Geometric quadratic chabauty and other topics in number theory

Lido, G.M.

Chapter 4

Discrete logarithms in small characteristic

Solving the discrete logarithm problem means the following: given a group G, a generator $g \in G$ and another element $h \in G$, find an integer z such that $g^z = h$. The hardness of this problem, which depends on the choice of G, has had implications in cryptography since the very beginning [33] of public-key cryptography. We are concerned with the cases where G is the multiplicative group of a finite field of *small characteristic*, which, for us, means a field of characteristic p and cardinality p^n for some integer $n > p$. Our main result is the following.

Theorem 4.0.1. *There exists a probabilistic algorithm, described in Section 4.4, that solves the discrete logarithm problem in $K^\times$ for all finite fields K of small characteristic in expected time*

$$(\log \#K)^{O(\log \log \#K)}.$$

An algorithm whose complexity is as above is called *quasi-polynomial*. In 2013 Barbulescu, Gaudry, Joux and Thomé presented in [19] the first heuristic quasi-polynomial algorithm solving the discrete logarithm in finite fields of small characteristic. One of their main ideas, originally in [56], was looking for a "simple" description of the Frobenius automorphism $\phi\colon K \to K$ and, if one can find such a simple description, using it in an index calculus algorithm to find relations among the elements of the factor base more easily.

In [49] a new algorithm was then presented, based on similar ideas, that was proven to terminate in quasi-polynomial expected time when it is possible to find a "simple" description of the Frobenius automorphism $\phi\colon K \to K$. In particular, we could deduce Theorem 4.0.1 if we knew that all finite fields of small characteristic K can be embedded in a slightly larger field K' admitting a presentation as in [49]. Unfortunately, the author

is not aware of any proof of this fact, even though computations like [56, Table 1] support it.

Our algorithm is based on the same approach as [49], adapted to fields admitting a different kind of presentation in terms of elliptic curves. Since over a finite field $\mathbb{F}_q$ there are many non-isomorphic elliptic curves, it is easy to prove that all finite fields of small characteristic can be embedded in a slightly larger field admitting such an elliptic presentation.

Elliptic presentations were firstly introduced in [30], as we have learnt after our first (incomplete) attempt to prove Theorem 4.0.1 using elliptic presentations (see the author's master's thesis [67]). In [65] Kleinjung and Wesolowski have independently proved Theorem 4.0.1, also using elliptic presentations of finite fields. One of the main differences between the present approach and the one in [65] is the proof of the correctness of the algorithms. In both cases it is a matter of showing the irreducibility of certain curves: the approach in [65] is based on the ideas in [64], while we mostly rely on a little bit of Galois theory over function fields; both approaches use some cumbersome computations and in our case these computations are mostly contained in Proposition 4.6.3 and in the Claims 4.8.2.3, 4.8.2.6, 4.8.3.2. The practical feasibility of algorithms using elliptic presentations has been studied by Joux and Pierrot in [57].

In Section 4.1 we define elliptic presentations and we prove that all finite fields of small characteristic can be embedded in a slightly larger field admitting an elliptic presentation. Section 4.2 has technical importance: given an elliptic presentation, we define a finite and small set of points on the associated elliptic curve that we call "traps" since they interfere with our algorithm. In Section 4.3 we describe the general setup of our algorithm and we explain how to pass from a factor base made of irreducible polynomials in $\mathbb{F}_q[x]$ to a factor base made of irreducible divisors on an elliptic curve $E/\mathbb{F}_q$. In Section 4.4 we give our algorithm, stated in terms of a descent procedure that is described in Section 4.5. A more precise statement about the complexity of the main algorithm is given in Theorem 4.4.4. Our descent procedure consists of two steps, presented and analysed in Section 4.5 under an assumption on the number of points of certain varieties that are used in these steps. These assumptions are proven in Section 4.8 for the first step and in Section 4.7 for the second and easier step. In Section 4.6 we prove a lemma, mainly using some Galois theory over function fields, that is useful in Sections 4.7 and 4.8.

Acknowledgements I thank René Schoof for introducing me to this research problem in 2016 and for the useful ideas that lead to substantial simplifications.

4.1 Elliptic presentations

One of the main ideas in [56] and in the original quasi-polynomial algorithm [19], is to present a field K using two subfields $\mathbb{F}_q \subsetneq \mathbb{F}_Q \subseteq K$ of order q, Q (both "small" compared to $\#K$) and an element $x_1 \in K$ generating the extension $\mathbb{F}_Q \subset K$ such that the q-th Frobenius acts on x_1 in a simple way, namely $x_1^q = f(x_1)$ for some $f \in \mathbb{F}_q(x)$ of degree at most 2. We now define a presentation based on a similar idea: describing K as $\mathbb{F}_q(x_1, y_1)$ where $\mathbb{F}_q$ is a finite field of order q "small" compared to $\#K$ and x_1, y_1 are two elements of K on which the q-th Frobenius acts in a "simple" way.

Let q be a prime power, let n be a positive integer and let K be a field of cardinality q^n. Let $\mathbb{F}_q$ be a finite field of cardinality q and let $\overline{\mathbb{F}_q}$ be its algebraic closure. Suppose there exists an elliptic curve $E/\mathbb{F}_q$ defined by a Weierstrass equation and a point $P_0 \in E(\mathbb{F}_q)$ of order n. Denoting by ϕ be the q-th Frobenius on the elliptic curve E, the map $E \to E$ given by $P \mapsto \phi(P) - P$ is surjective. Therefore there is a point $P_1 = (x_1, y_1) \in E(\overline{\mathbb{F}_q})$ such that $\phi(P_1) = P_1 + P_0$. Hence

$$(x_1^{q^i}, y_1^{q^i}) = \phi^i(P_1) = P_1 + i \cdot P_0 \quad \text{for every } i \in \mathbb{Z}\,, \tag{4.1.1}$$

implying that the field extension $\mathbb{F}_q \subset \mathbb{F}_q(x_1, y_1)$ has degree n. Hence $\mathbb{F}_q(x_1, y_1)$ is isomorphic to K. Moreover, using the addition formulas on E, we see that the q-th Frobenius acts on the pair (x_1, y_1) in a "simple" way: there are polynomials $f_1, f_2, f_3 \in \mathbb{F}_q(x, y)$ of small degree such that

$$x_1^q = f_1(x_1, y_1)/f_3(x_1, y_1)\,, \quad y_1^q = f_2(x_1, y_1)/f_3(x_1, y_1)\,.$$

With this heuristic in mind, we give the following definition.

Definition 4.1.2. Let $E/\mathbb{F}_q$ be an elliptic curve defined by a Weierstrass polynomial in $\mathbb{F}_q[x, y]$ and let P_0 be a $\mathbb{F}_q$-point on E. An $(E/\mathbb{F}_q, P_0)$-*presentation* of a finite field K is an ideal $\mathfrak{m} \subset \mathbb{F}_q[x, y]$ such that

(i) K is isomorphic to $\mathbb{F}_q[x, y]/\mathfrak{m}$ with a chosen isomorphism;

(ii) denoting $\phi\colon E \to E$ the q-th Frobenius, there exists a point $P_1 = (x_1, y_1)$ in $E(\overline{\mathbb{F}_q})$ such that $\phi(P_1) = P_1 + P_0$ and $\mathfrak{m} = \{f \in \mathbb{F}_q[x, y] : f(x_1, y_1) = 0\}$;

(iii) $q > 2$ and, under the isomorphism (i), we have $[K : \mathbb{F}_q] > 2$.

Sometimes we omit the dependence on $(E/\mathbb{F}_q, P_0)$ and we simply write "elliptic presentation". The technical hypothesis $q > 2$ is used in the proof of Claim 4.8.2.3.

Remark 4.1.3. Any elliptic presentation $\mathfrak{m}$ is a maximal ideal, since $\mathbb{F}_q[x, y]/\mathfrak{m}$ is a field.

Remark 4.1.4. If $\mathfrak{m}$ is an elliptic presentation, then the inclusion $\mathbb{F}_q[x] \to \mathbb{F}_q[x,y]$ induces an isomorphism $\mathbb{F}_q[x]/\mu \cong \mathbb{F}_q[x,y]/\mathfrak{m}$ for a certain $\mu \in \mathbb{F}_q[x]$.

Proving this is equivalent to proving that x generates the extension $\mathbb{F}_q \subset \mathbb{F}_q[x,y]/\mathfrak{m}$. Using the notation in Definition 4.1.2, this is equivalent to proving that $\mathbb{F}_q(x_1)$ is equal to $\mathbb{F}_q(x_1,y_1)$. If, for the sake of contradiction, this is not the case, then the Weierstrass equation satisfied by x_1 and y_1 implies that the extension $\mathbb{F}_q(x_1) \subset \mathbb{F}_q(x_1,y_1)$ has degree 2, hence $[\mathbb{F}_q(x_1) : \mathbb{F}_q] = \frac{n}{2}$, where $n := [\mathbb{F}_q(x_1,y_1) : \mathbb{F}_q] = [K : \mathbb{F}_q]$. Using Equation 4.1.1, we deduce that

$$x(P_1) = x_1 = x_1^{q^{n/2}} = x(\phi^{n/2}P_1) = x(P_1 + \tfrac{n}{2}P_0) \quad \Longrightarrow \quad P_1 + \tfrac{n}{2}P_0 = \pm P_1\,.$$

Since, by Equation 4.1.1, the order of P_0 is equal to n, we have $P_1 + \frac{n}{2}P_0 = -P_1$, implying that $2P_1$ lies $E(\mathbb{F}_q)$. Therefore P_0 has order 2, contradicting $n = [K : \mathbb{F}_q] > 2$ in (iii).

