COMPOSITIO MATHEMATICA

On the discrete logarithm problem in elliptic curves

Claus Diem

Compositio Math. **147** (2011), 75–104.

doi:10.1112/S0010437X10005075

FOUNDATION
COMPOSITIO
MATHEMATICA

The London Mathematical Society

Compositio Math. 147 (2011) 75–104
doi:10.1112/S0010437X10005075

On the discrete logarithm problem in elliptic curves

Claus Diem

Dedicated to Gerhard Frey

Abstract

We study the elliptic curve discrete logarithm problem over finite extension fields. We show that for any sequences of prime powers $(q_i)_{i\in\mathbb{N}}$ and natural numbers $(n_i)_{i\in\mathbb{N}}$ with $n_i \longrightarrow \infty$ and $n_i/\log(q_i) \longrightarrow 0$ for $i \longrightarrow \infty$, the elliptic curve discrete logarithm problem restricted to curves over the fields $\mathbb{F}_{q_i^{n_i}}$ can be solved in subexponential expected time $(q_i^{n_i})^{o(1)}$. We also show that there exists a sequence of prime powers $(q_i)_{i\in\mathbb{N}}$ such that the problem restricted to curves over $\mathbb{F}_{q_i}$ can be solved in an expected time of $e^{\mathcal{O}(\log(q_i)^{2/3})}$.

Contents

1. Introduction

The classical discrete logarithm problem in finite prime fields can be solved in an expected time which is subexponential in the bit-length of 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 bit-length of 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 over prime fields), it was up until 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 the following results. Here and in the following, q is always a prime power and n a natural number.

(i) Let sequences of prime powers $(q_i)_{i\in\mathbb{N}}$ and natural numbers $(n_i)_{i\in\mathbb{N}}$ with $n_i \longrightarrow \infty$ and $n_i/\log(q_i) \longrightarrow 0$ for $i \longrightarrow \infty$ be given. Then the discrete logarithm problem in the groups of

Received 12 April 2009, accepted in final form 28 April 2010, published online 15 October 2010.
2000 Mathematics Subject Classification 11Y16 (primary), 14G15, 14G50, 68Q24 (secondary).
Keywords: elliptic curves, discrete logarithm problem.

rational points of elliptic curves over the fields $\mathbb{F}_{q_i^{n_i}}$ can be solved in an expected time of

$$(q_i^{n_i})^{o(1)}.$$

(ii) Let $\beta \in [\frac{1}{2}, 1)$ and $a, b > 0$ be fixed. Let

$$\alpha := \frac{1-\beta}{2\beta} = \frac{1}{2} \cdot \left(\frac{1}{\beta} - 1\right) \in \left(0, \frac{1}{2}\right] \quad \text{and} \quad \gamma := \frac{2\beta}{\beta+1} = 2 \cdot \left(1 - \frac{1}{\beta+1}\right) < 1.$$

Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{q^n}$ with

$$a \cdot \log(q)^\alpha \leqslant n \leqslant b \cdot \log(q)^\beta$$

can be solved in an expected time of

$$e^{\mathcal{O}(\log(q^n)^\gamma)}.$$

(iii) Let 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

$$a \cdot \sqrt{\log(q)} \leqslant n \leqslant b \cdot \sqrt{\log(q)}$$

can be solved in an expected time of

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

Note that, in result (ii), γ as a function of β is strictly monotonically increasing from $\frac{2}{3}$ for $\beta = \frac{1}{2}$ to 1 in the limit, and α is strictly monotonically decreasing from $\frac{1}{2}$ to 0 in the limit. Result (iii) is a special case of result (ii) for $\alpha = \beta = \frac{1}{2}$.

Our main result is the following theorem.

THEOREM. *The discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{q^n}$ can be solved in an expected time of*

$$e^{\mathcal{O}(\max(\log(q), n^2))}.$$

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.

Given the theorem, it is easy to establish results (i) and (ii) (and therefore also result (iii)) above. Result (i) follows immediately, and a proof of result (ii) is as follows.

Let α, β, γ and a, b as in result (ii) be given. Note that $\beta = 1/(2\alpha+1)$ and $\gamma = 1/(\alpha+1)$. Now first, as $a \cdot \log(q)^\alpha \leqslant n$, we have $\log(q) = \log(q)^{\gamma\cdot(\alpha+1)} \leqslant (1/a \cdot \log(q) \cdot n)^\gamma = 1/a^\gamma \cdot (\log(q^n))^\gamma$. Second, as $n \leqslant b \cdot \log(q)^\beta$, we have $n^2 = n^{\gamma\cdot(1+(1/\beta))} \leqslant (n \cdot b^{1/\beta} \cdot \log(q))^\gamma = b^{\gamma/\beta} \cdot (\log(q^n))^\gamma$.

The method: index calculus. Index calculus is originally a method to compute discrete logarithms (or indices in the classical terminology) in the multiplicative groups of finite prime fields. It can 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 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 at most 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.

https://doi.org/10.1112/S0010437X10005075

A similar method can also be used to compute discrete logarithms in other finite groups: if one considers the multiplicative groups of finite fields of a fixed characteristic, one substitutes prime numbers by irreducible polynomials whose degree is below a certain bound. If one considers the degree zero class groups of curves over a fixed finite field, one proceeds similarly, substituting polynomials by effective divisors and irreducible polynomials by prime divisors.

It is common to use the term index calculus to refer to the general method of computing discrete logarithms by relation generation and linear algebra. The algorithm for the theorem is also based on this method. However, in contrast to the algorithms mentioned above, the factor base is defined in an *algebraic* rather than an *arithmetic* way; in particular, 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 $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_{q^n}}$ of degree two which satisfies $\varphi \circ [-1] = \varphi$ as well as a certain additional condition (Condition 2.7). The factor base is then given by

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

The relation generation relies on an algorithm which we call a 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 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 $i = 1, \ldots, n$ such that

$$P_1 + \cdots + P_n = P.$$

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 $(P_1, \ldots, P_n)$. However, it might also fail 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. 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 2004 Igor 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 $m \in \mathbb{N}$, $m \geqslant 2$. Let $\overline{K}$ be an algebraic closure of K. Then the mth summation polynomial as defined by Semaev is an irreducible polynomial $f \in K[x_1, \ldots, x_m]$ such that 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 $\overline{K}$. These summation polynomials have degree 2^{m-2} in each variable.

https://doi.org/10.1112/S0010437X10005075

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 led both Pierrick Gaudry and the author to reflect on the question of whether a similar approach over extension fields might not give algorithms which are asymptotically faster than generic algorithms for certain input classes.

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

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

on a randomized random access machine.[1] The current author, on the other hand, tried to see whether 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 become subexponential, and this study finally led 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.

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 a 'decomposition algorithm' followed by the computation of a suitable covering φ and finally the index calculus algorithm for the theorem. In § 3 we introduce homogeneous summation polynomials via a geometric approach. In the last section we give some geometric background on the decomposition algorithm and its analysis.

Notation and terminology. We set $\mathbb{N} := \{1, 2, 3, \ldots\}$ and $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$.

An 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.

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

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

https://doi.org/10.1112/S0010437X10005075

Products of projective lines play an important role in this work. We set $\mathbb{P}^1 := \mathrm{Proj}(\mathbb{Z}[X, Y])$ and $x := X/Y$. 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 ith 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 $x_i := X_i/Y_i$ 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 $x := X/Z$, $y := Y/Z$. 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 sets $\mathcal{O}(f)$ and $\tilde{\mathcal{O}}(f)$ of functions $S \longrightarrow \mathbb{R}$. Additionally, we define the set of functions which are polynomially bounded in f as

$$\mathcal{P}oly(f) := \{g : S \longrightarrow \mathbb{R} : \exists c > 0, N \in \mathbb{N} : \forall n \in S \text{ with } n \geqslant N : |g(n)| \leqslant f(n)^c\}.$$

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 (for example, elliptic curves etc.) by bit-strings, as usual.

