbb{P}^1_k)^{m-1}$ is a generically separable flat covering of degree 2^{m-1}.

Below we show that the map $N \longrightarrow H$ generically has degree 2, and the map $H \longrightarrow (\mathbb{P}^1_k)^{m-1}$ generically has degree 2^{m-2}. This statement implies statements a) and b) in the lemma. Indeed, first as $N \longrightarrow H$ generically has degree 2, the induced map $N/[-1] \longrightarrow H$ generically has degree 1, that is, it is birational. Second, the fact that the map $H \longrightarrow (\mathbb{P}^1_k)^{m-1}$ is quasi-finite and generically of degree 2^{m-2} implies that the last component of the multidegree of H is 2^{m-2}. "By symmetry" (or by a repetition of the argument with projections to different components) then all components of the multidegree are 2^{m-2}.

Note first that we have already established that both maps are generically separable, and that the product of the two degrees is 2^{m-1}. Therefore, it suffices to show that the extension of function fields $k(N)|k(H)$ has separability degree 2.

We are going to apply the isomorphism $E^{m-1} \longrightarrow N$ which is the inverse of the projection $N \longrightarrow E^{m-1}$ and consider the extension $k(E^{m-1})|k(H)$.

Let $\Omega := \overline{k(E^{m-1})}$, let $p_i : E^{m-1} \longrightarrow E$ be the projection to the i^{th} coordinate, and let $P_i \in E(\Omega)$ be the induced points. (That is, P_i is the morphism $\text{Spec}(\Omega) \longrightarrow \text{Spec}(k(E^{m-1})) \longrightarrow E^{m-1} \xrightarrow{p_i} E$, where the first two morphisms are the canonical ones.) Let $p_m := -\sum_{i=1}^{m-1} p_i$ and $P_m := -\sum_{i=1}^{m-1} P_i$.

Then the inverse of the projection $N \longrightarrow E^{m-1}$ to the first $m-1$ coordinates is given by $(p_1, \ldots, p_m)$; the corresponding Ω-valued point of N is given by $(P_1, \ldots, P_m)$.

The points $P_1, \ldots, P_{m-1}$ are linearly independent, since the maps $p_1, \ldots, p_{m-1}$ are linearly independent, the map $\text{Mor}_k(E^{m-1}, E) \longrightarrow E(k(E^{m-1}))$ is injective (in fact, it is an isomorphism), and the map $E(k(E^{m-1})) \longrightarrow \text{Spec}(\Omega)$ is injective too.

Now let us consider the preimage of $x(P_1, \ldots, P_m) = (x \circ P_1, \ldots, x \circ P_m) \in H(\Omega)$ in $N(\Omega)$. This set consists of all tuples $(\epsilon_1 P_1, \ldots, \epsilon_m P_m) \in E^m(\Omega)$ with $\epsilon_i = \pm 1$ and $\sum_{i=1}^m \epsilon_i P_i = O$. Clearly, there are exactly two such tuples: $\pm(P_1, \ldots, P_m)$.

We conclude: There are exactly two Ω-valued points of E^{m-1} which induce the Ω-valued point $(x \circ P_1, \ldots, x \circ P_m) \in H(\Omega)$ under the projection $N \longrightarrow H$. This means that there are exactly two extensions of the canonical inclusion $k(E^{m-1}) \longrightarrow \Omega$ to $k(N)$. Therefore, the separability degree of the extension $k(E^{m-1})|k(H)$ is 2.

We come to c). We still (wlog.) only consider the projection $p : H \longrightarrow (\mathbb{P}^1_k)^{m-1}$ to the first $m-1$ components. As the map is quasi-finite and as H has multidegree $(2^{m-2}, \ldots, 2^{m-2})$, each fiber has degree 2^{m-2}. With other words: The Hilbert polynomials of the fibers are equal to 2^{m-2}. With [Har77, Theorem 9.9] we conclude that p is flat.

Note that H is a projective over $(\mathbb{P}^1)^{m-1}$, thus in particular proper. Moreover, p is quasi-finite. These two properties together are equivalent to being finite by [Gro61, Proposition 4.4.2]. □

Now clearly, if S is any irreducible polynomial in $k[X_1, Y_1, \ldots, X_m, Y_m]$ which is multihomogeneous, then S satisfies the conditions of Proposition 2.1 if and only if $H = V(S)$. This establishes Proposition 2.1.

Thus the m^{th} summation polynomial (cf. Definition 2.2) with respect to φ is the (up to a multiplicative constant unique) polynomial S with $V(S) = H$.

Remark 4.3 Let $\alpha \in \mathrm{Aut}(\mathbb{P}^1_k)$. Then $H_{\alpha\circ\varphi,m} = \alpha(H_{\varphi,m})$, with other words: $H_{\alpha^{-1}\circ\varphi,m} = \alpha^{-1}(H_{\varphi,m})$. This implies that $S_{\alpha^{-1}\circ\varphi,m} = \alpha^*(S_{\varphi,m})$.

We now discuss how the summation polynomials for elliptic curves in Weierstraß form can be given in an explicit and constructive way, following [Sem98].

Lemma 4.4 *Let E be an elliptic curve in $\mathbb{P}^2_k$ in Weierstraß form:*

$$E = V(Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3))$$

with $a_1, a_2, a_3, a_4, a_6 \in k$ and $O = [0 : 1 : 0]$. Then the 3^{rd} summation polynomial of E with respect to $x_{|E}$ is

$$\begin{aligned}&\big((x_1^2x_2^2 + x_2^2x_3^2 + x_1^2x_3^2) - 2(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2)\\ &-(a_1^2 + 4a_2)x_1x_2x_3 - (a_1a_3 + 2a_4) \cdot (x_1x_2 + x_2x_3 + x_1x_3)\\ &-(a_3^2 + 4a_6) \cdot (x_1 + x_2 + x_3)\\ &-a_1^2a_6 + a_1a_3a_4 - a_2a_3^2 - 4a_2a_6 + a_4^2\big) \cdot Y_1^2Y_2^2Y_3^2\ .\end{aligned}$$

Sketch of the proof. Let S be the polynomial in the lemma. Using the inversion and addition formulae for elliptic curves in Weierstraß form (cf. [Sil86]), one can check (with a rather lengthy computation) that for all $P_1, P_2 \in E(\overline{k})$, $S(x(P_1), x(P_2), x(P_1 + x(P_3)) = 0$. This implies that S_3 divides S. As both polynomials have multidegree $(2, 2, 2)$, it follows that they are equal. Let us note here that one only has to check that $S(x(P_1), x(P_2), x(P_1 + P_3))$ for $P_1 \neq \pm P_2$ and $P_1, P_2 \neq O$ because then S vanishes on an open part of H_3 and thus also on all of H_3. □

Let us indicate how the polynomial S was *found*, following [Sem04]:

Let $P_1, P_2 \in E(\overline{k})$ with $P_1, P_2 \neq O$ and $P_1 \neq \pm P_2$. Then clearly both $x(P_1+P_2)$ and $x(P_1-P_2)$ satisfy the polynomial $(x-x(P_1+P_2))(x-x(P_1+$

P_2)). So we computed this polynomial over the field $\mathbb{Q}(a_1, a_2, a_3, a_4, a_6)$ and for "generic" P_1, P_2, using the computer algebra system MAGMA. The polynomial S is then obtained by multiplication with the denominator and homogenization.

Lemma 4.5 *Let E still be an elliptic curve and $\varphi : E \longrightarrow \mathbb{P}^1_k$ a covering of degree 2 with $\varphi \circ [-1] = \varphi$. Let $s, t \in \mathbb{N}$ with $s, t \geq 2$. Then*

$$S_{\varphi,s+t}(X_1, Y_1, \ldots, X_{s+t}, Y_{s+t}) =$$

$$\mathrm{Res}_{(X,Y)}(S_{\varphi,s+1}(X_1, Y_1, \ldots, X_s, Y_s, X, Y),$$
$$S_{\varphi,t+1}(X_{s+1}, Y_{s+1}, \ldots, X_{s+t}, Y_{s+t}, X, Y)) \ .$$

Here by $\mathrm{Res}_{(X,Y)}$ we mean the usual Sylvester resultant for homogeneous polynomials in X and Y of degrees 2^{s-1} and 2^{t-1}.

Proof. For $(P_1, \ldots, P_{s+t}) \in (E(\overline{k}))^{s+t}$ we have $P_1 + \cdots + P_{s+t} = O$ if and only if there exists some $P \in E(\overline{k})$ with $P_1 + \cdots + P_s + P = O$ and $P_{s+1} + \cdots + P_{s+t} + P = O$.

It follows that topologically the hyperplane H_{s+t} is the image of $V(S_{\varphi,s+1}(X_1, Y_1, \ldots, X_s, Y_s, X, Y), S_{\varphi,t+1}(X_{s+1}, Y_{s+1}, \ldots, X_{s+t-1}, Y_{s+t}, X, Y))$ in $(\mathbb{P}^1_k)^n \times \mathrm{Proj}(k[X, Y])$ under the projection to $(\mathbb{P}^1_k)^n$. As H_{s+t} is irreducible it follows that the resultant in the lemma is (up to a multiplicative constant) a power of $S_{\varphi,s+t}$.