We now show that any finite field K of small characteristic can be embedded in a "slightly larger" field admitting an elliptic presentation with q "small" compared to $\#K$.

Proposition 4.1.5. *For any finite field K of small characteristic there exists an extension $K \subset K'$ having a elliptic presentation $\mathfrak{m} \subset \mathbb{F}_q[x,y]$ of K' such that*

$$\log(\#K') \leq 13\log(\#K)\log\log(\#K) \quad \textit{and} \quad q \leq \log(\#K')^4\,.$$

Moreover such K' and its presentation can be computed in polynomial time in $\log(\#K)$.

Proof. Let $\#K = p^n$ for a prime p and an integer $n > p$. Put $k_0 := \lceil \log_p n \rceil$ and $q := p^{2k_0}$, so that n has a multiple n_1 in the interval $[q - \sqrt{q} + 1, q + 1]$. If $n_1 \equiv 1 \bmod p$ we define $n_2 := n_1 + n$, otherwise we define $n_2 := n_1$. Since n_2 in an integer contained in the Hasse interval $[q - 2\sqrt{q} + 1; q + 2\sqrt{q} + 1]$ that is not congruent to 1 modulo p, by [90, Theorems 1a, 3] we can choose an elliptic curve $E/\mathbb{F}_q$ whose group of rational points $E(\mathbb{F}_q)$ is cyclic of order n_2. Since n divides n_2, we can choose a point $P_0 \in E(\mathbb{F}_q)$ of order n.

We can assume E is defined by a Weierstrass polynomial. Since the map $P \mapsto \phi(P) - P$ is surjective, we can choose a point $(x_1,y_1) = P_1 \in E(\overline{\mathbb{F}_q})$ such that $\phi(P_1) = P_1 + P_0$. We define

$$\mathfrak{m} := \{f \in \mathbb{F}_q[x,y] : f(x_1,y_1) = 0\}\,, \quad K' := \mathbb{F}_q(x_1,y_1) \subset \overline{\mathbb{F}_q}\,.$$

The map $\mathbb{F}_q[x,y] \to K$ sending $x \mapsto x_1, y \mapsto y_1$ induces an isomorphism $\mathbb{F}_q[x,y]/\mathfrak{m} \cong K'$. To prove that $\mathfrak{m}$ is an elliptic presentation of K' it remains to show that both q and $[K' : \mathbb{F}_q]$ are larger than 2: in the first case it is true because $k_0 > 1$, in the second case it is true because, by (4.1.1), the degree of $\mathbb{F}_q \subset K'$ is equal to the order n of P_0, and $n > p \geq 2$.

Since $[K' : \mathbb{F}_q] = n$ divides $[K' : \mathbb{F}_p]$, the field K' has a subfield with p^n elements. In other words K can be embedded in K'. Moreover we have

$$\log(\#K') = n \log q < 2n \log(p)(\log_p(n)+1) \leq 4 \log(p) \log(n) \leq 13 \log(\#K) \log\log(\#K),$$
$$2 < p^2 \leq q = p^{2\lceil \log_p n \rceil} < p^{2+2\log_p n} = (pn)^2 \leq n^4 < \log(q^n)^4 = \log(\#K')^4 .$$

We now prove that it is possible to compute such K' and $\mathfrak{m}$ in polynomial time in $\log(\#K)$. We describe a procedure following the abstract part of the proof. Computing k_0, q, n_1 is easy. We can construct a field $\mathbb{F}_q$ by testing the primality of all polynomials of degree $2k_0$ over $\mathbb{F}_p$ until an irreducible ν is found and define $\mathbb{F}_q = \mathbb{F}_p[T]/\nu$; since there are less than n^2 polynomials of this type, this takes polynomial time. Similarly we can find an elliptic curve E with an $\mathbb{F}_q$-point P_0 of order n in polynomial time, by listing all possible Weierstrass equations (there are less than q^6), testing if they define an elliptic curve and, when they do, enumerate all their $\mathbb{F}_q$-points. Then, using the addition formula on E, we write down the ideal $I \subset \mathbb{F}_q[x, y]$ whose vanishing locus inside $\mathbb{A}^2$ is the set of points $P = (x, y) \in E(\overline{\mathbb{F}_q})$ such that $\phi(P) = P + P_0$. As we showed before, the set of such points is non-empty, hence I is a proper ideal and we can find a maximal ideal $\mathfrak{m}$ containing I. We don't need general algorithms for primary decomposition since we can take $\mathfrak{m} = (\mu(x), \lambda(x, y))$, with (μ) being an irreducible factor of the generator of the ideal $J \cap \mathbb{F}_q[x]$ and $\lambda(x, y)$ being an irreducible factor of the image of the Weierstrass equation of E inside $(\mathbb{F}_q[x]/\mu)[y]$. Since the Weiestrass polynomial is monic in y, we can assume that λ is monic in y too. Hence there is a point $P_1 = (x_1, y_1)$ in the vanishing locus of $(\mu(x), \lambda(x, y)) = \mathfrak{m}$. Since $\mathfrak{m}$ contains I, the point P_1 lies on E and satisfies $\phi(P_1) = P_1 + P_0$. The maximality of $\mathfrak{m}$ implies that $\mathbb{F}_q[x, y](\mathfrak{m}) = \mathbb{F}_q(x_1, y_1) = K'$. Hence $\mathfrak{m}$ is the elliptic presentation we want. □

Notation 4.1.6. For the rest of the article $\mathbb{F}_q$ is a finite field with q elements, $\overline{\mathbb{F}_q}$ is its algebraic closure, K is a finite extension of $\mathbb{F}_q$, the ideal $\mathfrak{m} \subset \mathbb{F}_q[x, y]$ is a $(E/\mathbb{F}_q, P_0)$-presentation of K, the map $\phi\colon E \to E$ is the q-th Frobenius and $P_1 = (x_1, y_1) \in E(\overline{\mathbb{F}_q})$ is a point such that $\mathfrak{m} = \{f \in \mathbb{F}_q[x, y] : f(x_1, y_1) = 0\}$. By O_E we denote the neutral element of $E(\mathbb{F}_q)$.

4.2 Traps

As first pointed out in [27], there are certain polynomials, called "traps" for which the descent procedure in [19] does not work. In [19] such traps are dealt with differently than the other polynomials. In [49] the notion of "trap" is extended: it includes not only polynomials for which the descent procedure is proven not to work, but also polynomials

for which the authors do not give proof of the descent's correctness. In [49] traps are avoided by the algorithm.

We describe a descent procedure stated in terms of points and divisors on E and there are certain points in $E(\overline{\mathbb{F}_q})$ that play the role of "traps", as in [49]. The definition of this subset of $E(\overline{\mathbb{F}_q})$ is rather cumbersome, but it is easy to deduce that we have less than $15q^4$ traps. In particular, in contrast to [49], we can include them in the factor base.

Definition 4.2.1. A point $P \in E(\overline{\mathbb{F}_q})$ is a *trap* if it satisfies one of the following conditions:

$$2P = 0\,, \quad \text{or} \quad (2\phi - \mathrm{Id})(\phi^2 - \phi + \mathrm{Id})(P) = P_0\,, \quad \text{or} \quad (2\phi - \mathrm{Id})(\phi + \mathrm{Id})(P) = 2P_0$$
$$\text{or } (\phi^4 - \mathrm{Id})(P) = 4P_0\,, \quad \text{or } 2(\phi^3 - \mathrm{Id})(P) = 6P_0\,, \quad \text{or} \quad (2\phi + \mathrm{Id})(\phi - \mathrm{Id})(P) = 2P_0\,.$$

We explain why these points interfere with our strategy of proof in (4.7.2.2) and at the beginning of the proof of Claim 4.8.2.3.

4.3 Divisors and discrete logarithm

For us a divisor on E is a formal sum

$$D = \sum_{P \in E(\overline{\mathbb{F}_q})} n_P P\,,$$

where the n_P's are integers and $n_P = 0$ for all but a finite number of P's. The Galois group of $\mathbb{F}_q$ acts on the group of divisors by the formula

$$\sigma\left(\sum_{P \in E(\overline{\mathbb{F}_q})} n_P P\right) = \sum_{P \in E(\overline{\mathbb{F}_q})} n_P\, \sigma(P)\,.$$

For any algebraic extension $\mathbb{F}_q \subset k$ we define the set of divisors *defined over* k, denoted $\mathrm{Div}_k(E)$, to be the set of divisors D such that $\sigma D = D$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/k)$. We say that a divisor is *irreducible over* k if it is the sum, with multiplicity 1, of all the $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$-conjugates of some point $P \in E(\overline{\mathbb{F}_q})$. Every divisor defined over k is a $\mathbb{Z}$-combination of irreducible divisors over k. We refer to [97, Chapter 2] for the definitions of principal divisor and support of a divisor.