2. The key algorithms

In this section we outline the algorithm for the theorem.

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 § 3; here we merely mention the key results which are needed to describe the decomposition algorithm.

In § 3 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 two with $\varphi \circ [-1] = \varphi$. Let $m \in \mathbb{N}$ with $m \geqslant 2$. 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 mth *summation polynomial of E with respect to φ*.

Proposition 2.3. *Given an elliptic curve E in Weierstraß form over a finite field $\mathbb{F}_q m \in \mathbb{N}$ with $m \geqslant 2$ and $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$ of degree two with $\varphi \circ [-1] = \varphi$, the mth summation polynomial*

https://doi.org/10.1112/S0010437X10005075

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 two 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 $(n+1)$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, similarly to $S_{\varphi,n+1}$ 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.

(i) There exist $P_1, \ldots, P_n \in E(\overline{K})$ such that $P_1 + \cdots + P_n = P$ and $\varphi(P_i) = Q_i$ for all $i = 1, \ldots, n$.

(ii) $S_{\varphi,n+1}(Q_1, \ldots, Q_n, \varphi(P)) = 0$.

(iii) 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 $V(S^{(1)}, \ldots, S^{(n)})$.

DEFINITION 2.4. A tuple $(P_1, \ldots, P_n) \in E(K)^n$ with $P_1 + \cdots + P_n = P$ and $\varphi(P_i) \in \mathbb{P}^1(k)$ for $i = 1, \ldots, n$ is called a *decomposition* of P with respect to φ. Let such a decomposition be given and let $Q_i := \varphi(P_i)$. Now if $(Q_1, \ldots, Q_n)$ is an isolated point of $V(S^{(1)}, \ldots, S^{(n)})$, the decomposition is said to be *φ-isolated*.

The 'decomposition problem' is now 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 $P \in E(\mathbb{F}_{q^n})$ of degree two with $[-1] \circ \varphi = \varphi$, output a list of decompositions of P with respect to φ containing all φ-isolated decompositions. A 'decomposition algorithm' is then a randomized algorithm for this problem.

We now outline such an algorithm. The basis is the following proposition.

PROPOSITION 2.5. (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 $d \in \mathbb{N}$. Then 'with multiplicities', there are at most $n! \cdot d^n$ isolated points in $V(F_1, \ldots, F_n)$. Or with other words: the degree of the degree zero part of the cycle defined by $V(F_1, \ldots, F_n)$ is at most $n! \cdot d^n$. Equality holds if and only if the scheme is zero-dimensional.*

(b) *There exists a randomized algorithm with the following specification: 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 $(d, d, \ldots, d)$*

https://doi.org/10.1112/S0010437X10005075

for some $d \in \mathbb{N}$ and prime power q, the algorithm outputs a list of $\mathbb{F}_q$-rational points of $V(F_1, \ldots, F_\ell)$ containing all $\mathbb{F}_q$-rational isolated points. Moreover, the expected running time is in $\mathcal{P}oly(n! \cdot d^n \cdot \log(q))$, and the list has a size of $\mathcal{P}oly(n! \cdot d^n)$.

Sketch of a proof. Part (a) follows from intersection theory in $(\mathbb{P}^1_k)^n$. For background information, we give a more general statement in § 4.2 (Lemma 4.7).

The computational statement can be obtained via an algorithm by Rojas [Roj99] and the factorization of a univariate polynomial. This algorithm relies on 'twisted Chow forms' or, as one might also say, on U-resultants of toric deformations. We note here that the use of twisted Chow forms for polynomial system solving was pioneered by Canny [Can90].

Let $k = \mathbb{F}_q$, and let $(\mathbb{G}_m)_k = \mathbb{A}^1_k - \{0\}$ be the one-dimensional standard torus over k. Then, given $F_1, \ldots, F_n$ as above, with the algorithm by Rojas and the factorization of a univariate polynomial, one can obtain a list of $\mathbb{F}_q$-rational points of $V(F_1, \ldots, F_\ell) \cap ((\mathbb{G}_m)_k)^n$ containing all $\mathbb{F}_q$-rational isolated points. The expected running time is in $\mathcal{P}oly(n! \cdot d^n \cdot \log(q))$, and the list has size at most $n! \cdot d^n$.

Now $\mathbb{P}^1_k$ can be covered by two copies of $(\mathbb{G}_m)_k$. Therefore, by applying Rojas' algorithm 2^n-times with different coordinates on the n factors of $(\mathbb{P}^1_k)^n$ one can obtain a list of points which contains all $\mathbb{F}_q$-rational points. □

We then 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 $\mathcal{P}oly(e^{n^2} \cdot \log(q))$. We then apply an algorithm as in the previous proposition. (As the polynomials are symmetric, we only have to apply Rojas' algorithm n instead of 2^n times.) Let L be the list output by this algorithm.

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 entries of L. For each such entry $(Q_1, \ldots, Q_n)$ we consider all possible tuples $(P_1, \ldots, P_n) \in E(\mathbb{F}_{q^n})^n$ with $\varphi(P_i) = Q_i$ 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 $(Q_1, \ldots, Q_n) \in L$ 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 $(Q_1, \ldots, Q_n)$. The expected total running time is then still in $\mathcal{P}oly(e^{n^2} \cdot \log(q))$.

We obtain the following proposition.

Proposition 2.6. *There exists a decomposition algorithm which operates in an expected time of $\mathcal{P}oly(e^{n^2} \cdot \log(q))$.*

In order to analyze the index calculus algorithm we need a lower bound on the probability that a uniformly randomly distributed point has a φ-isolated decomposition. In order to derive such a lower bound, we need the following condition on the covering φ.

Condition 2.7. There exists a point $R \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ which is a ramification point of φ such that the points $R, \sigma(R), \ldots, \sigma^{n-1}(R)$ are all distinct and φ is unramified at $\sigma(R), \ldots, \sigma^{n-1}(R)$.

Here and in what follows, σ is the relative Frobenius automorphism of $\overline{k}|k$.

In the next subsection we prove the following proposition.

https://doi.org/10.1112/S0010437X10005075

PROPOSITION 2.8. *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 two with $\varphi \circ [-1] = \varphi$ satisfying Condition 2.7 in an expected time of $\mathcal{P}oly(n \cdot \log(q))$.*

The key result for the analysis of the algorithm for the theorem is now as follows.

PROPOSITION 2.9. *Let $\epsilon > 0$. Then for n large enough*[2] *and $(2+\epsilon) \cdot n^2 \leqslant \log_2(q)$ 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 two with $\varphi \circ [-1] = \varphi$ such that Condition 2.7 is satisfied.*

Then the probability that a uniformly distributed point of $E(\mathbb{F}_{q^n})$ has a φ-isolated decomposition is at least $q^{-\frac{1}{2}}$.

Section 4 is devoted to the proof of this proposition.

2.2 Computing a suitable covering

We discuss how a covering $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_{q^n}}$ satisfying Condition 2.7 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 $\varphi := \alpha \circ x_{|E}$.

2.2.1 *Even characteristic.* First, let $j(E) = 0$. Then by an easy coordinate change the 'affine part' of E is defined by a polynomial

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

with $a_3 \neq 0$ (see [Sil86, Appendix A]). Now $x_{|E}$ is ramified exactly over ∞. We set $\alpha := (ax-1)/x$ 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.

Now let $j(E) \neq 0$. Then wlog. 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.