In order to prove that the resultant is (up to a constant) equal to $S_{\varphi,s+t}$, we consider their multidegrees.

The generic Sylvester resultant for polynomials of degrees a and b has degree b in the coefficients of the first polynomial and degree a in the coefficients of the second polynomial. We apply this with $a = 2^{s-1}$ and $b = 2^{t-1}$. In our case we obtain a polynomial of degree $2^{s-1} \cdot 2^{t-1} = 2^{s+t-2}$ in (X_i, Y_i) for all $i = 1, \ldots, s + t$.

As $S_{\varphi,s+t}$ has multidegree $(2^{s+t-2}, \ldots, 2^{s+t-2})$, the result follows. □

The two preceding lemmata give rise to algorithmic constructions of the summation polynomials over finite fields.

First, given an elliptic curve in Weierstraß form and a covering of degree 2 $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$ with $\varphi \circ [-1] = \varphi$ (which means that the automorphism $\alpha \in \mathrm{Aut}(\mathbb{P}^1_k)$ with $\varphi = \alpha \circ x_{|E}$ is given), one can easily determine $S_{\varphi,3}$ via Lemma 4.4 and Remark 4.3.

Further, one can compute $S_{\varphi,m}$ for $m \geq 3$ from $S_{\varphi,m-1}$ and $S_{\varphi,3}$ by applying the above lemma with $s = m - 2$ and $t = 2$. This computation can be performed via interpolation provided that $q \geq 2^{m-2}$ (which means that $\#\mathbb{P}^1(\mathbb{F}_q) \geq 2^{m-2} + 1$) (cf. Proposition 3.19).

Proposition 4.6 *Given an elliptic curve E over a finite field $\mathbb{F}_q$ with $q \geq 2^{m-2}$ in Weierstraß form and a covering $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$ of degree 2 with $\varphi \circ [-1] = \varphi$, a natural number $m \geq 3$, one can compute the m^{th} summation polynomial of E with respect to φ in a time of $\mathcal{P}oly(e^{m^2} \cdot \log(q))$.*

By passing to field extensions if necessary, one obtains Proposition 2.3.

5 Geometric background on the algorithm and analysis

The main purpose of this section is to prove Proposition 2.7. Additionally, we give some background information on the definition of the factor base from a geometric point of view.

5.1 Weil restrictions

We make use of *Weil restrictions* of schemes. Here we briefly recall the definition and some basic properties of Weil restrictions. For further information we refer to [BLR80, 7.6] and [Die01, Chapter 1].

Let S' and S be locally noetherian schemes, and let a flat covering $S' \longrightarrow S$ (a finite and flat morphism) be fixed. (Note here that a flat covering is locally free (see [Mat89, Theorem 7.10]).) Let X' be an S'-scheme such that the fibers of X' over S' are quasi-projective. Then one can show that the functor from S-schemes to sets $Z \mapsto \mathrm{Mor}_{S'}(Z_{S'}, X')$ is representable by an S-scheme; the (up to unique isomorphism unique) representing object is called the *Weil restriction* of X' with respect to $S' \longrightarrow S$. We denote it by $\mathrm{Res}^{S'}_S(X')$.[4]

A reformulation of this definition is: The Weil restriction of X' with respect to $S' \longrightarrow S$ is a an S-scheme $\mathrm{Res}^{S'}_S(X')$ together with an S'-morphism $u : (\mathrm{Res}^{S'}_S(X'))_{S'} \longrightarrow X'$ such that the following holds: Whenever Z is an S-scheme, and $\alpha : Z \times_S S' = Z_{S'} \longrightarrow X'$ is an S'-morphism, there is a unique S-morphism $\beta : Z \longrightarrow \mathrm{Res}^{S'}_S(Z)$ with $\alpha = \beta_{S'} \circ u$, where $\beta_{S'} := \beta \times_S S' = \beta \times_S \mathrm{id}_{S'}$. We denote the morphism β by $\alpha_{\circledcirc}$.

The assignment $X \mapsto \mathrm{Res}^{S'}_S(X')$ gives rise to a functor (which we call *scalar-restriction functor*) from the category of S'-schemes with quasi-projective fibers to the category of S-schemes. Moreover, if X' is an affine S'-scheme, then $\mathrm{Res}^{S'}_S(X')$ is an affine S-scheme.

We will use the following two lemmata. The proofs are rather easy and therefore omitted.

[4] The similarity between the notations for Weil restrictions and resultants is accidental.

Lemma 5.1 *Let $S' \longrightarrow S$ be as above, and let X', Y', W' be S'-schemes with S'-morphisms $X' \longrightarrow W'$ and $Y' \longrightarrow W'$. Then we have a Cartesian diagram*

$$\begin{tikzcd}
\mathrm{Res}_S^{S'}(X' \times_{W'} Y') \arrow[r] \arrow[d] & \mathrm{Res}_S^{S'}(Y') \arrow[d] \\
\mathrm{Res}_S^{S'}(X') \arrow[r] & \mathrm{Res}_S^{S'}(W')
\end{tikzcd}$$

with the obvious canonical morphisms.

Lemma 5.2 *Let $S' \longrightarrow S$ as above, let T be an S-scheme, and let $T' := T \times_S S'$. Let X' be a T'-scheme with structural morphism $\alpha : X' \longrightarrow T'$.*

Let $v : (\mathrm{Res}_T^{T'}(X'))_{T'} \longrightarrow X'$ be the universal morphism; v is thus a T'-morphism. We have $(\mathrm{Res}_T^{T'}(X')) \times_T T' \simeq (\mathrm{Res}_T^{T'}(X')) \times_S S'$, and v is in particular an S'-morphism. Thus by the universal property of $\mathrm{Res}_S^{S'}(X')$ we have an induced S-morphism $v_{\circledcirc} : \mathrm{Res}_T^{T'}(X') \longrightarrow \mathrm{Res}_S^{S'}(X')$.

Now we have a Cartesian diagram

$$\begin{tikzcd}
\mathrm{Res}_T^{T'}(X') \arrow[r] \arrow[d] & \mathrm{Res}_S^{S'}(X') \arrow[d] \\
T \arrow[r] & \mathrm{Res}_S^{S'}(T')\ ,
\end{tikzcd}$$

where the morphisms are defined as follows: The left morphism is the structural morphism, the right morphism is $\mathrm{Res}_S^{S'}(\alpha)$, the upper morphism is $v_{\circledcirc}$, and the lower morphism is the morphism $\mathrm{id}_{\circledcirc} : T \longrightarrow \mathrm{Res}_S^{S'}(T')$ corresponding to the identity on T' under the defining functorial property of $\mathrm{Res}_S^{S'}(T')$.

Let now $K|k$ be a finite field extension. Then if X' is a quasi-projective (resp. projective) scheme over K, $\mathrm{Res}_k^K(X')$ is a quasi-projective (resp. projective) scheme of dimension $[K : k] \cdot \dim(X')$ over k. Note that by the defining functorial property of the Weil restriction we have in particular a bijection

$$X'(K) = \mathrm{Mor}_K(\mathrm{Spec}(K), X') \longrightarrow \mathrm{Res}_k^K(X')(k) = \mathrm{Mor}_k(\mathrm{Spec}(k), \mathrm{Res}_k^K(X')),$$
$$P \mapsto P_{\circledcirc}\ .$$

If X' is a group scheme over K, $\mathrm{Res}_k^K(X')$ is in a natural way again a group scheme, and in particular if A' is an abelian variety over K, then $\mathrm{Res}_k^K(A')$ is in a natural way an abelian variety too.

Let $K|k$ now be an extension of finite fields of degree n, and let σ be the relative Frobenius automorphism of $K|k$. We denote the induced isomorphism $\mathrm{Spec}(k) \longrightarrow \mathrm{Spec}(k)$ again by σ. Let X' be a quasi-projective

K-scheme. Then we have a canonical isomorphism

$$(\mathrm{Res}_k^K(X'))_K \simeq \prod_{i=0}^{n-1} \sigma^i(X')$$

of K-schemes under which the universal morphism $u : (\mathrm{Res}_k^K(X'))_K \longrightarrow X'$ corresponds to the projection

$$u : \prod_{i=0}^{n-1} \sigma^i(X') \longrightarrow X' \; .$$

Moreover, if Z is any k-scheme and $\alpha : Z_K \longrightarrow X'$ is a morphism, then $(\alpha_{\circledcirc})_K$ corresponds to

$$(\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)) : Z_K \longrightarrow \prod_{i=0}^{n-1} \sigma^i(X')$$

and if $\varphi : X' \longrightarrow Y'$ is a morphism of quasi-projective K-schemes, then $\mathrm{Res}_k^K(\varphi)$ corresponds to

$$\varphi \times \sigma(\varphi) \times \cdots \times \sigma^{n-1}(\varphi) : \prod_{i=0}^{n-1} \sigma^i(X') \longrightarrow \prod_{i=0}^{n-1} \sigma^i(Y') \; .$$

5.2 Background on the factor base

Let still $K|k$ be an extension of finite fields of degree n, and as above let σ the Frobenius automorphism relative to k. Let E be an elliptic curve over K, and let us fix a covering $\varphi : E \longrightarrow \mathbb{P}^1_K$ of degree 2 with $\varphi \circ [-1] = \varphi$.