We need two quantities to describe the "complexity" of a divisor. The first one is the *absolute degree* of a divisor, defined as as

$$\mathrm{absdeg}\left(\sum_{P \in E(\overline{\mathbb{F}_q})} n_P(P)\right) := \sum_{P \in E(\overline{\mathbb{F}_q})} |n_P|\,.$$

The second quantity is analogous to the degree of the splitting field of a polynomial, but we decide to "ignore" trap points. We say that a point is *good* if it is not a trap point, we say that a divisor on E is *good* if it is supported outside the set of traps. Given an algebraic extension $\mathbb{F}_q \subset k$ and a divisor $D \in \mathrm{Div}_k(E)$, there is a unique good divisor D^{good}, defined over k, such that $D - D^{\mathrm{good}}$ is supported on the set of trap points. We define the *essential degree of D over k* to be the least common multiple of the degrees of the irreducible divisors appearing in the support of D^{good}. In other words, if we denote as $k(D^{\mathrm{good}})$ the minimal algebraic extension $\widetilde{k} \supset k$ such that the support of D is contained in $E(\widetilde{k})$, then

$$\mathrm{essdeg}_k(D) := [k(D^{\mathrm{good}}) : k] .$$

If $D^{\mathrm{good}} = 0$ we take $\mathrm{essdeg}_k(D) = 1$.

Now consider the discrete logarithm problem in a field having an elliptic presentation $\mathfrak{m}$. First of all, if q is small compared to $\#K$, for example $q \leq (\log K)^4$ as in Proposition 4.1.5, and if we are able to compute discrete logarithms in $K^\times/\mathbb{F}_q^\times$ in quasi-polynomial time, then we can also compute discrete logarithms in $K^\times$ in quasi-polynomial time. Hence in the rest of the article we are concerned with computing discrete logarithms in $K^\times/\mathbb{F}_q^\times$.

Denoting $\mathbb{F}_q[x,y]_{\mathfrak{m}}$ the localization of $\mathbb{F}_q[x,y]$ at the maximal ideal $\mathfrak{m}$, we have

$$K \cong \mathbb{F}_q[x,y]/\mathfrak{m} \cong \mathbb{F}_q[x,y]_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}} .$$

An element f of $(\mathbb{F}_q[x,y]_{\mathfrak{m}})^\times$ defines a rational function on E which is defined over $\mathbb{F}_q$ and regular and non-vanishing in P_1. We represent elements in $K^\times/\mathbb{F}_q^\times$ with elements of $\mathbb{F}_q(E)$ that are regular and non-vanishing on P_1.

Let g, h be elements of $\mathbb{F}_q(E)$ both regular and non-vanishing on P_1 and let us suppose that g generates the group $K^\times/\mathbb{F}_q^\times$. Then the logarithm of h in base g is a well defined integer modulo $\frac{\#K-1}{q-1}$ that we denote $\log_{\mathfrak{m},g}(h)$ or simply $\log h$. Since we are working modulo $\mathbb{F}_q^\times$, the logarithm of h only depends on the divisor of zeroes and poles of h: if $h' \in \mathbb{F}_q(E)$ satisfies $\mathrm{div}(h) = \mathrm{div}(h')$, then $h/h' \in \mathbb{F}_q^\times$ and consequently $\log(h) = \log(h')$. Hence, putting

$$\log(\mathrm{div}(h)) := \log(h) ,$$

we define the discrete logarithm as homomorphism whose domain is the subgroup of $\mathrm{Div}_{\mathbb{F}_q}(E)$ made of principal divisors, supported outside P_1 and whose image is $\mathbb{Z}/(\frac{\#K-1}{q-1})\mathbb{Z}$. The kernel of this morphism is a subgroup of $\mathrm{Div}_{\mathbb{F}_q}(E)$, hence it defines the following equivalence relation on $\mathrm{Div}_{\mathbb{F}_q}(E)$

$$\begin{aligned} D_1 \sim D_2 &\iff D_1 - D_2 \in \mathrm{Ker}(\log) \\ &\iff \exists f \in \mathbb{F}_q(E) \text{ such that } f(P_1) = 1 \text{ and } \mathrm{div}(f) = D_1 - D_2 . \end{aligned} \tag{4.3.1}$$

We notice that this equivalence relation does not depend on g and that, given rational functions $h_1, h_2 \in \mathbb{F}_q(E)$ regular and non-vanishing on P_1, we have $\log h_1 = \log h_2$ if and only if $\mathrm{div}(h_1) \sim \mathrm{div}(h_2)$. Motivated by this, for all divisors $D_1, D_2 \in \mathrm{Div}_{\mathbb{F}_q}(E)$ we use the notation

$$\log_{\mathfrak{m}} D_1 = \log_{\mathfrak{m}} D_2 \iff D_1 \sim D_2 \,.$$

Notice that we do not define the expression $\log_{\mathfrak{m}}(D)$ or $\log_{\mathfrak{m},g}(D)$ for any D in $\mathrm{Div}_{\mathbb{F}_q}(E)$, since the function log might not extend to a morphism $\mathrm{Div}_{\mathbb{F}_q}(E) \to \mathbb{Z}/(\frac{\#K-1}{q-1})\mathbb{Z}$. In our algorithm we use the equivalence relation (4.3.1) to recover equalities of the form $\log h_1 = \log h_2$.

4.4 The main algorithm

As in [49] our algorithm is based on a descent procedure, stated in terms of divisors on E.

Theorem 4.4.1. *There exists an algorithm, described in the proof, that takes as input an $(E/\mathbb{F}_q, P_0)$-presentation $\mathfrak{m}$ and a divisor $D \in \mathrm{Div}_{\mathbb{F}_q}(E)$ such that $\mathrm{essdeg}_{\mathbb{F}_q}(D) = 2^m$ for some integer $m \geq 7$ and computes a divisor $D' \in \mathrm{Div}_{\mathbb{F}_q}(E)$ such that*

$$\log_{\mathfrak{m}} D = \log_{\mathfrak{m}} D' \,, \quad (\mathrm{essdeg}_{\mathbb{F}_q} D') \mid 2^{m-1} \,, \quad \mathrm{absdeg}(D') \leq 4q^2 \mathrm{absdeg} D \,.$$

This algorithm is probabilistic and runs in expected polynomial time in $q\mathrm{absdeg}(D)$.

Applying repeatedly the algorithm of the above theorem we deduce the following result.

Corollary 4.4.2. *There exists an algorithm, described in the proof, that takes as input an $(E/\mathbb{F}_q, P_0)$-presentation and a divisor $D \in \mathrm{Div}_{\mathbb{F}_q}(E)$ such that $\mathrm{essdeg}_{\mathbb{F}_q} D = 2^m$ for some integer m and computes a divisor $D' \in \mathrm{Div}_{\mathbb{F}_q}(E)$ such that*

$$\log_{\mathfrak{m}} D = \log_{\mathfrak{m}} D' \,, \quad \mathrm{essdeg}_{\mathbb{F}_q} D' \mid 64 \,, \quad \mathrm{absdeg}(D') \leq (2q)^{2m} \mathrm{absdeg}(D) \,.$$

This algorithm is probabilistic and runs in expected polynomial time in $q^m\mathrm{absdeg}(D)$.

The algorithm in [49] is based on the descent procedure [49, Theorem 3]. Using the same ideas we use the descent procedure of the last corollary to describe our main algorithm, which computes discrete logarithms in finite fields with an elliptic presentation.

The idea is setting up an index calculus with factor base the irreducible divisors whose essential degree divides 64. To collect relations we use a "zig-zag descent": for every $f = g^a h^b$, we first use the polynomial μ determined in Remark 4.1.4 to find

$f' \equiv f \bmod \mathfrak{m}$ such that the essential degree of $\mathrm{div}(f')$ is a power of 2, and we then apply the descent procedure to express $\log(f) = \log(f')$ as the logarithm of sums of elements in the factor base.

Main Algorithm Input: an $(E/\mathbb{F}_q, P_0)$-epresentation $\mathfrak{m} \subset \mathbb{F}_q[x,y]$ of a field K and two polynomials $g, h \in \mathbb{F}_q[x,y] \setminus \mathfrak{m}$ such that g generates the group $(\mathbb{F}_q[x,y]/\mathfrak{m})^\times / \mathbb{F}_q^\times$.

Output: an integer z such that

$$g^z \equiv \gamma \cdot h \pmod{\mathfrak{m}} \quad \text{for some } \gamma \in \mathbb{F}_q^\times ,$$

which is equivalent to $g^z = h$ in the group $K^\times/\mathbb{F}_q^\times$.