2.2.2 *Odd characteristic.* Now wlog. the 'affine part' of E is defined by

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

where $f(x) \in \mathbb{F}_{q^n}[x]$ is monic of degree three. 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 2.8 now follows from the following lemma. (Note that we only apply the lemma in the case that q is odd.)

[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 $n \geqslant C$.

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

https://doi.org/10.1112/S0010437X10005075

Lemma 2.10. *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 at least 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 $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}, \lambda \mapsto \lambda^{q^i} - \lambda$ 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 that 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 $3\sum_{i=1}^{n-1} q^{\gcd(i,n)} \leqslant 3(n-1) \cdot q^{n/2}$, and therefore the probability in question is

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

For $n \geqslant 10$ this is at least $\frac{5}{32} > 0$.

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

2.3 The index calculus algorithm

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

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

This proposition implies the theorem:

Let an instance consisting of a prime power q, a natural number n, an elliptic curve E over $\mathbb{F}_{q^n}$ and two points $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$ be given.

We then proceed with a case distinction.

If $3 \cdot n^2 \leqslant \log_2(q)$, we apply an algorithm for Proposition 2.11. Thus for these instances we obtain an expected running time which is polynomially bounded in $q = e^{\log(q)}$.

If, on the other hand, $3 \cdot n^2 > \log_2(q)$, we set $m := \lceil (3 \cdot n^2)/\log_2(q) \rceil$. Note that $3 \cdot n^2 \leqslant \log_2(q^m)$ and $m \leqslant (6 \cdot n^2)/\log_2(q)$. We then apply an algorithm for Proposition 2.11 to the instance consisting of the prime power q^m, the natural number n, the elliptic curve $E_{\mathbb{F}_{q^{mn}}}$ over $\mathbb{F}_{q^{mn}}$ and $A, B \in E(\mathbb{F}_{q^{mn}})$. Thus for these instances the expected running time is then polynomially bounded in $q^m \leqslant q^{(6 \cdot n^2)/\log_2(q)} = 2^{6n^2} \in \mathcal{P}oly(e^{n^2})$.

In the theorem, only q^n but not q and n is part of the input. We can then apply the algorithm just outlined for all possible extension degrees 'in parallel'. The claimed expected running time still holds.

https://doi.org/10.1112/S0010437X10005075

We now outline an algorithm for Proposition 2.11. For any $\epsilon > 0$, the algorithm below computes the discrete logarithm in any expected time of $\mathcal{P}oly(q)$ provided that n is *large enough*. Proposition 2.11 can then be obtained by applying this algorithm 'in parallel' with a brute force computation.

The algorithm

Input: A prime power q, a natural number n with $(q,n) \neq (3,2)$, an elliptic curve E over $\mathbb{F}_{q^n}$ in Weierstraß form, $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$.

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

1. Compute $N \longleftarrow \#E(\mathbb{F}_{q^n})$.
2. Compute the factorization of N.
3. Compute a generating system C_1, C_2 of $E(\mathbb{F}_{q^n})$.
4. Choose a covering $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_{q^n}}$ of degree two with $\varphi \circ [-1] = \varphi$ satisfying Condition 2.7.
5. Construct the factor base $\mathcal{F} = \{F_1, F_2, \ldots, F_k\}$, that is, enumerate the set $\{P \in E(\mathbb{F}_{q^n}) \mid \varphi(P) \in \mathbb{P}^1(\mathbb{F}_q)\}$.
6. Construct matrices $R \in (\mathbb{Z}/N\mathbb{Z})^{(k+3)\times k}$ and $S \in (\mathbb{Z}/N\mathbb{Z})^{(k+3)\times 2}$ as well as vectors $\underline{\alpha}, \underline{\beta} \in (\mathbb{Z}/N\mathbb{Z})^{k+3}$ as follows:
   For $i = 1, \ldots, k+3$ do
   Repeat
   Choose uniformly and independently randomly $\alpha, \beta, s_1, s_2 \in \mathbb{Z}/N\mathbb{Z}$ and apply a decomposition algorithm to $s_1 C_1 + s_2 C_2 + \alpha A + \beta B$.
   Until a decomposition is obtained. Choose such a decomposition and let
   $$\sum_j r_{i,j} F_j = s_{i,1} C_1 + s_{i,2} C_2 + \alpha_i A + \beta_i B$$
   be the relation generated.
7. 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.
8. If $\beta_1' \in (\mathbb{Z}/N\mathbb{Z})^*$, let $\xi := -\alpha_1'/\beta_1'$, otherwise go back to Step 6.
9. Compute $\mathrm{ord}(A)$, using the factorization of N.
10. 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 $(k+3) \times (k+2)$-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 2 can be performed in an expected time of $\mathcal{P}oly(\exp((\log(N) \cdot \log(\log(N)))^{1/2}))$, for example with the algorithm by Lenstra and Pomerance [LP92].

Step 3 can be performed in expected polynomially bounded time with an algorithm by Miller [Mil04]. Briefly, one chooses two points uniformly at random and checks whether they form a generating system by computing the Weil pairing of the two points. For the claimed expected running time, one needs the factorization of N.

As already proven above, for $(q, n) \neq (3, 2)$, Step 4 can be performed in expected polynomially bounded time.

In Step 5, the factor base clearly has at most $2(q+1)$ elements and can therefore be constructed in an expected time of $\mathcal{P}oly(n \cdot \log(q)) \cdot q$.

Step 9 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 $L_i := N/\ell_i^{e_i}$, 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 Steps 6–8.

Step 6: Relation generation. As stated, we choose $\alpha, \beta, s_1, s_2 \in \{0, \ldots, \#E(\mathbb{F}_{q^n}) - 1\}$ uniformly at random and compute $s_1 C_1 + s_2 C_2 + \alpha A + \beta B$. Then we apply the decomposition algorithm as described in the previous subsection to this element and the covering φ.

We repeat this procedure until the decomposition algorithm outputs at least one decomposition of $s_1 C_1 + s_2 C_2 + \alpha A + \beta B$. Then we choose such a decomposition in such a way that the choice depends only on the element $s_1 C_1 + s_2 C_2 + \alpha A + \beta B$ and not on the further internal state of the algorithm.

The time to compute $s_1 C_1 + s_2 C_2 + \alpha A + \beta B$ is polynomial in $\log(q^n)$. By Proposition 2.6, 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 $s_1 C_1 + s_2 C_2 + \alpha A + \beta B$ is uniformly randomly distributed (and independent of previous choices). Therefore by Proposition 2.9 for instances with $(2+\epsilon) \cdot n^2 \leqslant \log_2(q)$ 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 $(2+\epsilon) \cdot n^2 \leqslant \log_2(q)$ and n large enough, 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 7: 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 $k + 2 \in \mathcal{O}(q)$. We therefore have a running time which is polynomially bounded in $q \cdot \log(N)$.

Step 8: Invertibility. We need to estimate the probability that β_1' is invertible. The key result is the following proposition.

Proposition 2.12. *Conditionally to any outcome of Step 5 of the algorithm, the random element β_1' is uniformly randomly distributed in $\mathbb{Z}/N\mathbb{Z}$.*

For $N \longrightarrow \infty$, we have $\phi(N)/N \in \Omega(1/\log\log(N))$ (cf. [RS62, Formula 3.41]). Therefore, the expected number of iterations of Steps 6–8 is in $\mathcal{O}(\log\log(N)) = \mathcal{O}(\log\log(q))$.

Proof of Proposition 2.12. We fix any outcome of Step 5 of the algorithm. Now, for each i, β_i is stochastically independent of $\alpha_i A + \beta_i B$. Therefore β_i is stochastically independent of the ith 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 $[\underline{u}]_\ell \neq \underline{0}$ 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 2.13. *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 then follows easily with the Chinese remainder theorem. □

The overall running time. Altogether we conclude as follows.