Let $\iota = \mathrm{id}_{\circledcirc} : \mathbb{P}^1_k \longrightarrow \mathrm{Res}_k^K(\mathbb{P}^1_K)$ be the morphism corresponding to the identity on $\mathbb{P}^1_K$. One can easily see (for example via base change to K) that ι is a closed immersion.

Let V be the preimage of $\iota(\mathbb{P}^1_k)$ under $\mathrm{Res}_k^K(\varphi) : \mathrm{Res}_k^K(E) \longrightarrow \mathrm{Res}_k^K(\mathbb{P}^1_k)$. This means by definition that we have a Cartesian diagram

$$\begin{tikzcd} V \arrow[r, hook] \arrow[d] & \mathrm{Res}_k^K(E) \arrow[d, "\mathrm{Res}_k^K(\varphi)"] \\ \mathbb{P}^1_k \arrow[r, hook, "\iota"] & \mathrm{Res}_k^K(\mathbb{P}^1_k) \; . \end{tikzcd} \quad (6)$$

Note that $\mathrm{Res}_k^K(\varphi) : \mathrm{Res}_k^K(E) \longrightarrow \mathrm{Res}_k^K(\mathbb{P}^1_k)$ is a flat covering of degree 2^n (as one sees after base change to K), and therefore $V \longrightarrow \mathbb{P}^1_k$ is a flat covering of degree 2^n too.

Let us now explain the connection of these definitions to the definition of the factor base in the algorithm: Let us consider a particular run of the algorithm. Then under the bijection $\mathbb{P}^1(K) \simeq \mathrm{Res}_k^K(\mathbb{P}^1_K)(k)$ the inclusion $\mathbb{P}^1(k) \subseteq \mathbb{P}^1(K)$ corresponds to $\iota(\mathbb{P}^1_k(k)) \subseteq \mathrm{Res}_k^K(\mathbb{P}^1_K))(k)$. Therefore the factor base $\mathcal{F} = (\varphi^{-1}(\mathbb{P}^1_k)(k)) \subseteq E(K)$ corresponds to $V(k)$ under the bijection $E(K) \simeq \mathrm{Res}_k^K(E)(k)$. One can therefore say that the factor base is defined in a "geometric way" – something that immediately apparent from the definition of the factor base in the algorithm.

The addition on the Weil restriction induces a morphism $V^n \longrightarrow \mathrm{Res}_k^K(E)$, and – again under the bijection $E(K) \simeq \mathrm{Res}_k^K(E)(k)$ – for $P \in E(K)$ the tuples $(P_1, \ldots, P_n) \in E(K)^n$ with $\varphi(P_i) \in \mathbb{P}^1(k)$ and $\sum_i P_i = P$ correspond to the k-valued points of the fiber of $V^n \longrightarrow \mathrm{Res}_k^K(E)$ at $P_{\circledcirc}$, the k-rational point of $\mathrm{Res}_k^K(E)$ corresponding to P.

We now study V under Condition 2.13.

Proposition 5.3 *Let Condition 2.13 be satisfied. Then V is geometrically reduced and geometrically irreducible (and thus birational to a curve).*

Proof. By (6) and Lemma 5.2 we have $V \simeq \mathrm{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(E)$, with respect to the covering $\varphi : E \longrightarrow \mathbb{P}^1_k$. This implies that

$$V_K \simeq E \times_{\mathbb{P}^1_K} \sigma(E) \times_{\mathbb{P}^1_K} \cdots \times_{\mathbb{P}^1_K} \sigma^{n-1}(E) \ , \qquad (7)$$

where the morphisms are $\varphi : E \longrightarrow \mathbb{P}^1_K, \ldots, \sigma^{n-1}(\varphi) : \sigma^{n-1}(E) \longrightarrow \mathbb{P}^1_K$.

Let us now fix an algebraic closure $\overline{k(x)}$ of $k(x)$. Let us denote the Frobenius automorphism of $\overline{k}|k$ also by σ. Let us then prolong σ first to $\overline{k}(x)$ via $\sigma(x) := x$, and and let us fix any automorphism of $\overline{k(x)}|k(x)$ which restricts to σ; let us denote this automorphism again by σ. Moreover, let us fix an injection of $\overline{k}(E)$ into $\overline{k(x)}$ over $k(x)$.

We now consider the total quotient ring of the scheme $V_{\overline{k}}$, which is isomorphic to

$$\overline{k}(E) \otimes_{\overline{k}(x)} \sigma(\overline{k}(E)) \otimes_{\overline{k}(x)} \cdots \otimes_{\overline{k}(x)} \sigma^{n-1}(\overline{k}(E)) \ .$$

By Condition 2.13 for $i = 1, \ldots, n-1$, the extension $\sigma^i(\overline{k}(E))|\overline{k}(x)$ is ramified at $\sigma^i(P)$, but for any $j = 0, \ldots, i-1$, the extension $\sigma^j(\overline{k}(E))|\overline{k}(x)$ is not ramified at $\sigma^i(P)$, thus the extension $\overline{k}(E)\sigma(\overline{k}(E)) \cdots \sigma^{i-1}(\overline{k}(E))|\overline{k}(x)$ in $\overline{k(x)}$ is also not ramified at $\sigma^i(P)$. Thus $\sigma^i(\overline{k}(E))$ is not contained in $\overline{k}(E)\sigma(\overline{k}(E)) \cdots \sigma^{i-1}(\overline{k}(E))$. It follows therefore by induction that the extension $\overline{k}(E)\sigma(\overline{k}(E) \cdots \sigma^{n-1}(\overline{k}(E))|\overline{k}(x)$ in $\overline{k(x)}$ has degree 2^n. Thus the total quotient ring of $V_{\overline{k}}$ is is isomorphic to the composite $\overline{k}(E)\sigma(\overline{k}(E)) \cdots \sigma^{n-1}(\overline{k}(E))$ in $\overline{k(x)}$ and therefore a field. We see that $V_{\overline{k}}$ is reduced and irreducible, thus V is geometrically reduced and geometrically irreducible. □

Proposition 5.4 *Let us still assume that Condition 2.13 is satisfied, let $\mathcal{C}$ be the curve which is birational to V, and let $\pi : \mathcal{C} \longrightarrow V$ be a birational morphism. Then*

a) The genus of $\mathcal{C}$ is $\leq (2n-1)\cdot(2^n-1)$.

b) $\mathcal{C}(\overline{k})$ contains at most $n \cdot 2^{n+2}$ points which map to singular points under the birational morphism $\pi : \mathcal{C} \longrightarrow V$.

Proof. By a general result on elementary abelian extensions (see e.g. [KR89]) we have

$$g(\mathcal{C}) = \sum_L g(L) \ ,$$

where L runs over all subextensions of $\overline{k}(\mathcal{C})|\overline{k}(x)$ of degree 2. We show below that the genus of a function field L as in the sum is always $\leq 2n-1$. This implies that $g(\mathcal{C}) \leq (2n-1)\cdot(2^n-1)$.

To show the claim on the subfields L we proceed with a case distinction.

Let q be even. By Artin-Schreier theory every subfield L of $\overline{k(x)}|k(x)$ of degree 2 corresponds to the a 1-dimensional subspace of the $\mathbb{F}_2$-vector space $\overline{k}(x)/\mathcal{P}(\overline{k}(x))$, where $\mathcal{P}$ is the Artin-Schreier operator.

If now $\overline{k}(E)$ corresponds to $\langle\overline{f}\rangle$, where $\overline{f}$ is the residue class of some $f \in \overline{k}(x)$, then each field L as in the sum corresponds to $\langle a_0\overline{f} + a_1\overline{\sigma(f)} + \cdots + a_{n-1}\overline{\sigma^{n-1}(f)}\rangle$ for a uniquely defined tuple $(a_0,\dots,a_{n-1}) \in \mathbb{F}_2^n - \{0\}$.

Let first $j(E) = 0$. In this case the extension $\overline{k}(E)|\overline{k}(x)$ is ramified at one place, and $\overline{k}(E)$ corresponds to some space $\langle\overline{f}\rangle$, where f is either a polynomial of degree 3 or of the form $\frac{g}{(x-\lambda)^3}$ for $\lambda \in \overline{k}$ and $\deg(g) = 3$.

Using [Sti93, Proposition III.7.8] one sees: If L is any field as in the sum, then $L|\overline{k}(x)$ is ramified at at most n places (this is also immediately obvious), and the corresponding discriminant exponents are all 4. This implies that the genus of L is $\leq 2n-1$.

Let now $j(E) \neq 0$. In this case $\overline{k}(E)|\overline{k}(x)$ is ramified at 2 places, and $\overline{k}(E)$ corresponds to $\langle\overline{f}\rangle$, where f is the sum of two distinct polynomials f_1, f_2 such that each of these polynomials is either x or $\frac{1}{x-a}$ for some $a \in \overline{k}$. Now each subfield L as in the sum is ramified over at most $2n$ places and the different exponents are all 2. Again the genus of L is $\leq 2n-1$.