1. *Preparation:* Compute the monic polynomial $\mu \in \mathbb{F}_q[x]$ generating the ideal $\mathfrak{m} \cap \mathbb{F}_q[x]$. Compute polynomials $\tilde{g}, \tilde{h} \in \mathbb{F}_q[x]$ such that $\tilde{g} \equiv g$ and $\tilde{h} \equiv h$ modulo $\mathfrak{m}$. Put $c := \#E(\mathbb{F}_q)$, $n := \deg \mu$ and $m := \lceil \log n \rceil + 3$.

2. *Factor base:* List the irreducible divisors $D_1, \ldots, D_t \in \mathrm{Div}_{\mathbb{F}_q}(E)$ that do not contain P_1 and either have degree dividing 64 or are supported on the trap points.

3. *Collecting relations*: For $j = 1, \ldots, t+1$ do the following:

   Pick random integers $\alpha_j, \beta_j \in \{1, \ldots, \frac{q^n-1}{q-1}\}$ and compute $\tilde{g}^{\alpha_j}\tilde{h}^{\beta_j}$. Pick random polynomials $f(x)$ of degree 2^m such that $f \equiv \tilde{g}^{\alpha_j}\tilde{h}^{\beta_j} \pmod{\mu}$ until f is irreducible. Apply the descent procedure in Corollary 4.4.2 to find $v_j = (v_{j,1}, \ldots, v_{j,t}) \in \mathbb{Z}^t$ such that

   $$\log_{\mathfrak{m}}(\mathrm{div}(f)) = \log_{\mathfrak{m}}(v_{j,1}D_1 + \ldots + v_{j,t}D_t) .$$

4. *Linear algebra*: Compute $d_1, \ldots, d_{t+1} \in \mathbb{Z}$ such that $\gcd(d_1, \ldots, d_{t+1}) = 1$ and

   $$d_1 v_1 + \ldots + d_{t+1} v_{t+1} \equiv (0, \ldots, 0) \pmod{\tfrac{q^n-1}{q-1}c} .$$

   Put $a := d_1\alpha_1 + \ldots + d_{t+1}\alpha_{t+1}$ and $b := d_1\beta_1 + \ldots + d_{t+1}\beta_{t+1}$.

5. *Finished?*: If b is not invertible modulo $\frac{q^n-1}{q-1}$ go back to step 3, otherwise output

   $$z := -ab^{-1} \left(\bmod \tfrac{q^n-1}{q-1}\right)$$

Analysis of the main algorithm We first prove, assuming Theorem 4.4.1, that the algorithm, when it terminates, gives correct output. First of all we notice that, as explained in Remark 4.1.4, the polynomials $\mu, \tilde{g}$ and $\tilde{h}$ exist and that $\tilde{g}$ and $\tilde{h}$ define the same element as g, respectively h, in $K \cong \mathbb{F}_q[x,y]/\mathfrak{m}$. Let d_j, α_j, β_j and v_j be the

integers and vectors of integers stored at the beginning of the fourth step the last time it is executed. By definition of d_j, we have

$$\sum_{j=1}^{t+1}\sum_{i=1}^{t} d_j v_{j,i} D_i = \tfrac{q^n-1}{q-1} c \cdot D\,,$$

for a certain $D \in \mathrm{Div}_{\mathbb{F}_q}(E)$. The divisor cD is principal because $c = \#\mathrm{Pic}^0(E/\mathbb{F}_q)$ and, since for all j the divisor $\sum_i v_{j,i} D_i$ is principal, D has degree 0. Choosing λ in $\mathbb{F}_q(E)$ such that $\mathrm{div}(\lambda) = cD$, we have

$$\sum_{j=1}^{t+1}\sum_{i=1}^{t} d_j v_{j,i} D_i = \mathrm{div}(\lambda^{\frac{q^n-1}{q-1}})\,. \tag{4.4.3}$$

Writing log for $\log_{\mathfrak{m},g}$, by definition of v_j we have

$$\log(g^{\alpha_j} h^{\beta_j}) = \log\left(\sum_{i=1}^{t} v_{j,i} D_i\right)\,.$$

This, together with Equation (4.4.3), imply the following equalities in $\mathbb{Z}/\frac{q^n-1}{q-1}\mathbb{Z}$

$$\begin{aligned} a + b\log(h) &= \sum_{j=1}^{t+1} d_j(\alpha_j + \beta_j \log(h)) = \sum_{j=1}^{t+1} d_j \log(g^{\alpha_j} h^{\beta_j}) = \sum_{j=1}^{t+1} d_j \log\left(\sum_{i=1}^{t} v_{j,i} D_i\right) \\ &= \log\left(\sum_{j=1}^{t+1}\sum_{i=1}^{t} d_j v_{j,i} D_i\right) = \log\left(\mathrm{div}(\lambda^{\frac{q^n-1}{q-1}})\right) = \tfrac{q^n-1}{q-1}\log(\lambda) = 0\,, \end{aligned}$$

implying that the output z of the algorithm is correct.

We now estimate the running time step by step. The first step can be performed with easy Groebner basis computations. Now the second step. We represent irreducible divisors D not supported on O_E in the following way: either D is the vanishing locus of a prime ideal $(a(x), W(x,y))$ with a monic and irreducible and W the Weierstrass polynomial defining E, or D is the vanishing locus of a prime ideal $(a(x), y - b(x))$ for some polynomials $a, b \in \mathbb{F}_q[x]$ and a monic irreducible; in the first case $\deg D = 2\deg a$, in the second case $\deg D = \deg a$. We can list all the irreducible divisors with degree dividing 64 by listing all monic irreducible polynomials $\mu_1, \ldots, \mu_r \in \mathbb{F}_q[x]$ of degree dividing 64 and, for each i compute the prime ideals containing (μ_i, W), which amounts to factoring W as a polynomial in y, considered over the field $\mathbb{F}_q[x]/\mu_i$. Listing all the divisors supported on the trap points can be done case by case. For example we can list the irreducible divisors supported on the set $S := \{P \in E(\overline{\mathbb{F}_q}) : \phi^4(P) - P = 4P_0\}$ by writing down, with the addition formula on E, an ideal $J \subset \mathbb{F}_q[x,y]$ whose vanishing

locus is $S \subset \mathbb{A}^2(\overline{\mathbb{F}}_q)$ and computing all the prime ideals containing J. The divisor O_E appears among $D_1, \ldots, D_s$ because O_E is a trap point. Since there are q^{64} monic polynomials of degree 64 and at most $15q^4$ trap points and since, using [15], factoring a polynomial of degree d in $\mathbb{F}_q[x]$ takes on average $O(\log(q)d^3)$ operations, the second step takes polynomial time in q. Moreover, we have $t \leq 2q^{64}$.

Now the third step. By [100, Theorem 5.1], if $f(x)$ is a random polynomial of degree 2^m congruent to $\tilde{g}^{\alpha_j}\tilde{h}^{\beta_j}$ modulo μ, then the probability of f being irreducible is at least 2^{-m-1}. Therefore finding a good f requires on average $O(2^m) = O(n)$ primality tests, hence $O(n^4 \log q)$ operations. By assumption finding the vector v_j requires polynomial time in $q^m 2^{m+1}$. We deduce that the third step has probabilistic complexity $tq^{O(\log n)} = q^{O(\log n)}$.

The fourth step can be can be performed by computing a Hermite normal form of the matrix having the v_j's as columns. Since $c \leq q+2\sqrt{q}+1$, the entries of the v_j are at most as big as $4q^{n+1}$. Therefore the fourth step is polynomial in $t\log(q^n)$, hence polynomial in n.

The last step only requires arithmetic modulo $(q^n-1)/(q-1)$.

To understand how many times each step is repeated on average, we need to estimate the probability that, in the last step, b is invertible modulo $(q^n-1)/(q-1)$ and to do so we look at the quantities in the algorithms as if they were random variables. The vector $(d_1, \ldots, d_{t+1})$ only depends on the elements $h^{\alpha_j}g^{\beta_j}$'s and on the randomness contained in the descent procedure and in step 2. Since the α_j's and β_j's are independent variables and since g is a generator, we deduce that the vector $(\beta_1, \ldots, \beta_{t+1})$ is independent of $(g^{\alpha_1}h^{\beta_1}, \ldots, g^{\alpha_{t+1}}h^{\beta_{t*1}})$, hence also independent of the vector $(d_1, \ldots, d_{t+1})$. Since $(\beta_1, \ldots, \beta_{t+1})$ takes on all values in $\{0, \ldots, q^n - 1\}^{t+1}$ with the same probability and $\gcd(d_1, \ldots, d_{t+1}) = 1$, then

$$b = d_1\beta_1 + \ldots d_{t+1}\beta_{t+1}$$

takes all values in $\mathbb{Z}/(q^n - 1)\mathbb{Z}$ with the same probability. Hence

$$\left(\text{probability that } b \text{ is coprime to } \tfrac{q^n-1}{q-1}\right) = \phi\left(\tfrac{q^n-1}{q-1}\right) / \tfrac{q^n-1}{q-1} \gg \frac{1}{\log\log q^n}$$

When running the algorithm, the first and the second step get executed once and the other steps get executed the same number of times, say r, whose expected value is the inverse of the above probability. Since r is $O(\log\log(q^n))$ on average and each step has average complexity at most $q^{O(\log n)}$, the average complexity of the algorithm is $O(q^{O(\log n)})$. Hence, assuming Theorem 4.4.1 we have proved the following theorem.