We again restrict ourselves to instances with $(2+\epsilon)\cdot n^2 \leqslant \log_2(q)$. 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.

3. 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 $m \in \mathbb{N}$, $m \geqslant 2$, and let $\varphi : E \longrightarrow \mathbb{P}^1_k$ be a covering of degree two 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 3.1. 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).

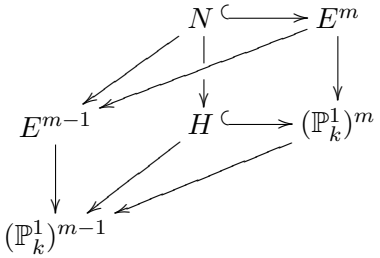
PROPOSITION 3.2. (a) *The induced map $N/[-1] \longrightarrow H$ is finite and birational.*

(b) *H is a hypersurface 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



where the vertical maps are induced by the covering φ and 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

https://doi.org/10.1112/S0010437X10005075

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 two, 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 two, the induced map $N/[-1] \longrightarrow H$ generically has degree one, 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 the function fields $k(N)|k(H)$ has separability degree two.

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 ith coordinate, and let $P_i \in E(\Omega)$ be the induced points. (That is, P_i is the morphism $\mathrm{Spec}(\Omega) \longrightarrow \mathrm{Spec}(k(E^{m-1})) \longrightarrow E^{m-1} \xrightarrow{p_i} E$, 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 $\mathrm{Mor}_k(E^{m-1}, E) \longrightarrow E(k(E^{m-1}))$ is injective (in fact, it is an isomorphism), and the map $E(k(E^{m-1})) \longrightarrow \mathrm{Spec}(\Omega)$ is injective too.

Now let us consider the preimage of $\varphi(P_1, \ldots, P_m) = (\varphi \circ P_1, \ldots, \varphi \circ P_m) \in H(\Omega)$ 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 as follows: there are exactly two Ω-valued points of E^{m-1} which induce the Ω-valued point $(\varphi \circ P_1, \ldots, \varphi \circ P_m) \in H(\Omega)$ 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 two.

We come to part (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}. In 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 $(\mathbb{P}^1)^{m-1}_k$, thus it is, 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 mth 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 3.3. Let $\alpha \in \mathrm{Aut}(\mathbb{P}^1_k)$. Then $H_{\alpha\circ\varphi,m} = \alpha(H_{\varphi,m})$ or, in 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 [Sem04].

LEMMA 3.4. *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 third summation polynomial of E with respect to $x_{|E}$ is

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

Sketch of a 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 $P_1, P_2 \in E(\bar{k})$, we have $S(x(P_1), x(P_2), x(P_1 + P_2)) = 0$. 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 $S(x(P_1), x(P_2), x(P_1 + P_3)) = 0$ 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 $P_1, P_2 \in E(\bar{k})$ 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 $(x - x(P_1 + P_2))(x - x(P_1 - P_2))$. 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 [BCP97]. The polynomial S is then obtained by multiplication with the denominator and homogenization.

LEMMA 3.5. *Let E still be an elliptic curve and let $\varphi : E \longrightarrow \mathbb{P}^1_k$ be a covering of degree two with $\varphi \circ [-1] = \varphi$. Let $s, t \in \mathbb{N}$ with $s, t \geqslant 2$. Then*

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

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

It follows that topologically the hypersurface 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. □

https://doi.org/10.1112/S0010437X10005075

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 two $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$ 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 3.4 and Remark 3.3.

Further, one can compute $S_{\varphi,m}$ for $m \geqslant 3$ 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 $q \geqslant 2^{m-2}$ (which means that $\#\mathbb{P}^1(\mathbb{F}_q) \geqslant 2^{m-2}+1$). For completeness we give here the interpolation result we apply.

Proposition 3.6 (Multihomogeneous interpolation). (a) *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 $(a_{i,j}, b_{i,j}) \in k^2 - \{0\}$ 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 $F(a_{1,j_1}, b_{1,j_2}, \ldots, a_{n,j_n}, b_{n,j_n}) = c_{\underline{j}}$ for all $\underline{j} \in S$.*

(b) *Given a prime power q and elements as above over $k = \mathbb{F}_q$, the interpolating polynomial F can be computed in a time of $\mathcal{P}oly((d_1+1)\cdots(d_n+1)\cdot\log(q))$.*

Proof. Let us first consider the classical one-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 $L_j := \prod_{\ell \neq j}(b_\ell X - a_\ell Y)/(a_j b_\ell - a_\ell b_j)$ we have $F = \sum_j c_j L_j$.

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, by the induction hypothesis, for each $j = 1, \ldots, d_n+1$, we have $F(X_1, Y_1, \ldots, X_{n-1}, Y_{n-1}, a_{n,j}, b_{n,j}) = 0 \in k[X_1, Y_1, \ldots, X_{n-1}, Y_{n-1}]$. 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 one-dimensional interpolation problem, we conclude that $F = 0$.

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

For each $j = 1, \ldots, d_n+1$ there is by the 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 $L_j := \prod_{\ell \neq j}(b_\ell X_n - a_\ell Y_n)/(a_j b_\ell - a_\ell b_j)$ for $j = 1, \ldots, d_n+1$. Then the polynomial $F := \sum_j C_j L_j$ fulfills the requirements.

The computational result can easily be obtained via a linear algebra algorithm. □

This gives the following proposition.

Proposition 3.7. *Given a natural number $m \geqslant 3$, a prime power q with $q \geqslant 2^{m-2}$, an elliptic curve E over $\mathbb{F}_q$ in Weierstraß form and a covering $\varphi : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$ of degree two with $\varphi \circ [-1] = \varphi$, one can compute the mth 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.

https://doi.org/10.1112/S0010437X10005075

4. Geometric background on the algorithm and analysis

The main purpose of this section is to prove Proposition 2.9. Additionally, we give some background information on the definition of the factor base from a geometric point of view.

4.1 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, ch. 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 the category of S-schemes to the category of sets $Z \mapsto \mathrm{Mor}_{S'}(Z_{S'}, X')$ is representable by an S-scheme; the (unique up to unique isomorphism) 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 as follows. The Weil restriction of X' with respect to $S' \longrightarrow S$ is 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 $\beta : Z \longrightarrow \mathrm{Res}_S^{S'}(X')$ with $\alpha = u \circ \beta_{S'}$, 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 the *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.

LEMMA 4.1. *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*

$$\begin{array}{ccc} \mathrm{Res}_S^{S'}(X' \times_{W'} Y') & \longrightarrow & \mathrm{Res}_S^{S'}(Y') \\ \downarrow & & \downarrow \\ \mathrm{Res}_S^{S'}(X') & \longrightarrow & \mathrm{Res}_S^{S'}(W') \end{array}$$

with the obvious canonical morphisms.

LEMMA 4.2. *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

$$\begin{array}{ccc} \mathrm{Res}_T^{T'}(X') & \longrightarrow & \mathrm{Res}_S^{S'}(X') \\ \downarrow & & \downarrow \\ T & \longrightarrow & \mathrm{Res}_S^{S'}(T') \end{array}$$

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

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* $\mathrm{Res}_S^{S'}(T')$.