Let q be odd. In this case $\overline{k}(E)|\overline{k}(x)$ is (tamely) ramified at 4 places. If thus L is as in the sum, $L|\overline{k}(x)$ is ramified at at most $4n$ places. Thus the genus of L is $\leq 2n-1$.

We come to b). Let S be the set of points of $\mathbb{P}^1(\overline{k})$ over which one of the coverings $\sigma^i(E) \longrightarrow \mathbb{P}^1_{\overline{k}}$ is ramified. Using the fact that a morphism obtained from an étale morphism via base change is étale we obtain: The canonical morphism $V \longrightarrow \mathbb{P}^1_k$ is étale outside S. This implies that V is smooth outside the preimage of S, and the birational morphism $\pi : \mathcal{C} \longrightarrow V$ is an isomorphism outside the preimages of S. With other words: All points in $\mathcal{C}(\overline{k})$ which map to singular points of V are contained in the preimage of S.

As the covering $\mathcal{C} \longrightarrow \mathbb{P}^1_k$ has degree 2^n, the preimage of the set S has at most $\#S \cdot 2^n \leq 4n \cdot 2^n$ elements. □

Remark 5.5 Let $k = \mathbb{F}_q$. Then under Condition 2.13 by the above propositions, and the Hasse-Weil bound we have

$$\begin{aligned} &\#\{P \in E(K) \mid \varphi(P) \in \mathbb{P}^1(k)\} = \#V(k) \\ &\geq q + 1 - 2 \cdot (2n-1) \cdot (2^n - 1) \cdot q^{\frac{1}{2}} - n \cdot 2^{n+2} + 1 \; . \end{aligned}$$

For $\log_2(q) \geq 3n$, that is, $2^{\frac{3}{2} \cdot n} \leq q^{\frac{1}{2}}$, and n large enough we have

$$V(k) \geq \frac{1}{2} \cdot (q+1) \; .$$

(The bound $q \geq 3\log_2(n)$ is a bit arbitrary but it serves its purposes, and in order to complete the analysis of the algorithm for the Theorem, we anyway have to impose a more restricted bound.)

This result shows that if φ satisfies Condition 2.13, the set $\{P \in E(K) \mid \varphi(P) \in \mathbb{P}^1(k)\}$ is "reasonably large". Note that this applies then of course in particular to the factor base constructed in the algorithm for the Theorem. We remark however that the main purpose of showing that V is birational to a curve is not to prove that a suitably large factor base can be efficiently constructed – this goal can also easily be reached by choosing the automorphism α used to define φ in a randomized fashion. Rather the key statement is that V^n contains an irreducibility component which maps surjectively to $\mathrm{Res}^K_k(E)$ under the addition morphism and which contains "enough" elements.

5.3 The role of the summation polynomials

Let the hyperplane $H = H_{n+1}$ of $(\mathbb{P}^1_k)^{n+1}$ be defined as in Section 4.

By applying the scalar-restriction functor, we obtain:

$$\mathrm{Res}^K_k(H) \longrightarrow \mathrm{Res}^K_k((\mathbb{P}^1_K)^{n+1}) \simeq (\mathrm{Res}^K_k(\mathbb{P}^1_K))^{n+1} \; .$$

Via base change to K one sees immediately that we have a closed immersion.

Let X be the scheme-theoretic preimage of $\mathrm{Res}^K_k(H)$ in $(\mathbb{P}^1_k)^n \times \mathrm{Res}^K_k(\mathbb{P}^1_K)$ under the closed immersion $\iota \times \iota \times \cdots \times \iota \times \mathrm{id} : (\mathbb{P}^1_k)^n \times \mathrm{Res}^K_k(\mathbb{P}^1_K) \longrightarrow$

$\mathrm{Res}_k^K((\mathbb{P}^1))^{n+1}$. This means by definition that we have a Cartesian diagram

$$\begin{tikzcd} X \arrow[r, hook] \arrow[d, hook] & \mathrm{Res}_k^K(H) \arrow[d, hook] \\ (\mathbb{P}^1_k)^n \times \mathrm{Res}_k^K(\mathbb{P}^1_K) \arrow[r, hook] & (\mathrm{Res}_k^K(\mathbb{P}^1_K))^{n+1} \; . \end{tikzcd} \tag{8}$$

Note that – again under the obvious bijections – the elements of $X(k)$ correspond to the tuples $(Q_1, \ldots, Q_n, Q)$ with $Q_i \in \mathbb{P}^1(k)$ and $Q \in \mathbb{P}^1(K)$ with $(Q_1, \ldots, Q_n, Q) \in H(K)$. The latter condition means of course that there are $P_1, \ldots, P_n, P \in E(\overline{K})$ with $\varphi(P_i) = Q_i$ and $\sum_i P_i = P$.

Notation 5.6 Let $p_1 : (\mathbb{P}^1_k)^n \times \mathrm{Res}_k^K(\mathbb{P}^1_K) \longrightarrow (\mathbb{P}^1_k)^n$ and $p_2 : (\mathbb{P}^1_k)^n \times \mathrm{Res}_k^K(\mathbb{P}^1_K) \longrightarrow \mathrm{Res}_k^K(\mathbb{P}^1_K)$ be the two projections.

Lemma 5.7 *$(p_1)_{|X} : X \longrightarrow (\mathbb{P}^1_k)^n$ is a flat covering of degree $2^{(n-1)\cdot n}$.*

Proof. By Lemma 4.2 c) the projection to the first n components $H \longrightarrow (\mathbb{P}^1_K)^n$ is a flat covering of degree 2^{n-1}. Therefore the induced map $\mathrm{Res}_k^K(H) \longrightarrow \mathrm{Res}_k^K((\mathbb{P}^1_K)^n) \simeq (\mathrm{Res}_k^K(\mathbb{P}^1))^n$ is a flat covering of degree $2^{(n-1)\cdot n}$. The map $(p_1)_{|X} : X \longrightarrow (\mathbb{P}^1_k)^n$ is obtained from this map via base change with $\iota \times \cdots \times \iota : (\mathbb{P}^1_k)^n \longrightarrow (\mathrm{Res}_k^K(\mathbb{P}^1_K))^n$. □

Notation 5.8 Let G be the graph of $-a_n : V^n \longrightarrow \mathrm{Res}_k^K(E)$, where a_n is the restriction of the addition morphism to V^n. (Note the minus sign!)

As in Section 4 let for $m \in \mathbb{N}$ N_m be the kernel of the addition morphism $E^m \longrightarrow E$. One easily sees that $\mathrm{Res}_k^K(N_m)$ is (as a subscheme of $\mathrm{Res}_k^K(E^m)$) the kernel of the addition homomorphism on $\mathrm{Res}_k^K(E^m)$. Let now $N := N_{n+1}$. By considering Z-valued points for any k-scheme Z, one obtains immediately:

Lemma 5.9 *G is the scheme-theoretic intersection of $V^n \times \mathrm{Res}_k^K(E)$ and $\mathrm{Res}_k^K(N)$ in $\mathrm{Res}_k^K(E^{n+1}) \simeq (\mathrm{Res}_k^K(E))^{n+1}$.*

Proposition 5.10 *There is a canonical surjective morphism $G \longrightarrow X$. Moreover, if Condition 2.13 is satisfied, then X is geometrically irreducible.*

Proof. Let us consider the commutative diagram

$$\begin{tikzcd}
G \arrow[rrr, hook] \arrow[dd, hook] & & & \mathrm{Res}_k^K(N) \arrow[dr] \arrow[dd, hook] & \\
& & X \arrow[rr, hook] \arrow[dd, hook] & & \mathrm{Res}_k^K(H) \arrow[dd, hook] \\
V^n \times \mathrm{Res}_k^K(E) \arrow[rrr, hook] \arrow[drr] & & & (\mathrm{Res}_k^K(E))^{n+1} \arrow[dr] & \\
& & (\mathbb{P}_k^1)^n \times \mathrm{Res}_k^K(\mathbb{P}_K^1) \arrow[rr, hook] & & (\mathrm{Res}_k^K(\mathbb{P}_K^1))^{n+1}
\end{tikzcd}$$

with the obvious canonical morphisms. As by definition of X the right-lower subdiagram (i.e. diagram (8)) is Cartesian, we have an induced morphism $G \longrightarrow X$.

It suffices to prove the surjectivity on $\overline{k}$-valued points. So let $Q \in X(\overline{k})$. As the map $N \longrightarrow H$ is surjective, so is $\mathrm{Res}_k^K(N) \longrightarrow \mathrm{Res}_k^K(H)$. Let us consider Q as a point in $\mathrm{Res}_k^K(H)(\overline{k})$, and let us fix a preimage $P \in \mathrm{Res}_k^K(N)(\overline{k})$.