Theorem 4.4.4. *The above Main Algorithm solves the discrete logarithm problem in the group $K^\times/\mathbb{F}_q^\times$ for all finite fields K having an elliptic presentation $\mathfrak{m} \subset \mathbb{F}_q[x, y]$. It runs in expected time $q^{O(\log[K:\mathbb{F}_q])}$.*

Theorem 4.0.1 follows from Theorem 4.4.4 and Proposition 4.1.5: the latter states that any finite field of small characteristic K can be embedded in a slightly larger field K' having an elliptic presentation $\mathfrak{m} \subset \mathbb{F}_q[x,y]$ such that $q \leq \log(\#K')^4$ and Theorem 4.0.1 implies that the discrete logarithm problem is at most quasi-polynomial for such a K'. Moreover, by Proposition 4.1.5, such a K', together with its elliptic presentation, can be found in polynomial time in $\log(\#K)$, by [66] we can compute an embedding $K \hookrightarrow K'$ in polynomial time in $\log(\#K)$ and by [89, Theorem 15] a random element $g' \in K'$ has probability $\phi(\#K')/\#K' \gg 1/\log\log \#K'$ of being a generator of K': hence, given elements $g, h \in K$, we can compute $\log_g(h)$ by embedding K inside K' and trying to compute the pair $(\log_{g'} g, \log_{g'} h)$ for different random values of $g' \in K'$.

Proposition 4.1.5 is proven, while Theorem 4.4.4 relies on the the existence of a descent procedure as described in Theorem 4.4.1. In the rest of the article, we describe this descent procedure.

4.5 Strategy of proof of Theorem 4.4.1: the descent procedure

Since the descent is trivial for divisors supported on the trap points, it is enough to prove Theorem 4.4.1 and describe the descent procedure for divisors D that are good and irreducible over $\mathbb{F}_q$. In other words, if we write $2^m = 4l$, we can suppose that

$$D = Q + \sigma Q + \ldots + \sigma^{4l-1} Q\,,$$

where Q is a good point on E such that $[\mathbb{F}_q(Q) : \mathbb{F}_q] = 4l = 2^m$ and σ is a generator of $\mathrm{Gal}(\mathbb{F}_q(Q)/\mathbb{F}_q)$. Let k be the unique subfield of $\mathbb{F}_q(Q)$ such that $[k : \mathbb{F}_q] = l$ and let us define

$$\tilde{D} := Q + \sigma^l Q + \sigma^{2l} Q + \sigma^{3l} Q \quad \in \mathrm{Div}_k(E)\,.$$

We can do a sort of "base change to k" and work with $\tilde{D}$. Suppose we have an algorithm to find a divisor $\tilde{D}' \in \mathrm{Div}_k(E)$ such that

$$\mathrm{absdeg}\tilde{D}' \leq 16q^2\,, \quad \mathrm{essdeg}_k \tilde{D}' \mid 2\,,$$

and a function $g \in k(E)$ such that

$$\mathrm{div}(g) = \tilde{D} - \tilde{D}'\,, \quad g(\tau(P_1)) = 1 \quad \text{for all } \tau \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)\,. \tag{4.5.1}$$

Then the divisor

$$D' := \tilde{D}' + \sigma(\tilde{D}') + \ldots \sigma^{l-1}(\tilde{D}')\,,$$

satisfies the conditions in Theorem 4.4.1: the absolute and essential degree of D' are easy to estimate and we have $\log_{\mathfrak{m}} D = \log_{\mathfrak{m}} D'$ because the rational function $f := gg^{\sigma} \cdots g^{\sigma^{l-1}}$ satisfies $f(P_1) = 1$ and $\mathrm{div}(f) = D - D'$.

Hence, in order to prove Theorem 4.4.1, it is enough to describe a probabilistic algorithm that takes k and $\tilde{D}$ as input and, in expected polynomial time in ql, computes a good divisor $\tilde{D}'$ with the properties above. We do it in two steps and we replace the second part of Equation (4.5.1) with a stronger requirement: we ask that $g(P) = 1$ for all the points $P \in E(\overline{\mathbb{F}_q})$ such that $\phi(P) = P + P_0$. Moreover, the hypothesis that l is a power of 2 is not necessary.

Proposition 4.5.2. *There is an algorithm, described in the proof, with the following property*

- *it takes as input an $(E/\mathbb{F}_q, P_0)$-presentation, a finite field extension $\mathbb{F}_q \subset k$ of degree $l \geq 80$ and a divisor $D \in \mathrm{Div}_k(E)$ such that $\mathrm{essdeg}_k D = 4$*
- *it computes a rational function $g \in k(E)$ and a divisor $D' = D_1 + D_2 \in \mathrm{Div}_k(E)$ such that*

$$D - D' = \mathrm{div}(g)\,, \quad g(P) = 1 \text{ for all } P \in E(\overline{\mathbb{F}_q}) \text{ such that } \phi(P) = P + P_0\,,$$
$$\mathrm{essdeg}_k(D_1) \mid 3\,, \quad \mathrm{essdeg}_k(D_2) \mid 2\,, \quad \mathrm{absdeg} D_1 + \mathrm{absdeg} D_2 \leq 2q\mathrm{absdeg} D\,;$$

- *it is probabilistic and runs in expected polynomial time in $q \cdot \log(\#k) \cdot \mathrm{absdeg}(D)$.*

Proposition 4.5.3. *There is an algorithm, described in the proof, with the following property*

- *it takes as input an $(E/\mathbb{F}_q, P_0)$-presentation, an extension of finite fields $\mathbb{F}_q \subset k$ of degree at least 80 and a divisor $D \in \mathrm{Div}_k(E)$ such that $\mathrm{essdeg}_k D = 3$;*
- *it computes a rational function $g \in k(E)$ and a divisor $D' \in \mathrm{Div}_k(E)$ such that*

$$D - D' = \mathrm{div}(g)\,, \quad g(P) = 1 \text{ for all } P \in E(\overline{\mathbb{F}_q}) \text{ such that } \phi(P) = P + P_0\,,$$
$$\mathrm{essdeg}_k(D') \mid 2\,, \quad \mathrm{absdeg}(D') \leq 2q\mathrm{absdeg}(D)\,;$$

- *it is probabilistic and runs in expected polynomial time in $q \cdot \log(\#k) \cdot \mathrm{absdeg}(D)$.*

We now describe our strategy to prove the above two propositions. Let $D \in \mathrm{Div}_k(E)$ be a divisor such that $\epsilon := \mathrm{essdeg}_k(D)$ is either equal to 3 (the case of Proposition 4.5.3) or 4 (the case of Proposition 4.5.2). Let x, y be the usual coordinates on E and let $h \to h^{\phi}$ be the automorphism of $k(E)$ such that $x^{\phi} = x$, $y^{\phi} = y$ and $\alpha^{\phi} = \alpha^q$ for all

$\alpha \in k$. As before we can suppose that D is good and irreducible over k. In other words, we suppose

$$D = Q + \ldots + \sigma^{\varepsilon-1}Q\,,$$

where Q is a good point on E defined over an extension of k of degree ε and σ is a generator of $\mathrm{Gal}(k(Q)/k)$. For every point $P \in E(\overline{\mathbb{F}_q})$ such that $\phi(P) = P + P_0$ and for every function $f \in k(E)$ regular on P we have

$$f(P)^q = f^\phi(\phi(P)) = f^\phi(P + P_0) = (f^\phi \circ \tau_{P_0})(P)\,, \tag{4.5.4}$$

where τ_{P_0} is the translation by P_0 on E. Hence, for any choice of $a, b, c, d \in k$ such that $cf^{q+1}+df^q+af+b$ does not vanish on P, we have

$$\frac{(cf+d)(f^\phi \circ \tau_{P_0}) + af + b}{cf^{q+1} + df^q + af + b}(P) = 1\,.$$

Hence we look for a function g as in Propositions 4.5.2 or 4.5.3 having the shape

$$g = \frac{(cf+d)(f^\phi \circ \tau_{P_0}) + af + b}{cf^{q+1} + df^q + af + b}\,, \tag{4.5.5}$$

for some $a, b, c, d \in k$ and $f \in k(E)$. Heuristically, the advantage of such a g, is that, if f has few poles, then the numerator in the above expression also has few poles and the denominator has a probability about $1/q^3$ of splitting into linear polynomials in f.