Now let $K|k$ be a finite separable field extension. If X' is a quasi-projective (respectively projective) scheme over K, then $\mathrm{Res}_k^K(X')$ is a quasi-projective (respectively 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, then $\mathrm{Res}_k^K(X')$ is in a natural way again a group scheme, and 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 $\sigma_{K|k}$ be the relative Frobenius automorphism of $K|k$. We denote the induced isomorphism $\mathrm{Spec}(k) \longrightarrow \mathrm{Spec}(k)$ again by $\sigma_{K|k}$. Let X' be a quasi-projective K-scheme. Then we have a canonical isomorphism

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

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

$$u : \prod_{i=0}^{n-1} \sigma_{K|k}^i(X') \longrightarrow X'.$$

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

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

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

$$\varphi \times \sigma_{K|k}(\varphi) \times \cdots \times \sigma_{K|k}^{n-1}(\varphi) : \prod_{i=0}^{n-1} \sigma_{K|k}^i(X') \longrightarrow \prod_{i=0}^{n-1} \sigma_{K|k}^i(Y').$$

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

The proof of Proposition 2.9 relies crucially on intersection theory in products of projective lines and on the theory of resultants for multihomogeneous polynomials. In this subsection we state some results on intersection theory and resultants in this specific situation.

For this subsection, let k be any field.

Notation 4.3. Let V be a fixed quasi-projective variety, and let X be a closed subscheme of V. Then we denote the class of X 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.)

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

Proposition 4.4. *Let* $h_i := [V(X_i)] \in \mathrm{CH}((\mathbb{P}^1_k)^n)$ *for* $i = 1, \ldots, n$. *Then 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, § 5.2]). We remark here that the book [Ful93] is concerned with toric varieties over the complex numbers. 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 4.5. 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 powers of $\mathbb{P}^1_k$. The considerations below follow immediately from the axioms of intersection theory in [Har77, Appendix A].

For $n_1 > n_2$, let $p : (\mathbb{P}^1_k)^{n_1} \longrightarrow (\mathbb{P}^1_k)^{n_2}$ be the projection to the first n_2 components. Let us denote by h_i, for $i = 1, \ldots, n_1$ or $i = 1, \ldots, n_2$, 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 4.4. This means that it is given by $p^*(h_i) = h_i$.

The push-forward $p_* : \mathrm{CH}((\mathbb{P}^1_k)^{n_1}) \longrightarrow \mathrm{CH}((\mathbb{P}^1_k)^{n_2})$, which is a group homomorphism, is given as follows.

Lemma 4.6. *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.*

For completeness we mention the following lemma.

Lemma 4.7. *Let* $F_1, \ldots, F_n$ *be multihomogeneous polynomials. Let the multidegree of* F_i *be* $(d_{i,1}, \ldots, d_{i,n})$, *and let* $D := (d_{i,j})_{i,j}$.

(a) *The zero-cycle* $[V(F_1)] \cdots [V(F_n)]$ *has degree* $\mathrm{Perm}(D)$, *the permanent of* D. *In particular, if the multidegree of each* F_i *is* $(d, \ldots, d)$ *for a common* $d \in \mathbb{N}$, *then the cycle has degree* $n! \cdot d^n$.

(b) *The degree zero part of the class of* $V(F_1, \ldots, F_n)$ *in the Chow ring has degree at most* $\mathrm{Perm}(D)$.

(c) *We have equality in part (b) if and only if* $V(F_1, \ldots, F_n)$ *is zero-dimensional.*

Sketch of a proof. Part (a) follows immediately from Proposition 4.4.

Part (b) can easily be obtained from Krull's Hautidealsatz and Axiom A7 on intersection theory in [Har77, Appendix A].

For part (c) see [Ful84, Proposition 8.2]. □

Intersection theory and the theory of resultants are closely connected. Let us recall the definition and basic properties in the situation under consideration.

Note for the following that according to our convention $\mathbb{N} = \{1, 2, \ldots\}$. Let us fix some $n \in \mathbb{N}$. For $\underline{d} \in \mathbb{N}$, let $M_{\underline{d}}$ be the set of monomials of multidegree $\underline{d}$ in $k[X_1, Y_1, \ldots, X_n, Y_n]$.

Let some $\underline{d}^{(i)} \in \mathbb{N}^n$ be given for each $i = 1, \ldots, n+1$. We want to define the generic resultant for multihomogeneous polynomials of multidegrees $\underline{d}^{(1)}, \ldots, \underline{d}^{(n+1)}$ over k. For this

we consider a 'universal coefficient ring', which is a multivariate polynomial ring over k 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 $k[(c_{i,m})_{i=1,\dots,n+1,m\in M_{\underline{d}^{(i)}}}]$. We define the *generic system of $n+1$ multihomogeneous polynomials with multidegrees* $\underline{d}^{(1)},\dots,\underline{d}^{(n+1)}$ as $G_1,\dots,G_{n+1} \in k[(c_{i,m})_{i,m}][X_1,Y_1,\dots,X_n,Y_n]$ with $G_i = \sum_{m\in M_{\underline{d}^{(i)}}} c_{i,m}\, m$.

The generic resultant for multihomogeneous systems with the given degrees is then an element of $k[(c_{i,m})_{i,m}]$, and the resultant of a particular system of multihomogeneous polynomials with the given degrees is obtained by substituting the coefficients of the polynomials for the generic coefficients. The key statements are summarized in the following proposition.

Proposition 4.8. (a) *There is an irreducible polynomial* $\mathrm{Res} \in k[(c_{i,m})_{i=1,\dots,n+1,m\in M_{\underline{d}^{(i)}}}]$ *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 field extensions* $K|k$ *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 is unique up to multiplication by a non-trivial constant.*

(c) *The polynomial* Res *is geometrically irreducible.*

(d) *For each* $i=1,\dots,n+1$, 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.*

This proposition follows from general results [GKZ94, § 3.3] applied to multihomogeneous polynomials. Note that all results in [GKZ94] are formulated over the complex numbers, but the proof of this result holds over arbitrary fields as well.

4.3 Background on the factor base

As at the end of § 4.1, let $K|k$ be an extension of finite fields of degree n. Let E be an elliptic curve over K, and let us fix a covering $\varphi : E \longrightarrow \mathbb{P}^1_K$ of degree two 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.

$$\begin{array}{ccc} V & \hookrightarrow & \mathrm{Res}^K_k(E) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Res}^K_k(\varphi)} \\ \mathbb{P}^1_k & \overset{\iota}{\hookrightarrow} & \mathrm{Res}^K_k(\mathbb{P}^1_k) \end{array} \tag{3}$$

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 $\iota(\mathbb{P}^1_k(k)) \subseteq \mathrm{Res}^K_k(\mathbb{P}^1_K)(k)$.

https://doi.org/10.1112/S0010437X10005075

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', which is something that is not 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_∞, the k-rational point of $\mathrm{Res}^K_k(E)$ corresponding to P.

We now study V under Condition 2.7.

PROPOSITION 4.9. *Let Condition 2.7 be satisfied. Then V is geometrically reduced and geometrically irreducible (and thus birational to a curve).*

Proof. By (3) and Lemma 4.2 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

$$V_K \simeq E \times_{\mathbb{P}^1_K} \sigma_{K|k}(E) \times_{\mathbb{P}^1_K} \cdots \times_{\mathbb{P}^1_K} \sigma^{n-1}_{K|k}(E), \tag{4}$$

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

Let us now fix an algebraic closure $\overline{k(x)}$ of $k(x)$, and let σ again be the relative Frobenius automorphism of $\overline{k}|k$. Let us then prolong σ first to $\overline{k}(x)$ via $\sigma(x) := x$, 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 2.7 for $i = 1, \ldots, n-1$, the extension $\sigma^i(\overline{k}(E))|\overline{k}(x)$ is ramified at $\sigma^i(R)$, but for any $j = 0, \ldots, i-1$, the extension $\sigma^j(\overline{k}(E))|\overline{k}(x)$ is unramified at $\sigma^i(R)$; 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 unramified at $\sigma^i(R)$. 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 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 4.10. *Let us still assume that Condition 2.7 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 at most $(2n-1) \cdot (2^n - 1)$;*
(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, for example, [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 two. We show below that the genus of a function field L as in the sum is always at most $2n-1$. This implies that $g(\mathcal{C}) \leqslant (2n-1) \cdot (2^n - 1)$.

https://doi.org/10.1112/S0010437X10005075

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 $\overline{k(x)}|\overline{k}(x)$ of degree two corresponds to a one-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.