We claim that P lies in $G(\overline{k})$, or with other words that the image of P in $(\mathrm{Res}_k^K(E))^{n+1}(\overline{k})$ lies in $(V^n \times \mathrm{Res}_k^K(E))(\overline{k})$. For this we have to check that the image of P in $\mathrm{Res}_k^K(\mathbb{P}_K^1))(\overline{k})$ lies in $((\mathbb{P}^1)^n \times \mathrm{Res}_k^K(\mathbb{P}_K^1))(\overline{k})$. But this is obvious as the image is nothing but the point Q we started with.

Let now Condition 2.13 be satisfied. By Proposition 5.3 V is then geometrically reduced and geometrically irreducible, thus so is V^n, which is isomorphic to the graph G. As the map $G \longrightarrow X$ is surjective, X is then also geometrically irreducible. □

Let us now fix some $Q \in \mathbb{P}^1(K)$. Following our notation, let $Q_{\circledcirc}$ be the corresponding k-rational point of $\mathrm{Res}_k^K(\mathbb{P}_K^1)$. Let $X_{Q_{\circledcirc}}$ be the fiber of X at $Q_{\circledcirc}$, that is, we have the Cartesian diagram

$$\begin{tikzcd}
X_{Q_{\circledcirc}} \arrow[r, hook] \arrow[d, hook] & X \arrow[d, hook] \\
(\mathbb{P}_k^1)^n \arrow[r, hook] \arrow[d] & (\mathbb{P}_k^1)^n \times \mathrm{Res}_k^K(\mathbb{P}_K^1) \arrow[d] \\
\mathrm{Spec}(k) \arrow[r, hook, "Q_{\circledcirc}"] & \mathrm{Res}_k^K(\mathbb{P}_K^1)\ .
\end{tikzcd}$$

Then we have the following connection with the decomposition algorithm:

Proposition 5.11 *As a subscheme of* $(\mathbb{P}^1_k)^n \times \mathrm{Res}^K_k(\mathbb{P}^1_K)$*,* $X_{Q_\circledcirc}$ *is* $V(S^{(1)}, \dots, S^{(n)})$*, where the polynomials* $S^{(j)} \in k[X_1, Y_1, \dots, X_n, Y_n]$ *are defined as in Equation (2).*

We show first:

Lemma 5.12 *Let* $H_Q \subset (\mathbb{P}^1_K)^n$ *be the restriction of* H *to* $(\mathbb{P}^1_K)^n$ *via the closed immersion* $\mathrm{id} \times \cdots \times \mathrm{id} \times Q : (\mathbb{P}^1_K)^n \simeq (\mathbb{P}^1_K)^n \times_K \mathrm{Spec}(K) \longrightarrow (\mathbb{P}^1_K)^{n+1}$*. Then we have a Cartesian diagram*

$$\begin{tikzcd}
X_{Q_\circledcirc} \arrow[r, hook] \arrow[d, hook] & \mathrm{Res}^K_k(H_Q) \arrow[d, hook] \\
(\mathbb{P}^1_k)^n \arrow[r, hook] & (\mathrm{Res}^K_k(\mathbb{P}^1_K))^n ,
\end{tikzcd}$$

where the lower arrow is given by $\iota \times \cdots \times \iota$*.*

Proof. We have $\mathrm{Res}^K_k(\mathrm{Spec}(K)) = \mathrm{Spec}(k)$ and $\mathrm{Res}^K_k(Q) = Q_\circledcirc$. By Lemma 5.1 the defining Cartesian diagram

$$\begin{tikzcd}
H_Q \arrow[r, hook] \arrow[d, hook] & H \arrow[d, hook] \\
(\mathbb{P}^1_K)^n \arrow[r, hook] & (\mathbb{P}^1)^{n+1}
\end{tikzcd}$$

gives rise to the Cartesian diagram

$$\begin{tikzcd}
\mathrm{Res}^K_k(H_Q) \arrow[r, hook] \arrow[d, hook] & \mathrm{Res}^K_k(H) \arrow[d, hook] \\
(\mathrm{Res}^K_k(\mathbb{P}^1_K))^n \arrow[r, hook] & (\mathrm{Res}^K_k(\mathbb{P}^1_K))^{n+1} ,
\end{tikzcd}$$

where the lower arrow is given by $\mathrm{id} \times \cdots \times \mathrm{id} \times Q_\circledcirc : (\mathrm{Res}^K_k(\mathbb{P}^1_K))^n \simeq (\mathrm{Res}^K_k(\mathbb{P}^1_K))^n \times_k \mathrm{Spec}(k) \longrightarrow (\mathrm{Res}^K_k(\mathbb{P}^1_K))^{n+1}$.

Now $X_{Q_\circledcirc}$ is the pull-back of $\mathrm{Res}^K_k(H)$ to $(\mathbb{P}^1_k)^n$ under the map $\iota \times \cdots \times \iota \times Q_\circledcirc : (\mathbb{P}^1_k)^n \simeq (\mathbb{P}^1_k)^n \times_k \mathrm{Spec}(k) \longrightarrow (\mathrm{Res}^K_k(\mathbb{P}^1_K))^{n+1}$. This implies that we have a Cartesian diagram

$$\begin{tikzcd}
X_{Q_\circledcirc} \arrow[r, hook] \arrow[d, hook] & \mathrm{Res}^K_k(H_Q) \arrow[r, hook] \arrow[d, hook] & \mathrm{Res}^K_k(H) \arrow[d, hook] \\
(\mathbb{P}^1)^n_k \arrow[r, hook] & (\mathrm{Res}^K_k(\mathbb{P}^1_K))^n \arrow[r, hook] & (\mathrm{Res}^K_k(\mathbb{P}^1_K))^{n+1} .
\end{tikzcd}$$

□

We come to the *proof* of Proposition 5.11.

By Lemma 5.12 and Lemma 5.2 we have a commutative diagram

$$\begin{tikzcd}
X_{Q_{\circledcirc}} \arrow[rr, "\sim"] \arrow[dr, hook] & & \mathrm{Res}^{(\mathbb{P}^1_K)^n}_{(\mathbb{P}^1_k)^n}(H_Q) \arrow[dl] \\
 & (\mathbb{P}^1_k)^n \, , &
\end{tikzcd}$$

where the arrow to the left is the structural morphism, which of course is then also a closed immersion.

To establish the result we thus have to show that as a closed subscheme of $(\mathbb{P}^1_k)^n$, $\mathrm{Res}^{(\mathbb{P}^1_K)^n}_{(\mathbb{P}^1_k)^n}(H_Q)$ is equal to $V(S^{(1)}, \ldots, S^{(n)})$.

Let now $S_{\varphi,n+1}$ be the same summation polynomial as in subsection 2.1 (recall that the $(n+1)^{\text{th}}$ summation polynomial with respect to φ is only unique up to multiplication by a non-trivial constant). Also, let $b_1, \ldots, b_n$ be the fixed k-basis of K from subsection 2.1. Note that $b_1, \ldots, b_n$ is then also a basis of the free $k[x_1, \ldots, x_n]$-module $K[x_1, \ldots, x_n]$. Moreover, let $S' := S_{\varphi,n+1}(X_1, Y_1, \ldots, X_n, Y_n, Q)$ be the polynomial obtained by inserting the same coordinates of $Q = \varphi(P)$ into the summation polynomial as in 2.1 (again these are only unique up to multiplication by a non-trivial constant).

We now prove the result by restriction to affine parts of $(\mathbb{P}^1_k)^n$.

Let for the moment $X_{i,1} := X_i$ and $X_{i,2} := Y_i$. Moreover, let for some multihomogeneous polynomial $F \in k[X_1, Y_1, \ldots, X_n, Y_n]$ $U_F := (\mathbb{P}^1_k)^n - V(F)$ be the corresponding open subscheme.

One can now show that for any $\underline{a} \in \{1, 2\}^n$, the restrictions of both schemes to $U_{X_{1,a_1}} \cap U_{X_{2,a_2}} \cap \cdots \cap U_{X_{n,a_n}}$ are equal; and this implies that the schemes are equal. For notational convenience we consider in the following the case of $\underline{a} = (2, \ldots, 2)$ ("dehomogenization with respect to $Y_1, \ldots, Y_n$"); the other cases can be established in exactly the same way.

Let $s(x_1, \ldots, x_n) := S'(x_1, 1, x_2, 1, \ldots, x_n, 1) \in K[x_1, \ldots, x_n]$. Then $H_Q \cap \mathbb{A}^n_k \subseteq \mathbb{A}^n_k = \mathrm{Spec}(k[x_1, \ldots, x_n])$ corresponds to the quotient ring $k[x_1, \ldots, x_n]/(s)$ of $k[x_1, \ldots, x_n]$.