We now look for conditions on f and a, b, c, d implying that the function g and the divisor

$$D' := D - \mathrm{div}(g)\,, \tag{4.5.6}$$

have the desired properties. If P is a pole of g, then P is either a pole of f, a pole of $f^\phi \circ \tau_{P_0}$ or a zero of $cf^{q+1}+df^q+af+b$. Since all poles P of g appear in the support of D', we want all these poles to satisfy the inequality $[k(P) : k] \leq \varepsilon - 1$. This happens if the following conditions are satisfied:

(I) the function f has at most $\varepsilon-1$ poles counted with multiplicity;

(II) the polynomial $cT^{q+1} + dT^q + aT + b$ splits into linear factors in $k[T]$.

We want Q and all its conjugates to be zeroes of g. If the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has rank 0 or 1, then $g = (a'f^\phi+b')/(a'f^q+b')$ for some $a', b' \in k$ and this, together with condition (I), prevents Q from being a zero of g. We deduce that the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ must be invertible. Moreover we notice that the definition of g only depends on the class of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{PGL}_2(k)$. Assuming (I) and (II), the point Q is neither a pole of f nor a zero of the denominator in (4.5.5). Hence Q and all its conjugates are zeroes of g if and only if they are zeroes of

the numerator of (4.5.5). Assuming (I) and (II), the function $cf+d$ never vanishes on Q or its conjugates. Hence, using the natural action of PGL_2 on $\mathbb{P}^1$, we see that Q and its conjugates are zeroes of g if and only if

(III) $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f(\sigma^i Q) = -f^{\phi}(\sigma^i Q + P_0) \quad$ for $i = 0, 1, \ldots, \varepsilon-1$.

Assuming (I), the numerator of 4.5.5 has at most $2(\varepsilon-1)$ poles and $2(\varepsilon-1)$ zeroes counted with multiplicity. Assuming also (III), the numerator of 4.5.5 has at most $\varepsilon-2$ zeroes that are different from $\sigma^i Q$ and this set of points is stable under the action of $\mathrm{Gal}(\overline{k}/k)$. We deduce that all the zeros $P \neq \sigma^i Q$ of g satisfy the inequality $[k(P) : k] \leq \epsilon-1$. Hence the same inequality is satisfied by all the points in the support of D' . As noticed when defining g, we want that

(IV) for every point P on E such that $\phi(P) = P + P_0$, the function f is regular on P and $cf^{q+1}+df^q+af+b$ does not vanish on P.

Condition (I) implies that $\mathrm{absdeg}(D')$ is at most $2q\epsilon$.

We showed that the conditions (I), (II), (III), (IV) imply that the function g in (4.5.5) and the divisor $D' = D-\mathrm{div}(g)$ satisfy the requirements of Proposition 4.5.2 or Proposition 4.5.3.

Remark 4.5.7. If $Q \notin \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cdot P_1$ is a point such that $\phi(Q) = Q + P_0$, then Equation 4.5.4 implies that conditions (III) and (IV) exclude each other. This explains why such points Q create problems to our strategy and need to be marked as *traps*.

In Section 4.7 and Section 4.8 we prove that there are many such pairs $(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$ and we give a procedure to find them when $\varepsilon = 3$, $\varepsilon = 4$ respectively:

- We choose a family of functions f satisfying (I) and we parametrize them with k-points on a variety $\mathcal{F}$.
- We impose some conditions slightly stronger than (II), (III), (IV), describing a variety $\mathcal{C} \subset \mathcal{F}\times\mathrm{PGL}_2\times\mathbb{A}^1$ with the following property: for any point $(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z) \in \mathcal{C}(k)$, the pair $(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$ satisfies (I), (II), (III), (IV).

  In particular, $\mathcal{C}$ is a curve in the case $\epsilon = 3$, a surface in the case $\epsilon = 4$
- We prove that the geometrically irreducible components of $\mathcal{C}$ are defined over k and we deduce that $\mathcal{C}(k)$ has cardinality at least $\frac{1}{2}(\#k)^{\dim \mathcal{C}}$; this is the point in the proof where we use the technical hypothesis $[k : \mathbb{F}_q] \geq 80$ (details after Equations (4.7.3.3) and 4.8.4.3).

Using $\mathcal{C}$ we can easily describe the algorithms of Proposition 4.5.2 and Proposition 4.5.3, when D is an irreducible divisor defined over k: one first looks for a point

$(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z)$ in $\mathcal{C}(k)$ and then computes g and D using the formulas (4.5.5) and (4.5.6). This procedure takes average polynomial time in $q \log(\#k)$ because, as explained in Sections 4.7.3 and 4.8.4, the variety $\mathcal{C}$ is a closed subvariety of $\mathbb{A}^9$ with degree $O(q^9)$.

4.6 A technical lemma

In this section we take a break from our main topic and we prove Lemma 4.6.6. This lemma is useful to study the variety $\mathcal{C}$ used in the algorithms of Propositions 4.5.2 and 4.5.3. We split the proof into two propositions.

Because of condition (II), we are interested in the splitting field over a finite extension $\mathbb{F}_q \subset k$ of polynomials of the form $c'T^{q+1}+d'T^q+a'T+b' \in k[T]$. In particular, in Sections 4.7 and 4.8 the matrix $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ varies in an algebraic family: we have a variety $\mathcal{B}$ and $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(P)$ where $a, b, c, d \in k(\mathcal{B})$ and P is a point varying in $\mathcal{B}(k)$. We are interested in studying the splitting field of polynomials $cT^{q+1}+dT^q+aT+b$ over function fields, as in the next proposition.

For any extension of fields $k \subset \mathbb{K}$, its *field of constants* is the subfield of $\mathbb{K}$ containing all the elements that are algebraic over k. For any irreducible variety $\mathcal{C}/k$ we have that $\mathcal{C}$ is geometrically irreducible if and only if k is the field of constants of the extension $k \subset k(\mathcal{C})$.

Proposition 4.6.1. *Let $\mathbb{F}_q \subset k$ be an extension of finite fields and let $k \subset \mathbb{K}$ be a field extension with field of constants k. Let $v : \mathbb{K}^\times \to \mathbb{Z}$ be a valuation with ring of integral elements $\mathcal{O}_v \subset \mathbb{K}$ and generator π_v of the maximal ideal of $\mathcal{O}_v$. Let a, b, c, d be elements of $\mathcal{O}_v$ such that*

$$\begin{aligned} &v(ad-bc) = 1, \qquad v(d^q c - a c^q) = 0 \qquad \text{and} \\ &c\lambda^q - c^q(ad-bc)\lambda^{-1} \not\equiv d^q c - a c^q \pmod{\pi_v^2} \quad \forall \lambda \in \mathcal{O}_v^\times . \end{aligned} \tag{4.6.1.1}$$

Then the splitting field of the polynomial

$$F(T) := cT^{q+1} + dT^q + aT + b \quad \in \mathbb{K}[T] ,$$

is an extension of k having field of constants equal to k.

Proof. For any field extension $\mathbb{K} \subset \widetilde{\mathbb{K}}$, we denote $\widetilde{\mathbb{K}}(F)$ the splitting field of F over $\widetilde{\mathbb{K}}$, which is a separable extension of $\widetilde{\mathbb{K}}$ because the discriminant of F is a power of $ad-bc$ and $ad-bc \neq 0$. Since the field of constants of $k \subset \mathbb{K}$ is equal to k, then $\mathbb{K}' := \mathbb{K} \otimes_k \overline{k}$ is a field and the statement of the proposition is equivalent to the equality

$$\mathrm{Gal}(\mathbb{K}(F)/\mathbb{K}) = \mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}') .$$

By [23, Theorems 2.5 and 3.2] there exists a bijection between the roots of F and $\mathbb{P}^1(\mathbb{F}_q)$ that identifies the action of $\mathrm{Gal}(\mathbb{K}(F)/\mathbb{K})$ on the roots with the action of a subgroup of $G := \mathrm{PGL}_2(\mathbb{F}_q)$ on $\mathbb{P}^1(\mathbb{F}_q)$. We choose such a bijection and we identify $\mathrm{Gal}(\mathbb{K}(F)/\mathbb{K})$ and $\mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}')$ with two subgroups of G. If we prove that $\mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}')$ contains a Borel subgroup B of G the proposition follows: the only subgroups of PGL_2 containing B are the whole G and B itself and, since B is not normal inside G, we deduce that either $\mathrm{Gal}(\mathbb{K}(F)/\mathbb{K}) = \mathrm{Gal}(\mathbb{K}(F)/\mathbb{K}') = B$ or $\mathrm{Gal}(\mathbb{K}(F)/\mathbb{K}) = \mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}') = G$.