Now if $\overline{k}(E)$ 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 $(a_0, \ldots, a_{n-1}) \in \mathbb{F}_2^n - \{0\}$.

First, let $j(E) = 0$. 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 three or of the form $g/(x-\lambda)^3$ 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 at most $2n-1$.

Now let $j(E) \neq 0$. 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 $1/(x-a)$ 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 at most $2n-1$.

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 most $4n$ places. Thus the genus of L is at most $2n-1$.

We come to part (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 that 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 preimage of S. In 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 $\#S \cdot 2^n \leqslant 4n \cdot 2^n$ elements. □

Proposition 4.11. *Let $k = \mathbb{F}_q$, and let $n \geqslant 2$ and $\log_2(q) \geqslant 7n$. Then, under Condition 2.7,*

$$\#\{P \in E(K) \mid \varphi(P) \in \mathbb{P}^1(k)\} = \#V(k) \geqslant \tfrac{1}{2} \cdot (q+1)\,.$$

Proof. By the above propositions and the Hasse–Weil bound we have

$$\#V(k) \geqslant q + 1 - 2 \cdot (2n-1) \cdot (2^n - 1) \cdot q^{\frac{1}{2}} - n \cdot 2^{n+2} + 1 \geqslant q + 1 - n \cdot 2^{n+2} \cdot (q^{\frac{1}{2}} + 1).$$

Now, $q^{\frac{1}{2}} + 1 \leqslant 2 \cdot (q+1)/q^{\frac{1}{2}}$ and thus

$$n \cdot 2^{n+2} \cdot (q^{\frac{1}{2}} + 1) \leqslant 2^{n/2} \cdot \frac{2^{n+3}}{q^{\frac{1}{2}}} \cdot (q+1) = \frac{2^{\frac{3}{2}n+4}}{q^{\frac{1}{2}}} \cdot \frac{q+1}{2} \leqslant \frac{2^{\frac{7}{2}n}}{q^{\frac{1}{2}}} \cdot \frac{q+1}{2} = \left(\frac{2^{7n}}{q}\right)^{\frac{1}{2}} \cdot \frac{q+1}{2}.$$

By assumption this is at most $(q+1)/2$ and thus $\#V(k) \geqslant (q+1)/2$. □

4.4 The role of the summation polynomials

Let the hypersurface $H = H_{n+1}$ of $(\mathbb{P}^1_k)^{n+1}$ be defined as in § 3.

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.

$$\begin{array}{ccc} X & \hookrightarrow & \mathrm{Res}_k^K(H) \\ \downarrow & & \downarrow \\ (\mathbb{P}^1_k)^n \times \mathrm{Res}_k^K(\mathbb{P}^1_K) & \hookrightarrow & (\mathrm{Res}_k^K(\mathbb{P}^1_K))^{n+1} \end{array} \tag{5}$$

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 $\varphi(P_i) = Q_i$, $\varphi(P) = Q$ and $\sum_i P_i = P$.

Notation 4.12. 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 4.13. *$(p_1)_{|X} : X \longrightarrow (\mathbb{P}^1_k)^n$ is a flat covering of degree $2^{(n-1)\cdot n}$.*

Proof. By Proposition 3.2(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 $\mathrm{Res}_k^K(H) \longrightarrow \mathrm{Res}_k^K((\mathbb{P}^1_K)^n) \simeq (\mathrm{Res}_k^K(\mathbb{P}^1_K))^n$ 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 $\iota \times \cdots \times \iota : (\mathbb{P}^1_k)^n \longrightarrow (\mathrm{Res}_k^K(\mathbb{P}^1_K))^n$. □

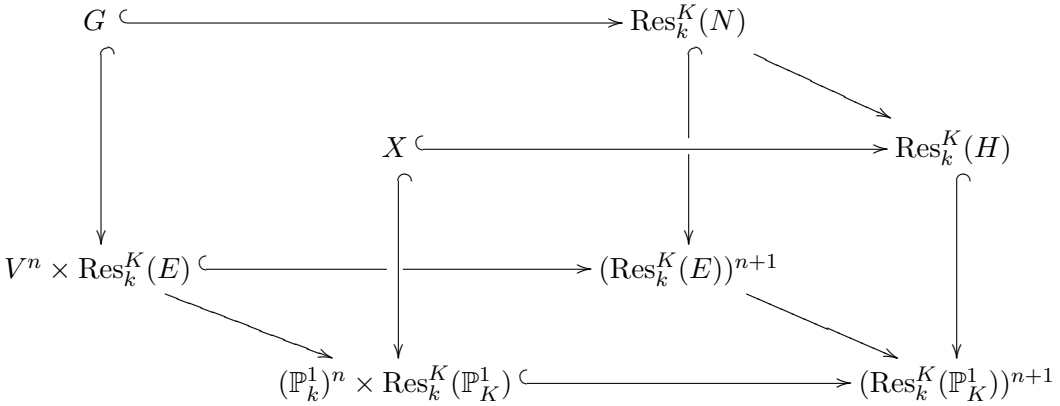
Notation 4.14. Let G be the graph of $-a_n : V^n \longrightarrow \mathrm{Res}_k^K(E)$, where a_n is the restriction of the addition morphism to V^n. (Note the minus sign!)

As in § 3, for $m \in \mathbb{N}$, let 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 $\mathrm{Res}_k^K(E^m)$. Now let $N := N_{n+1}$. By considering Z-valued points for any k-scheme Z, one obtains immediately the following.

LEMMA 4.15. *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 4.16. *There is a canonical surjective morphism $G \longrightarrow X$. Moreover, if Condition 2.7 is satisfied, then X is geometrically irreducible.*

Proof. Let us consider the commutative diagram



https://doi.org/10.1112/S0010437X10005075

with the obvious canonical morphisms. As by definition of X the right-lower subdiagram (i.e. diagram (5)) is Cartesian, we have an induced morphism $G \longrightarrow X$.

It suffices to prove the surjectivity on $\overline{k}$-valued points. Therefore 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 in 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 $\mathrm{Res}_k^K(\mathbb{P}^1_K)(\overline{k})$ lies in $((\mathbb{P}^1)^n \times \mathrm{Res}_k^K(\mathbb{P}^1_K))(\overline{k})$. But this is obvious as the image is nothing but the point Q we started with.

Now let Condition 2.7 be satisfied. By Proposition 4.9, 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 $\mathrm{Res}_k^K(\mathbb{P}^1_K)$. Let $X_{Q_\circledcirc}$ be the fiber of X at $Q_\circledcirc$, that is, we have the following Cartesian diagram.

$$\begin{array}{ccc}
X_{Q_\circledcirc} & \hookrightarrow & X \\
\downarrow & & \downarrow \\
(\mathbb{P}^1_k)^n & \hookrightarrow & (\mathbb{P}^1_k)^n \times \mathrm{Res}_k^K(\mathbb{P}^1_K) \\
\downarrow & & \downarrow \\
\mathrm{Spec}(k) & \xrightarrow{Q_\circledcirc} & \mathrm{Res}_k^K(\mathbb{P}^1_K)
\end{array}$$

Then we have the following connection with the decomposition problem.

Proposition 4.17. *As a subscheme of $(\mathbb{P}^1_k)^n$, $X_{Q_\circledcirc}$ is $V(S^{(1)}, \ldots, S^{(n)})$, where the polynomials $S^{(j)} \in k[X_1, Y_1, \ldots, X_n, Y_n]$ are defined as in (2).*

We first show the following lemma.