As the formation of the Weil restriction commutes with base-change on the base, we have $(\mathrm{Res}^{(\mathbb{P}^1_K)^n}_{(\mathbb{P}^1_k)^n}(H_Q)) \cap \mathbb{A}^n_k = \mathrm{Res}^{\mathbb{A}^n_K}_{\mathbb{A}^n_k}(H_Q \cap \mathbb{A}^n_K)$ as closed subschemes of $\mathbb{A}^n_k$. A defining system of polynomials for $\mathrm{Res}^{\mathbb{A}^n_K}_{\mathbb{A}^n_k}(H_Q \cap \mathbb{A}^n_K)$ can be derived via the well-known method to obtain defining equations for Weil restrictions of affine schemes over rings (see example [Die01, Chapter 1] or the proof of [BLR80, §7.6., Theorem 4]):

Let $s^{(1)}, \ldots, s^{(n)} \in k[x_1, \ldots, x_n]$ be defined by the equation

$$\sum_j b_j \, s^{(j)} = s \; .$$

Then $\mathrm{Res}_{\mathbb{A}^n_k}^{\mathbb{A}^n_K}(H_Q \cap \mathbb{A}^n_K) = \mathrm{Spec}(k[x_1, \ldots, x_n]/(s^{(1)}, \ldots, s^{(n)})) = V(s^{(1)}, \ldots, s^{(n)}) \subset \mathbb{A}^n_k$. But the $s^{(j)}$ are exactly the dehomogenizations of the polynomials $S^{(j)}$, and thus $(X_{Q_{\circledcirc}}) \cap \mathbb{A}^n_k = (\mathrm{Res}_{(\mathbb{P}^1_k)^n}^{(\mathbb{P}^1_K)^n}(H_Q)) \cap \mathbb{A}^n_k = \mathrm{Res}_{\mathbb{A}^n_k}^{\mathbb{A}^n_K}(H_Q \cap \mathbb{A}^n_K) = V(s^{(1)}, \ldots, s^{(n)}) = V(S^{(1)}, \ldots, S^{(n)}) \cap \mathbb{A}^n_k$ as subschemes of $\mathbb{A}^n_k$. □

5.4 Determination of non-zero-dimensional fibers

We are interested in the number of points $Q \in \mathbb{P}^1(K)$ for which the fiber $X_{Q_{\circledcirc}} = p_2^{-1}(Q_{\circledcirc})$ is not zero-dimensional. For this we first consider a base change to K, such that X_K is a closed subscheme of $(\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^n$, and we perform explicit computations in the Chow ring of $(\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^n$. We identify for notational reasons $(\mathbb{P}^1)^n \times (\mathbb{P}^1)^n$ componentwise with $\prod_{i=1}^n \mathrm{Proj}(\mathbb{Z}[X_{1,i}, Y_{1,i}]) \times \prod_{i=1}^n \mathrm{Proj}(\mathbb{Z}[X_{2,i}, Y_{2,i}])$, and let $h_{\ell,i}$ be the class of $X_{\ell,i}$ in the Chow ring of $(\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^n$.

Lemma 5.13 *The class of X_K in $\mathrm{CH}((\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^n)$ is $2^{(n-1)\cdot n} \prod_{i=1}^n (h_{1,1} + \cdots + h_{1,n} + h_{2,i})$.*

Proof. X_K is defined inside $(\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^n$ by the polynomials

$$F_j := S_{\varphi,n+1}(X_{1,1}, Y_{1,1}, \ldots, X_{1,n}, Y_{1,n}, X_{2,j}, Y_{2,j})$$

for $j = 1, \ldots, n$. One can easily see with this explicit description that for all $\ell = 2, \ldots, n$ no irreducibility component of $V(F_1, \ldots, F_{\ell-1})$ is contained in $V(F_\ell)$.

Indeed, let C be an irreducibility component of $V(F_1, \ldots, F_{\ell-1})$. Then $C = C' \times (\mathbb{P}^1_K)^{n-\ell+1}$ for some $C' \subseteq (\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^{\ell-1}$. Let $(Q_1, Q_2) \in C'(\overline{K})$, where $Q_1 \in (\mathbb{P}^1)^n(\overline{K})$ and $Q_2 \in (\mathbb{P}^1)^{\ell-1}(\overline{K})$. Now there are at most 2^{n-1} points in $Q_3 \in \mathbb{P}^1(\overline{K})$ with $F_\ell(Q_1, Q_3) = 0$. Choose some $Q_3 \in \mathbb{P}^1(\overline{K})$ which is distinct from these points, and choose $Q_4 \in (\mathbb{P}^1)^{n-\ell}(\overline{K})$ arbitrarily. Then (Q_1, Q_2, Q_3, Q_4) is a $\overline{K}$-valued point of C which does not lie in $V(F_\ell)(\overline{K})$.

We therefore have $[X_K] = [V(F_1)] \cdots [V(F_n)]$ in the Chow ring of $(\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^n$ (cf. Remark 3.5). Moreover, $[V(F_i)] = 2^{n-1}(h_{1,1} + \cdots + h_{1,n} + h_{2,i})$. This gives the statement. □

Lemma 5.14 *The map $(p_2)_{|X}$ is surjective.*

Proof. There are two possible ways to prove this statement:

First, by the previous lemma and Lemma 3.8 we have $((p_2)_K)_{\circledcirc}([X_K]) = n! \cdot 2^{(n-1)\cdot n}$, thus $(p_2)_K(X_K)$ is equal to the ambient space $\prod_{i=1}^n \mathrm{Proj}(K[X_{2,i}, Y_{2,i}])$.

Second, Let $Q = (Q_1, \ldots, Q_n) \in \prod_{i=1}^n \mathrm{Proj}(K[X_{2,i}, Y_{2,i}])(\overline{K})$. Then the geometric fiber X_Q is the subscheme of $\prod_{i=1}^n \mathrm{Proj}(\overline{K}[X_{1,i}, Y_{1,i}])$ defined by $F_i(X_{1,1}, Y_{1,n}, \ldots, X_{1,n}, Y_{1,n}, Q_i)$ for $i = 1, \ldots, n$. We see in particular that the fiber is never empty. More precisely, if it is zero-dimensional then its degree is $n! \cdot 2^{(n-1)\cdot n}$. □

Remark 5.15 From the fact that $(p_2)_{|X}$ is surjective one can easily deduce that the map $a_n : V^n \longrightarrow \mathrm{Res}_k^K(E)$ is also surjective.

Let now $q_i : \prod_{i=1}^n (\mathrm{Proj}(K[X_{1,i}, Y_{1,i}])) \longrightarrow \mathrm{Proj}(K[X_{1,i}, Y_{1,i}])$ be the projection to the i^{th} component.

For some $Q \in \prod_{i=1}^n (\mathrm{Proj}(K[X_{2,i}, Y_{2,i}]))(\overline{K})$ the geometric fiber X_Q (which is contained in $\prod_{i=1}^n \mathrm{Proj}(\overline{K}[X_{1,i}, Y_{1,i}])$) is zero-dimensional if and only if for no $i = 1, \ldots, n$ the image of X_Q under q_i is equal to $\mathrm{Proj}(\overline{K}[X_{1,i}, Y_{1,i}])$.

Let $R_i \in K[X_{1,i}, Y_{1,i}, X_{2,1}, Y_{2,1}, \ldots, X_{2,n}, Y_{2,n}]$ be the multigraded resultant of $F_1, \ldots, F_n$ with respect to the variables $X_{1,1}, Y_{1,1}, \ldots, X_{1,i-1}, Y_{1,i-1}, X_{1,i+1}, Y_{1,i+1}, \ldots, X_{1,n}, Y_{1,n}$. Then for $Q = (Q_1, \ldots, Q_n) \in \prod_{i=1}^n \mathrm{Proj}(K[X_{2,i}, Y_{2,i}])(\overline{K})$ the geometric fiber X_Q is zero-dimensional if and only if for all $i = 1, \ldots, n$ $R_i(X_i, Y_i, Q_1, \ldots, Q_n)$ is non-trivial (cf. also the proof of Proposition 3.16).

Note now that not all fibers are non-zero-dimensional because X has dimension n (see Lemma 5.7) and $(\mathbb{P}_K^1)^n$ has dimension n too. Thus the polynomials $R_1, \ldots, R_n$ are all non-trivial.

Lemma 5.16 *Each polynomial R_i has multidegree $(n! \cdot 2^{(n-1)\cdot n}, (n-1)! \cdot 2^{(n-1)\cdot n}, \ldots, (n-1)! \cdot 2^{(n-1)\cdot n})$.*

Proof. The polynomials $F_1, \ldots, F_n$ have multidegree $(2^{n-1}, \ldots, 2^{n-1}) \in \mathbb{N}^{n-1}$ with respect to the variables under consideration. Therefore the corresponding generic resultant is homogeneous in the coefficients of each of the polynomials of degree $(n-1)! \cdot 2^{(n-1)^2}$. This implies that the degree with respect to $X_{2,i}, Y_{2,i}$ for some i is $(n-1)! \cdot 2^{(n-1)^2} \cdot 2^{n-1} = (n-1)! \cdot 2^{(n-1)\cdot n}$. Moreover, the degree with respect to $X_{1,i}, Y_{1,i}$ is $(n-1)! \cdot 2^{(n-1)^2} \cdot n \cdot 2^{n-1} = n! \cdot 2^{(n-1)\cdot n}$. □

Let us now for every $i = 1, \ldots, n$ fix some non-trivial coefficient C_i of R_i regarded as a polynomial in $K[X_{2,n}, Y_{2,n}, \ldots, X_{2,n}, Y_{2,n}][X_{1,i}, Y_{1,i}]$. Then clearly the points $Q \in \prod_{i=1}^n \prod \mathrm{Proj}(K[X_{2,i}, Y_{2,i}])$ for which the fiber X_Q is not zero-dimensional are contained in

$$\bigcup_{i=1}^n V(C_i) \subseteq (\mathbb{P}_K^1)^n .$$

Let us fix some $i = 1, \dots, n$. Then $V(C_i)$ is an effective Cartier divisor of multidegree $((n-1)! \cdot 2^{(n-1)\cdot n}, \dots, (n-1)! \cdot 2^{(n-1)\cdot n})$ in $\prod_{i=1}^n \operatorname{Proj}(K[X_{2,i}, Y_{2,i}])$, and $(p_2)_K^{-1}(V(C_i))$ is an effective Cartier divisor of multidegree $(0, \dots, 0, (n-1)! \cdot 2^{(n-1)\cdot n}, \dots, (n-1)! \cdot 2^{(n-1)\cdot n})$ in $(\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^n$.