In the rest of the proof we show that $\mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}')$ contains a Borel subgroup working locally at v. We choose an extension of v to $\mathbb{K}'$ and consider the completion $\mathbb{K}'_v$ of $\mathbb{K}'$. Since $\mathrm{Gal}(\mathbb{K}'_v(F)/\mathbb{K}'_v)$ is a subgroup of $\mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}')$, it is enough to show that $\mathrm{Gal}(\mathbb{K}'_v(F)/\mathbb{K}'_v)$ is a Borel subgroup to prove the proposition. Since $ad-bc \equiv 0$ and $c \not\equiv 0$ modulo π_v, we have

$$F(T) \equiv c\Big(T^q + \frac{a}{c}\Big)\Big(T + \frac{d}{c}\Big) \pmod{\pi_v},$$

and, since $d^q c \neq a c^q \bmod \pi_v$, we deduce that $-\frac{d}{c}$ is a simple root of $F \bmod \pi_v$. By Hensel's Lemma, there exists a root $r_0 \in \mathbb{K}'_v$ of F that is v-integral and congruent to $-\frac{d}{c}$ modulo π_v. The group $\mathrm{Gal}(\mathbb{K}'_v(F)/\mathbb{K}'_v) \subset G$ stabilizes the element of $\mathbb{P}^1(\mathbb{F}_q)$ corresponding to r_0, hence it is contained in a Borel subgroup of G. Since Borel subgroups have cardinality $q(q-1)$, in order to prove the proposition it is enough showing that $[\mathbb{K}'(F) : \mathbb{K}']$ is at least $q(q-1)$. We show that the inertia degree of $\mathbb{K}' \subset \mathbb{K}'(F)$ is at least $q(q-1)$.

Since $\frac{a}{c}$ is a q-th power modulo π_v, then there exists a v-integral element $\gamma \in \mathbb{K}'_v$ such that $F(T) \equiv c(T+\gamma)^q(T + d/c) \bmod \pi_v$. Up to the substitution $F(T) \mapsto F(T-\gamma)$, which does not change $\mathbb{K}'_v(F)$ nor the quantities c, $ad-bc$ and $d^q c - a c^q$, we can suppose that

$$F(T) \equiv c\,T^q\Big(T + \frac{d}{c}\Big) \pmod{\pi_v}.$$

This implies that $v(d/c) = 0$, $v(a) \geq 1$ and $v(b) \geq 1$. If we had $v(b) \geq 2$, then the choice $\lambda := d$ would contradict the last congruence in (4.6.1.1). Hence we have $v(b) = 1$. The Newton polygon of F tells us that the roots $r_0, \ldots, r_q$ of F in the algebraic closure $\overline{\mathbb{K}'_v}$ of $\mathbb{K}'_v$ satisfy

$$v(r_0) = 0\,, \quad v(r_1) = \ldots = v(r_q) = \frac{1}{q}\,. \tag{4.6.2}$$

We now consider the polynomial

$$F_1(T) := F(T + r_1) = c_1 T^{q+1} + d_1 T^q + a_1 T + b_1 = c T^{q+1} + d_1 T^q + a_1 T \quad \in \overline{\mathbb{K}'_v}[T]\,.$$

The roots of F_1 are $r_i - r_1$. Using Equation (4.6.2), we deduce $v(c_1) = v(d_1) = 0$ and $v(a_1) > 0$. Using $a_1 d_1 - b_1 c_1 = ad - bc$, we see that $v(a_1) = v(a_1 d_1 - c_1 b_1) = v(ad-bc) = 1$.

The Newton polygon of F_1 tells us that

$$v(r_2 - r_1) = \ldots = v(r_q - r_1) = \frac{1}{q-1}\,.$$

This, together with Equation (4.6.2) and the fact that $\mathbb{K} \subset \mathbb{K}'$ is unramified, imply that the inertia degree of $\mathbb{K}'_v \subset \mathbb{K}'_v(F)$ is a multiple of $q(q-1)$ and consequently that $\mathrm{Gal}(\mathbb{K}'_v(F)/\mathbb{K}')$ is a Borel subgroup of G. □

We now prove that, for certain choices of $a, b, c, d \in \mathbb{K}$, Equation (4.6.1.1) is satisfied.

Proposition 4.6.3. *Let $\mathbb{K}$ be a field extension of $\mathbb{F}_q$, let $u_1, u_2, u_3, w_1, w_2, w_3$ be distinct elements of $\mathbb{K}$ and let $a, b, c, d \in \mathbb{K}$ be the elements defined by the following equality in $GL_2(\mathbb{K})$*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} w_3^q & w_1^q \\ 1 & 1 \end{pmatrix} \begin{pmatrix} w_1^q - w_2^q & 0 \\ 0 & w_2^q - w_3^q \end{pmatrix} \begin{pmatrix} u_2 - u_3 & 0 \\ 0 & u_1 - u_2 \end{pmatrix} \begin{pmatrix} 1 & -u_1 \\ -1 & u_3 \end{pmatrix}\,.$$

Then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ sends the three elements $u_1, u_2, u_3 \in \mathbb{P}^1(\mathbb{K})$ to $w_1^q, w_2^q, w_3^q \in \mathbb{P}^1(\mathbb{K})$ respectively.

Suppose, moreover, that $\mathbb{K}$ is equipped with a discrete valuation $v : \mathbb{K}^\times \to \mathbb{Z}$, that u_i, w_i are v-integral, that $v(w_i - w_j) = v(w_3 + u_i) = v(u_2 - u_3) = 0$ for $i \neq j$ and that $v(u_1 - u_2) = 1$. Then a, b, c, d satisfy (4.6.1.1).

Proof. To prove first part we notice that, given distinct elements $x, y, z \in \mathbb{K}$, the matrix

$$N_{x,y,z} := \begin{pmatrix} z & x \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x - y & 0 \\ 0 & y - z \end{pmatrix}$$

is invertible and acts on $\mathbb{P}^1(\mathbb{K})$ sending $0, 1, \infty = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ to x, y, z respectively. Using this definition we have $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \det(N_{u_1,u_2,u_3}) N_{w_1^q,w_2^q,w_3^q} N^{-1}_{u_1,u_2,u_3}$, hence $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ acts on $\mathbb{P}^1(\mathbb{K})$ sending

$$u_1 \mapsto 0 \mapsto w_1^q\,, \quad u_2 \mapsto 1 \mapsto w_2^q\,, \quad u_3 \mapsto \infty \mapsto w_3^q\,.$$

Now the second part of the lemma. Computing $\det(N_{u_1,u_2,u_3})$ and $\det(N_{w_1^q,w_2^q,w_3^q})$ we see that

$$ad - bc = (u_1 - u_2)(u_2 - u_3)(u_1 - u_3)(w_1 - w_2)^q (w_2 - w_3)^q (w_1 - w_3)^q$$

hence $v(ad - bc) = v(u_1 - u_2) + v(u_3 - u_1) = 1$ (the element $u_3 - u_1$ has valuation zero because it is the sum of $u_3 - u_2$ and $u_2 - u_1$ that have valuation 0, respectively 1. Writing

a, b, c, d as polynomials in the u_i's and the w_i's, we check that there is a multivariate polynomial f such that

$$\begin{aligned} d^q c - ac^q =& f(u_1,u_2,u_3,w_1,w_2,w_3)\cdot\big(u_1-u_2\big)^q \\ &+ (u_1-u_3)^q(w_1-w_2)^{q^2}(w_1-w_3)^q(u_2+w_2)^q\cdot\big(u_1-u_2\big) \\ &- (w_1-w_2)^{q^2+q}(u_1-u_3)^{q+1}(u_1+w_3)^q\,. \end{aligned} \tag{4.6.4}$$

Since $v(w_2-w_1) = v(u_3-u_1) = v(w_3+u_1) = 0$, we have $v(d^qc-ac^q) = 0$. Let $\mathcal{O}_v$ be the integral subring of $\mathbb{K}$, let $\pi_v := u_1-u_2$, which is a generator of the maximal ideal of $\mathcal{O}_v$. Now suppose by contradiction that there exists $\lambda \in \mathcal{O}_v^\times$ such that

$$c\lambda^q - a^q(ad-bc)\lambda^{-1} \equiv d^qc - ac^q \pmod{\pi_v^2}\,. \tag{4.6.5}$$

Using $ad-bc \equiv 0 \bmod \pi_v$ and the equality $c = (w_1-w_2)^q(u_1-u_3) - \pi_v(w_1-w_3)^q$, we deduce

$$\lambda^q \equiv \frac{d^qc-ac^q}{c} \equiv \Big(-(u_1-u_3)(u_1+w_3)(w_1-w_2)^q\Big)^q \pmod{\pi_v}\,,$$

If we replace λ by some $\lambda' \equiv \lambda$ modulo π_v, then the congruences (4.6.1.1) are still satisfied, hence we may suppose $\lambda = -(u_1-u_3)(u_1+w_3)(w_1-w_2)^q$. Substituting λ and (4.6.4) in (4.6.5) we get

$$\begin{aligned} 0 &\equiv c^q(ad-bc) + (d^qc-ac^q)\lambda - c\lambda^{q+1} \\ &\equiv -\pi_v(w_1-w_2)^{q^2+q}(w_1-w_3)^q(u_1-u_3)^{q+1}(w_2-w_3)^q(w_3+u_3) \qquad \pmod{\pi_v^2} \end{aligned}$$

which is absurd because $v(w_i-w_j) = v(u_1-u_3) = v(w_3+u_3) = 0$. □

We now prove the main result of this section. Varieties like $\mathcal{C}$ in the following lemma arise in Sections 4.7 and 4.8 when imposing conditions (II) and (III). Proving that the components of such curves are defined over k is useful to prove that such varieties have "many" k-rational points and consequently that conditions (II) and (III) are "often" true.