Lemma 4.18. *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*

$$\begin{array}{ccc}
X_{Q_\circledcirc} & \hookrightarrow & \mathrm{Res}_k^K(H_Q) \\
\downarrow & & \downarrow \\
(\mathbb{P}^1_k)^n & \hookrightarrow & (\mathrm{Res}_k^K(\mathbb{P}^1_K))^n
\end{array}$$

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 4.1 the defining Cartesian diagram

$$\begin{array}{ccc}
H_Q & \hookrightarrow & H \\
\downarrow & & \downarrow \\
(\mathbb{P}^1_K)^n & \hookrightarrow & (\mathbb{P}^1)^{n+1}
\end{array}$$

https://doi.org/10.1112/S0010437X10005075

gives rise to the Cartesian diagram

$$\begin{array}{ccc} \mathrm{Res}_k^K(H_Q) & \hookrightarrow & \mathrm{Res}_k^K(H) \\ \downarrow & & \downarrow \\ (\mathrm{Res}_k^K(\mathbb{P}^1_K))^n & \hookrightarrow & (\mathrm{Res}_k^K(\mathbb{P}^1_K))^{n+1} \end{array}$$

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

$$\begin{array}{ccccc} X_{Q_\circledcirc} & \hookrightarrow & \mathrm{Res}_k^K(H_Q) & \hookrightarrow & \mathrm{Res}_k^K(H) \\ \downarrow & & \downarrow & & \downarrow \\ (\mathbb{P}^1)^n_k & \hookrightarrow & (\mathrm{Res}_k^K(\mathbb{P}^1_K))^n & \hookrightarrow & (\mathrm{Res}_k^K(\mathbb{P}^1_K))^{n+1} \end{array}$$

□

We come to the proof of Proposition 4.17.

By Lemmas 4.18 and 4.2 we have a commutative diagram

$$\begin{array}{ccc} X_{Q_\circledcirc} & \xrightarrow{\sim} & \mathrm{Res}^{(\mathbb{P}^1_K)^n}_{(\mathbb{P}^1_k)^n}(H_Q) \\ & \searrow \quad \swarrow & \\ & (\mathbb{P}^1_k)^n & \end{array}$$

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 $V(S^{(1)}, \ldots, S^{(n)})$.

Now let $S_{\varphi,n+1}$ be the same summation polynomial as in § 2.1 (recall that the $(n+1)$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 § 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.

https://doi.org/10.1112/S0010437X10005075

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

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

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

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

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

4.5 Determination of non-zero-dimensional fibers

For the analysis of the algorithm 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 $\prod_{i=1}^n \operatorname{Proj}(\mathbb{Z}[X_{1,i},Y_{1,i}]) \times \prod_{i=1}^n \operatorname{Proj}(\mathbb{Z}[X_{2,i},Y_{2,i}])$, 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 4.19. *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

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

for $j = 1,\dots,n$. One can easily see with this explicit description that, for all $\ell = 2,\dots,n$, $V(F_1,\dots,F_{\ell-1})$ meets $V(F_\ell)$ properly.

Indeed, let C be an irreducibility component of $V(F_1,\dots,F_{\ell-1})$. 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 $V(F_\ell)(\overline{K})$.

By Axiom A7 on intersection theory in [Har77, Appendix A] we conclude that $[X_K] = [V(F_1)] \cdots [V(F_n)]$ in the Chow ring of $(\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^n$. Moreover, $[V(F_j)] = 2^{n-1}(h_{1,1} + \cdots + h_{1,n} + h_{2,j})$. This gives the statement. □

Lemma 4.20. *The map $(p_2)_{|X}$ is surjective.*

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

First, by the previous lemma and Lemma 4.6 we have $((p_2)_K)_*([X_K]) = n! \cdot 2^{(n-1)\cdot n}$; thus $(p_2)_K(X_K)$ is equal to the ambient space $\prod_{i=1}^n \operatorname{Proj}(K[X_{2,i},Y_{2,i}])$.

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 4.21. 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.

Now let $q_i : \prod_{i=1}^n (\mathrm{Proj}(K[X_{1,i}, Y_{1,i}])) \longrightarrow \mathrm{Proj}(K[X_{1,i}, Y_{1,i}])$ be the projection to the ith 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 $X_{1,1}, Y_{1,1}, \ldots, X_{1,i-1}, Y_{1,i-1}, X_{1,i+1}, Y_{1,i+1}, \ldots, X_{1,n}, Y_{1,n}$. Let $Q = (Q_1, \ldots, Q_n) \in \prod_{i=1}^n \mathrm{Proj}(K[X_{2,i}, Y_{2,i}])(\overline{K})$. Then $q_i(X_Q) = \mathrm{Proj}(\overline{K}[X_{1,i}, Y_{1,i}])$ if and only if $R_i(X_i, Y_i, Q_1, \ldots, Q_n) = 0$. Thus 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.

Note now that not all fibers are non-zero-dimensional because X has dimension n (see Lemma 4.13) and $(\mathbb{P}^1_K)^n$ has dimension n too. Thus the polynomials $R_1, \ldots, R_n$ are all non-trivial.

Lemma 4.22. *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. By Lemma 4.7 the corresponding generic resultant is homogeneous in the coefficients of each of the polynomials of degree $(n-1)! \cdot 2^{(n-1)^2}$. Now, for $j = 1, \ldots, n$, F_j has degree 2^{n-1} with respect to $X_{2,j}, Y_{2,j}$, and these variables do not occur in F_ℓ for $\ell \neq j$. This implies that the degree of R_i with respect to $X_{2,j}, Y_{2,j}$ is $(n-1)! \cdot 2^{(n-1)^2} \cdot 2^{n-1} = (n-1)! \cdot 2^{(n-1)\cdot n}$. Moreover, each polynomial F_ℓ has degree 2^{n-1} with respect to $X_{1,i}, Y_{1,i}$ and therefore the degree of R_i 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

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

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

It follows that

$$\begin{aligned}
&[X_K] \cdot [(p_2)_K^{-1}(V(C_i))] \\
&\quad = (n-1)! \cdot 2^{2(n-1)\cdot n} \cdot \left(\prod_{i=1}^n (h_{1,1} + \cdots + h_{1,n} + h_{2,i}) \right) \cdot (h_{2,1} + \cdots + h_{2,n})
\end{aligned}$$

in $\mathrm{CH}((\mathbb{P}^1_K)^n \times (\mathbb{P}^1_K)^n)$. With Lemma 4.6 this implies that

$$\begin{aligned}((p_1)_K)_*([X_K] \cdot [(p_2)_K^{-1}(V(C_i))]) &= (n-1)! \cdot 2^{2(n-1)\cdot n} \cdot n \cdot (h_{1,1} + \cdots + h_{1,n}) \\ &= n! \cdot 2^{2(n-1)\cdot n} \cdot (h_{1,1} + \cdots + h_{1,n}). \end{aligned} \tag{6}$$

Assumption 4.23. Let us from now on assume that Condition 2.7 is satisfied.

Notation 4.24. Let $k = \mathbb{F}_q$ (such that $K = \mathbb{F}_{q^n}$).

Recall that X is now geometrically irreducible (Proposition 4.16). 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 $[X_K] \cdot [(p_2)_K^{-1}(V(C_i))] = [X_K \cap (p_2)_K^{-1}(V(C_i))]$ by Axiom A7 on intersection theory in [Har77, Appendix A]. As the map $(p_1)_K : X_K \longrightarrow \prod_{i=1}^n \mathrm{Proj}([X_{1,i}, Y_{1,i}])$ is finite and flat (cf. Lemma 4.13), the dimension of $(p_1)_K(X_K \cap C_i)$ is equal to the dimension of $X_K \cap C_i$. With (6) we conclude the following lemma.