It follows that

$$[X_K] \cdot [(p_2)_K^{-1}(V(C_i))] =$$
$$(n-1)! \cdot 2^{2(n-1)\cdot n} \cdot (\prod_{i=1}^n (h_{1,1} + \dots + h_{1,n} + h_{2,i})) \cdot (h_{2,1} + \dots + h_{2,n})$$

in $\mathrm{CH}((\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^n)$. With Lemma 3.8 this implies that

$$\begin{array}{rl} & ((p_1)_K)_{\circledcirc}([X_K] \cdot [(p_2)_K^{-1}(V(C_i))]) \\ = & (n-1)! \cdot 2^{2(n-1)\cdot n} \cdot n \cdot (h_{1,1} + \dots + h_{1,n}) \\ = & n! \cdot 2^{2(n-1)\cdot n} \cdot (h_{1,1} + \dots + h_{1,n}) \ . \end{array} \tag{9}$$

Assumption 5.17 Let us from now on assume that Condition 2.13 is satisfied.

Notation 5.18 Let $k = \mathbb{F}_q$ (such that $K = \mathbb{F}_{q^n}$).

Recall that X is now geometrically irreducible (Proposition 5.10). Clearly X_K is not contained in $(p_2)_K^{-1}(V(C_i))$ (because otherwise $(p_2)_K(X_K)$ would be contained in $V(C_i)$, contradicting the surjectivity of p_2). Thus we have $[X_K] \cdot [(p_2)_K^{-1}(V(C_i))] = [X_K \cap (p_2)_K^{-1}(V(C_i))]$ (cf. Remark 3.5). As the map $(p_1)_K : X_K \longrightarrow \prod_{i=1}^n \operatorname{Proj}([X_{1,i}, Y_{1,i}])$ is finite and flat (cf. Lemma 5.7), the dimension of $(p_1)_K(X_K \cap C_i)$ is equal to the dimension of $X_K \cap C_i$. With (9) we conclude:

Lemma 5.19 $(p_1)_K(X_K \cap C_i)$ *(with the induced reduced scheme structure) is a reduced effective Cartier divisor of* $\prod_{i=1}^n \operatorname{Proj}([X_{1,i}, Y_{1,i}])$ *whose multidegree is componentwise* $\leq (n! \cdot 2^{2(n-1)\cdot n}, \dots, n! \cdot 2^{2(n-1)\cdot n})$.

The subscheme

$$\bigcup_{i=1}^{n} \bigcup_{j=0}^{n-1} \sigma^j((p_1)_K(X_K \cap C_i))$$

of $\prod_{i=1}^n \operatorname{Proj}([X_{1,i}, Y_{1,i}])$ is $\mathrm{Gal}(K|k)$-invariant. It thus descends to a subscheme of $(\mathbb{P}^1_k)^n$; let B be this scheme.

Lemma 5.20

a) *B is a reduced effective Cartier divisor whose multidegree is componentwise* $\leq (n^2 \cdot n! \cdot 2^{2(n-1)\cdot n}, \dots, n^2 \cdot n! \cdot 2^{2(n-1)\cdot n})$.

b) Let $Q \in (\mathbb{P}^1(\overline{k}))^n - B(k)$, and let Q' be any preimage of Q under p_1. Then the fiber $X_{p_2(Q')}$ is zero-dimensional.

c) There are at most $n^3 \cdot n! \cdot 2^{2(n-1)\cdot n} \cdot (q+1)^{n-1}$ points in $B(k)$.

Proof. Let A_i be a multihomogeneous polynomial defining $(p_1)_K(X_K \cap C_i)$. Then B is $V(\prod_{j=0}^{n-1} \sigma^j(A_1 \cdots A_n))^{\mathrm{red}}$. The polynomial in question has a multidegree which is componentwise $\leq (n^2 \cdot n! \cdot 2^{2(n-1)\cdot n}, \ldots, n^2 \cdot n! \cdot 2^{2(n-1)\cdot n})$.

Statement b) follows immediately from the definition of B.

Statement c) follows from a) and the following lemma. □

Lemma 5.21 *Let H be an effective Cartier divisor of multidegree $\underline{d}$ in $(\mathbb{P}^1_k)^n$. Then*

$$\#H(k) \leq (\sum_{i=1}^{n} d_i) \cdot (q+1)^{n-1} \; .$$

Proof. It clearly suffices to show the result under the condition that all indices of the multidegree are positive.

We proceed with induction by n. For $n = 1$ the claim is that $\#H(k) \leq d_1$, and this is surely correct.

Now let H be defined by the polynomial $F(X_1, Y_1, \ldots, X_n, Y_n) \in k[X_1, Y_1, \ldots, X_n, Y_n]$. Let us consider the projection to the first $n-1$ components $(\mathbb{P}^1_k)^n \longrightarrow (\mathbb{P}^1_k)^{n-1}$ and the induced morphism $H \longrightarrow (\mathbb{P}^1_k)^{n-1}$. Now for every point $P = (P_1, \ldots, P_{n-1}) \in (\mathbb{P}^1_k)^{n-1}(k)$ for which $F(P_1, \ldots, P_{n-1}, X_n, Y_n)$ does not vanish, the fiber has degree d_n, thus in particular it contains at most d_n k-rational points. Let now C be a non-trivial coefficient of F regarded as a polynomial in $k[X_1, Y_1, \ldots, X_{n-1}, Y_{n-1}][X_n, Y_n]$. Then all points $P \in (\mathbb{P}^1_k)^{n-1}(k)$ for which $F(P_1, \ldots, P_{n-1}, X_n, Y_n)$ vanishes are contained in $V(C)$. Now C has multidegree $(d_1, \ldots, d_{n-1})$, and thus $\#V(C)(k) \leq (\sum_{i=1}^{n-1} d_i) \cdot (q+1)^{n-2}$ by induction. We conclude:

$$\begin{aligned} \#H(k) \; &\leq d_n \cdot (q+1)^{n-1} + \#V(C)(k) \cdot (q+1) \\ &\leq d_n \cdot (q+1)^{n-1} + (\textstyle\sum_{i=1}^{n-1} d_i) \cdot (q+1)^{n-1} \\ &= (\textstyle\sum_{i=1}^{n} d_i) \cdot (q+1)^{n-1} \end{aligned}$$

□

Given an element $P \in E(K)$, the decomposition algorithm succeeds when applied to P if and only if the fiber $X_{\varphi(P)_{\circledcirc}}$ is zero-dimensional and contains a k-rational point $(Q_1, \ldots, Q_n)$ such that there exist $P_1, \ldots, P_n \in E(K)$ with $\varphi(P_i) = Q_i$ and $\sum_i P_i = P$.

We want to derive a lower bound on the number of such elements $P \in E(K)$.

In [Die09], among other things we study the complexity of the elliptic curve discrete logarithm problem restricted to curves over extension fields with a *fixed* extension degree n. As a preperation for this, we we now proceed a bit more generally:

Given any subset M of $\{ (P_1, \ldots, P_n) \in E(K)^n \mid \varphi(P_i) \in \mathbb{P}^1(k)$ for all $i = 1, \ldots, n \}$, we want to derive a lower bound on the number of elements $P \in E(K)$ such that the decomposition algorithm succeeds and there exist $P_1, \ldots, P_n \in M$ with $\sum_i P_i = \pm P$.

Let us for this consider the commutative diagram of sets of k-valued points

$$\begin{tikzcd}
G(k) \arrow[r, "\rho"] & X(k) \arrow[d, "(p_1)_{|X}"] \\
V^n(k) \arrow[u, "\gamma"] \arrow[r, "\tau"] & \prod_{i=1}^n \mathrm{Proj}(k[X_{1,i}, Y_{1,i}])(k)
\end{tikzcd} ,$$

where the map $\gamma : V(k) \longrightarrow G(k)$ is induced by the graph morphism, that is, it is explicitly given by $(P_1, \ldots, P_n) \mapsto (P_1, \ldots, P_n, -\sum_i P_i)$, the map $\rho : G(k) \longrightarrow X(k)$ is induced by the morphism $G \longrightarrow X$ defined in Proposition 5.10, and the map $\tau : V^n(k) \longrightarrow \prod_{i=1}^n \mathrm{Proj}(k[X_{1,i}, Y_{1,i}])(k)$ is induced componentwise by the canonical morphism in diagram (6).

Note that under the scalar restriction functor and in the context of the index calculus algorithm for the Theorem, $V(k)$ corresponds to the factor base $\mathcal{F} = \{P \in E(K) \mid \varphi(P) \in \mathbb{P}^1(k)\}$, $G(k)$ corresponds to the set of tuples $(P_1, \ldots, P_n, P)$ with $\varphi(P_i) \in \mathbb{P}^1(k)$ and $P = -\sum_i P_i$, and $X(k)$ corresponds to the set of tuples $(Q_1, \ldots, Q_n, Q)$ with $Q_i \in \mathbb{P}^1(k)$ and $Q \in \mathbb{P}^1(K)$ and $S_{n+1}(Q_1, \ldots, Q_n, Q) = 0$. The map γ corresponds then to the map which is again given by $(P_1, \ldots, P_n) \mapsto (P_1, \ldots, P_n, -\sum_i P_i)$, and the maps ρ and τ correspond to the componentwise application of φ.

Let $M \subseteq \{(P_1, \ldots, P_n) \in E(K)^n \mid \varphi(P_i) \in \mathbb{P}^1(k)$ for all $i = 1, \ldots, n\}$, and let $M_{\circledcirc}$ be the corresponding subset of $V(k)$. Then every element $P \in E(K)$ such that $\varphi(P)_{\circledcirc} \in \mathrm{Res}_k^K(\mathbb{P}^1_K)(k)$ is the image under p_2 of an element in $(\rho \circ \gamma)(M_{\circledcirc}) - p_1^{-1}(B(k))$ is an element as desired. (Indeed, if P is such an element, first the fiber $X_{\varphi(P)_{\circledcirc}}$ is zero-dimensional by Lemma 5.20 b), and second there exist $P_1, \ldots, P_n \in M$ with $\varphi(P_1 + \cdots + P_n) = \varphi(P)$, thus $P_1 + \cdots + P_n = \pm P$.)

We are thus interested in the cardinality of the set

$$p_2\big((\rho \circ \gamma)(M_{\circledcirc}) - p_1^{-1}(B(k))\big) .$$

For this we first derive a lower bound on

$$(\rho \circ \gamma)(M_{\circledcirc}) - p_1^{-1}(B(k)) .$$

The image of this set in $\prod_{i=1}^n \operatorname{Proj}(k[X_{1,i}, Y_{1,i}])(k)$ is contained in

$$\tau(M_{\circledcirc}) - B(k) \ .$$

As τ corresponds to the componentwise application of φ, we have $\#\tau(M_{\circledcirc}) \geq \frac{1}{2^n}\#M_{\circledcirc} = \frac{1}{2^n}\#M$.

With Lemma 5.20 c) we obtain:

$$\begin{aligned} & \#((\rho \circ \gamma)(M) - p_1^{-1}(B(k))) \\ \geq \ & \#(\tau(M_{\circledcirc}) - B(k)) \\ \geq \ & \tfrac{\#M}{2^n} - n^3 \cdot n! \cdot 2^{2(n-1)\cdot n} \cdot (q+1)^{n-1} \ . \end{aligned} \tag{10}$$

Now if an element Q in the set $p_2((\rho\circ\gamma)(V^n(k)) - p_1^{-1}(B(k)))$ is given, the fiber of $p_2(Q)$ under p_2 is zero-dimensional, and thus its degree is $n! \cdot 2^{(n-1)\cdot n}$ (see the proof of Lemma 5.14). We therefore have the following proposition.

Proposition 5.22 *Let*

$$M \subseteq \{(P_1, \ldots, P_n) \in E(K)^n \mid \varphi(P_i) \in \mathbb{P}^1(k) \textit{ for all } i = 1, \ldots, n\} \ .$$

Then the number of elements $P \in E(K)$ such that the decomposition algorithm succeeds and there exist $P_1, \ldots, P_n \in M$ with $P_1 + \cdots P_n = \pm P$ is

$$\geq \frac{\#M - n^3 \cdot 2^{2n^2-n} \cdot (q+1)^{n-1}}{n! \cdot 2^{n^2}} \ .$$

We now apply this proposition with $M = V(k)$. As mentioned in Remark 5.5 for $\log_2(q) \geq 3n$ and n large enough we have $\#V(k) \geq \frac{q+1}{2}$, thus $\#V^n(k) \geq \frac{(q+1)^n}{2^n}$. With Proposition 5.22 we obtain that the number of elements $P \in E(K)$ such that there exist $P_1, \ldots, P_n \in E(K)$ with $\varphi(P_i) \in \mathbb{P}^1(k)$ and $\sum P_i = P$ is

$$\geq \frac{(q+1)^{n-1}}{n! \cdot 2^{n\cdot(n+1)}} \cdot (q + 1 - n^3 \cdot 2^{2n^2}) \ .$$

Let now $\epsilon > 0$. Then for n large enough this is

$$\geq \frac{q^{n-1}}{n! \cdot 2^{n\cdot(n+1)}} \cdot (q - \frac{1}{2} \cdot 2^{(2+\epsilon)\cdot n^2}) \ .$$

Then for $\log_2(q) \geq (2+\epsilon) \cdot n^2$ this is

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

Again for n large enough and $\log_2(q) \geq (2+\epsilon)\cdot n^2$ this is

$$\geq 2 \cdot q^{n-\frac{1}{2}} \ .$$

We therefore have:

Proposition 5.23 *Let $\epsilon > 0$. Then for n large enough and $(2+\epsilon)\cdot n^2 \leq \log_2(q)$ there are at least $2 \cdot q^{n-\frac{1}{2}}$ elements in $E(K)$ for which the decomposition algorithm succeeds.*

And this implies Proposition 2.7, the main result for the analysis of the algorithm in subsection 2.2:

Proposition 5.24 *Let $\epsilon > 0$. Then for n large enough and $(2+\epsilon)\cdot n^2 \leq \log_2(q)$ the following holds: Let $E/\mathbb{F}_{q^n}$ be an elliptic curve, and let φ be chosen such that Condition 2.13 holds. Then the probability that the decomposition algorithm succeeds if applied to a uniformly randomly distributed element in $E(\mathbb{F}_{q^n})$ is $\geq q^{-\frac{1}{2}}$.*

References

[BLR80] S. Bosch, W. Lütkebohmert, and W. Raynaud. *Néron Models.* Springer-Verlag, 1980.

[CLO05] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer, 2005.

[CZ81] D. Cantor and H. Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Math. Comp.*, 154:587–592, 1981.

[Die01] C. Diem. *A study on theoretical and practical aspects of Weil-restrictions of varieties.* PhD thesis, University of Essen, 2001.

[Die09] C. Diem. On the discrete logarithm problem in class groups of curves. Conditionally accepted for publication at Math. Comp., available under http://www.math.uni-leipzig.de/∼diem, 2009.

[EG02] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta. Arith.*, 102:83–103, 2002.

[FR94] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm problem in divisor class groups. *Math. Comp.*, 62:865–874, 1994.

[Ful93] W. Fulton. *Introduction to Toric Varieties.* Princeton University Press, 1993.

[Gau09] P. Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *J. Symbolic Computation*, 2009. In press.

[GKZ94] I. Gelfand, M. Kapranov, and A. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants.* Birkäuser, 1994.

[Gro61] A. Grothendieck. Eléments de Géométrie Algébrique III, Première Partie. *Publication Mathématiques*, 11, 1961.

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

[KR89] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284:307–327, 1989.

[KSZ92] M. Kapranov, B. Sturmfels, and A. Zelevinsky. Chow polytopes and general resultants. *Duke Math. Journal*, 67:226–263, 1992.

[LP92] H.W. Lenstra and C. Pomerance. A rigorous time bound for factoring integers. *J. Amer. Math. Soc.*, 5, 1992.

[Mat89] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, 1989.

[MOV93] A. Menezes, T. Okomoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in finite fields. *IEEE Transactions on Information Theory*, 39:1639–1646, 1993.

[Mum65] D. Mumford. *Geometric Invariant Theory.* Springer-Verlag, 1965.

[RS62] J. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6(64-94), 1962.

[Sch85] R. Schoof. Elliptic curves over finite fields and the compuation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.

[Sem98] I. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Comp.*, 67:353–356, 1998.

[Sem04] I. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. available under http://eprint.iacr.org/2004/031, Feb. 2004.

[Sil86] J. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[Sti93] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer-Verlag, 1993.

[SZ94] B. Sturmfels and A. Zelevinsky. Multigraded Resultants of Sylvester Type. *J. Algebra*, 163:115–127, 1994.

Claus Diem
Universität Leipzig
Mathematisches Institut
Johannisgasse 26
04103 Leipzig
Deutschland
diem@math.uni-leipzig.de