Lemma 4.25. *$(p_1)_K(X_K \cap C_i)$ (with the induced reduced scheme structure) is a reduced effective Cartier divisor of $\prod_{i=1}^n \mathrm{Proj}([X_{1,i}, Y_{1,i}])$ whose multidegree is componentwise at most $(n! \cdot 2^{2(n-1)\cdot n}, \ldots, n! \cdot 2^{2(n-1)\cdot n})$.*

The subscheme

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

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

Lemma 4.26. (a) *B is a reduced effective Cartier divisor whose multidegree is componentwise at most $(n^2 \cdot n! \cdot 2^{2(n-1)\cdot n}, \ldots, n^2 \cdot n! \cdot 2^{2(n-1)\cdot n})$.*

(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 at most $(n^2 \cdot n! \cdot 2^{2(n-1)\cdot n}, \ldots, n^2 \cdot n! \cdot 2^{2(n-1)\cdot n})$.

Statement (b) follows immediately from the definition of B.

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

Lemma 4.27. *Let H be an effective Cartier divisor of multidegree $\underline{d}$ in $(\mathbb{P}^1_k)^n$. Then*

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

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

We proceed with induction by n. For $n = 1$ the claim is that $\#H(k) \leqslant d_1$, 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

https://doi.org/10.1112/S0010437X10005075

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. Now let 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 $\#V(C)(k) \leqslant (\sum_{i=1}^{n-1} d_i) \cdot (q+1)^{n-2}$ by induction. We conclude that

$$\begin{aligned}\#H(k) &\leqslant d_n \cdot (q+1)^{n-1} + \#V(C)(k) \cdot (q+1) \\ &\leqslant d_n \cdot (q+1)^{n-1} + \left(\sum_{i=1}^{n-1} d_i\right) \cdot (q+1)^{n-1} \\ &= \left(\sum_{i=1}^{n} d_i\right) \cdot (q+1)^{n-1}.\end{aligned}$$

□

Given an element $P \in E(K)$, there is a φ-isolated decomposition of P if and only if the fiber $X_{\varphi(P)_\circledcirc}$ contains an isolated 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 $\sum_i P_i = P$. This is, in particular, the case if the fiber is zero-dimensional and contains such a k-rational point.

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. In preparation for this, we now proceed a bit more generally.

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

For this, let us consider the commutative diagram of sets of k-valued points,

$$\begin{array}{ccc} G(k) & \xrightarrow{\quad\rho\quad} & X(k) \\ {\scriptstyle\gamma}\uparrow & & \downarrow{\scriptstyle(p_1)_{|X}} \\ V^n(k) & \xrightarrow{\quad\tau\quad} & \prod_{i=1}^n \operatorname{Proj}(k[X_{1,i}, Y_{1,i}])(k) \end{array}$$

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 4.16, and the map $\tau : V^n(k) \longrightarrow \prod_{i=1}^n \operatorname{Proj}(k[X_{1,i}, Y_{1,i}])(k)$ is induced componentwise by the canonical morphism in diagram (3).

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 then corresponds 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 $M \subseteq \{(P_1, \ldots, P_n) \in E(K)^n \mid \varphi(P_i) \in \mathbb{P}^1(k)\ \forall i = 1, \ldots, n\}$, and let $M_\circledcirc$ be the corresponding subset of $V^n(k)$. Then every element $P \in E(K)$ such that $\varphi(P)_\circledcirc \in \operatorname{Res}^K_k(\mathbb{P}^1_K)(k)$ 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.

https://doi.org/10.1112/S0010437X10005075

(Indeed, if P is such an element, first the fiber $X_{\varphi(P)_\circledcirc}$ is zero-dimensional by Lemma 4.26(b), and second there exist $P_1, \dots, P_n \in M$ 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

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

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 $\prod_{i=1}^n \mathrm{Proj}(k[X_{1,i}, Y_{1,i}])(k)$ is contained in

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

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

With Lemma 4.26(c) we obtain

$$\begin{aligned}\#((\rho \circ \gamma)(M_\circledcirc) - p_1^{-1}(B(k))) &\geqslant \#(\tau(M_\circledcirc) - B(k)) \\ &\geqslant \frac{\#M}{2^n} - n^3 \cdot n! \cdot 2^{2(n-1)\cdot n} \cdot (q+1)^{n-1}. \qquad (7)\end{aligned}$$

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 4.20). We therefore have the following proposition.

Proposition 4.28. *Let*

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

Then the number of elements $P \in E(K)$ such that there exists a φ-isolated decomposition $(P_1, \dots, P_n)$ of $\pm P$ with $P_1, \dots, P_n \in M$ is

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

We now apply this proposition with $M_\circledcirc = V(k)$. By Proposition 4.11 for $\log_2(q) \geqslant 7n$ and $n \geqslant 2$ we have $\#V(k) \geqslant (q+1)/2$; thus $\#V^n(k) \geqslant (q+1)^n/2^n$. With Proposition 4.28 we obtain that the number of elements $P \in E(K)$ such that there exist $P_1, \dots, P_n \in E(K)$ with $\varphi(P_i) \in \mathbb{P}^1(k)$ and $\sum_i P_i = P$ is

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

Now let $\epsilon > 0$. Then for n large enough this is

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

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

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

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

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

We therefore have the following proposition.

Proposition 4.29. *Let $\epsilon > 0$. Then for n large enough and $(2+\epsilon) \cdot n^2 \leqslant \log_2(q)$ there are at least $2 \cdot q^{n-\frac{1}{2}}$ elements in $E(K)$ which have φ-isolated decompositions.*

This implies Proposition 2.9, the main result for the analysis of the decomposition algorithm in § 2.1.

Acknowledgements

I thank Steven Galbraith, Pierrick Gaudry, Éric Schost, Nicolas Thériault, and the anonymous referees for their helpful comments.

References

BLR80 S. Bosch, W. Lütkebohmert and W. Raynaud, *Néron models* (Springer, Berlin, 1980).

BCP97 W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

Can90 J. Canny, *Generalized characteristic polynomials*, J. Symbolic. Comput. **9** (1990), 241–250.

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*. Math. Comp. (2009), doi: 10.1090/S0025-5718-2010-02281-1.

Ful84 W. Fulton, *Intersection theory* (Springer, Berlin, 1984).

Ful93 W. Fulton, *Introduction to toric varieties* (Princeton University Press, Princeton, NJ, 1993).

Gau09 P. Gaudry, *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, J. Symbolic. Comput. **44** (2009), 1690–1702.

GKZ94 I. Gelfand, M. Kapranov and A. Zelevinsky, *Discriminants, resultants, and multidimensional determinants* (Birkhäuser, Basel, 1994).

Gro61 A. Grothendieck, *Eléments de Géométrie Algébrique III, Première Partie*, Publ. Math. **11** (1961).

Har77 R. Hartshorne, *Algebraic geometry* (Springer, Berlin, 1977).

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

LP92 H. W. Lenstra and C. Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), 483–516.

Mat89 H. Matsumura, *Commutative ring theory* (Cambridge University Press, Cambridge, 1989).

Mil04 V. Miller, *The Weil pairing and its efficient computation*, J. Cryptology **17** (2004), 235–261.

Roj99 J. M. Rojas, *Solving degenerate sparse polynomial systems faster*, J. Symbolic. Comput. **28** (1999), 155–186.

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

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

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

Sil86 J. Silverman, *The arithmetic of elliptic curves* (Springer, Berlin, 1986).

Sti93 H. Stichtenoth, *Algebraic function fields and codes* (Springer, Berlin, 1993).

Claus Diem diem@math.uni-leipzig.de
University of Leipzig, Mathematical Institute, Johannisgasse 26, 04103 Leipzig, Germany