Lemma 4.6.6. *Let $\mathbb{F}_q \subset k$ be an extension of finite fields and let $\mathcal{B}/k$ be a geometrically irreducible variety. Let u_1, u_2, u_3, w_1, w_2, w_3 be distinct elements of $\overline{k}(\mathcal{B})$ and suppose there exists an irreducible divisor $Z \subset \mathcal{B}_{\overline{k}}$, generically contained in the smooth locus of $\mathcal{B}$, such that u_i, w_i are defined on the generic point of Z and such that*

Z is a zero of order 1 of u_1-u_2 and it is not a zero of $w_3+u_i, u_2-u_3, w_i-w_j$ for $i\neq j$.

Let $\mathcal{C} \subset \mathcal{B}\times \mathrm{PGL}_2 \times \mathbb{A}^1$ be the variety whose the points are the tuples $(R, \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right), z)$ such that

$$u_i(R) \text{ are defined and distinct,} \quad w_i(R) \text{ are defined and distinct,} \quad d^qc-ac^q \neq 0,$$
$$\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)\cdot u_i(R) = w_i^q(R) \text{ for } i=1,2,3 \qquad \text{and}$$
$$(d^qc-ac^q)^{q+1}(z^q-z)^{q^2-q} = c^{q^2+1}(ad-bc)^q\Big((z^{q^2}-z)/(z^q-z)\Big)^{q+1}$$

If $\mathcal{C}$ is defined over k, then its geometrically irreducible components are defined over k and pairwise disjoint.

Proof. We first look at the variety $\mathcal{B}_0 \subset \mathcal{B} \times \mathrm{PGL}_2$ whose points are the pairs (R, A) such that

$$u_i(R) \text{ are defined and distinct}, \quad w_i(R) \text{ are defined and distinct},$$
$$A \cdot u_i(R) = w_i^q(R) \text{ for } i = 1, 2, 3\,.$$

Since an element PGL_2 is uniquely determined by its action on three distinct points of $\mathbb{P}^1$, the projection $\mathcal{B}_0 \to \mathcal{B}$ is a birational equivalence, whose inverse, by the first part of Proposition 4.6.3, is given by $R \mapsto \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right)(R)$, where $a_1, b_1, c_1, d_1 \in \overline{k}(\mathcal{B})$ are defined by the following equality in $\mathrm{GL}_2(\overline{k}(\mathcal{B}))$

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} w_3^q & w_1^q \\ 1 & 1 \end{pmatrix} \begin{pmatrix} w_1^q - w_2^q & 0 \\ 0 & w_2^q - w_3^q \end{pmatrix} \begin{pmatrix} u_2 - u_3 & 0 \\ 0 & u_1 - u_2 \end{pmatrix} \begin{pmatrix} 1 & -u_1 \\ -1 & u_3 \end{pmatrix}.$$

Let $v\colon \overline{k}(\mathcal{B})^\times \to \mathbb{Z}$ be the valuation that determines the order of vanishing in Z of a rational function. The second part of Proposition 4.6.3 implies that a_1, b_1, c_1, d_1 satisfy (4.6.1.1), over the field $\overline{k}(\mathcal{B})$. In particular we have $c_1 \neq 0$ and $v(c_1) = 0$. Hence we can define the following rational functions on $\mathcal{C}$

$$a_2 := a_1/c_1\,, \quad b_2 := b_1/c_1\,, \quad c_2 := 1\,, \quad d_2 := d_1/c_1$$

which again satisfy (4.6.1.1) over the field $\overline{k}(\mathcal{B})$. The advantage of a_2, b_2, c_2, d_2 is that, as we now show, they are defined over k. Let $\mathcal{B}_1$ be the projection of $\mathcal{C}$ inside $\mathcal{B} \times \mathrm{PGL}_2$: since $\mathcal{C}$ is defined over k, the variety $\mathcal{B}_1$ is defined over k and, since $\mathcal{B}_1$ is a dense open subvariety of $\mathcal{B}_0$, the variety $\mathcal{B}_1$ is birational equivalent to $\mathcal{B}$ through the natural projection. Since a/c is a rational function on $\mathcal{B}_1$ defined over k, we deduce that $a_2 = a/c$ lies in $k(\mathcal{B}_1) = k(\mathcal{B})$ and analogously $b_2, c_2, d_2 \in k(\mathcal{B})$. A fortiori a_2, b_2, c_2, d_2 satisfy (4.6.1.1) inside the field $\mathbb{K} = k(\mathcal{B})$. By Proposition 4.6.1, k is the field of constants of the extension $k \subset \Sigma$, where Σ is the splitting field of

$$F(T) := c_2 T^{q+1} + d_2 T^q + a_2 T + b_2\,,$$

over $k(\mathcal{B})$. We deduce that there exists a geometrically irreducible variety $\mathcal{E}/k$ having field of rational functions Σ. Let $\pi\colon \mathcal{E} \dashrightarrow \mathcal{B}$ be the rational map induced by $k(\mathcal{B}) \subset \Sigma$ and let $r_0, \ldots, r_q \in \Sigma$ be the roots of F, interpreted as rational functions on $\mathcal{E}$. Using [23, Lemma 2.3] we see that, for any choice of integers $0 \leq i < j < m \leq q$,

$$z = z_{i,j,k} := \frac{r_i - r_j}{r_i - r_k} \in \Sigma = k(\mathcal{E}) \quad \text{satisfies}$$
$$(d_2^q c_2 - a_2 c_2^q)^{q+1} (z^q - z)^{q^2-q} = C_2^{q^2+1} (a_2 d_2 - b_2 c_2)^q \left((z^{q^2} - z)/(z^q - z)\right)^{q+1}$$

Hence, for each $0 \leq i < j < m \leq q$ we get a map

$$\phi_{i,j,m} \colon \mathcal{E} \dashrightarrow \mathcal{C}, \qquad S \longmapsto \left(\pi(S), \left(\begin{smallmatrix} a_2 & b_2 \\ c_2 & d_2 \end{smallmatrix}\right)(S), z_{i,j,m}(S)\right) .$$

Since all the $z_{i,j,m}$ are different, the union of all the images $\phi_{i,j,m}(\mathcal{E})$ is dense inside $\mathcal{C}$. Hence, up to shrinking $\mathcal{C}$, every geometrically irreducible component of $\mathcal{C}$ is also a geometrically irreducible component of $\phi_{i,j,m}(\mathcal{E})$ for some (i,j,m). Since $\mathcal{E}$ is defined over k and geometrically irreducible, the variety $\phi_{i,j,m}(\mathcal{E})$ is also defined over k and geometrically irreducible. We deduce that the irreducible components of $\mathcal{C}$ are defined over k.

Finally, we prove that the components of $\mathcal{C}$ are pairwise disjoint. The projection $\pi \colon \mathcal{C} \to \mathcal{B}_1$ has finite fibers whose number of $\overline{k}$-points counted with multiplicity is q^3-q , that is the degree, in z, of the polynomial

$$(d^q c - a c^q)^{q+1}(z^q - z)^{q^2-q} - c^{q^2+1}(ad-bc)^q \left((z^{q^2} - z)/(z^q - z)\right)^{q+1} .$$

If, by contradiction, there is a point $(R', \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right), z')$ lying in the intersection of two components of $\mathcal{C}$, then the fiber $\pi^{-1}(R', \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right))$ has cardinality smaller than q^3-q. In other words the polynomial

$$G(z) := (d'^q c' - a' c'^q)^{q+1}(z^q - z)^{q^2-q} - c'^{q^2+1}(a'd' - b'c')^q \left((z^{q^2} - z)/(z^q - z)\right)^{q+1} \in \overline{\mathbb{F}_q}[z]$$

has less than q^3-q roots. Since $a'd'-b'c' \neq 0$ and $d^q c' - a' c'^q \neq 0$, there is no root of G that is also a root of $z^q - z$ or $\frac{z^{q^2}-z}{z^q-z}$. In other words, G has no root lying in the finite field $\mathbb{F}_{q^2} \subset \overline{\mathbb{F}_q}$ with q^2 elements. Since z' is a root of G and since G is a $\overline{\mathbb{F}_q}$-linear combination of powers of $z^q - z$ and $\frac{z^{q^2}-z}{z^q-z}$, for any matrix $A \in \mathrm{PGL}_2(\mathbb{F}_q)$, the number $A \cdot z'$ is also a root of G. Since $\#\mathrm{PGL}_2(\mathbb{F}_q) = q^3-q$ is larger than the set of roots of G, there exists a matrix $A \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that $A \cdot z' = z'$, implying that z' lies in $\mathbb{F}_q^2$, which is absurd. □

Remark 4.6.7. Let $\mathbb{F}_q \subset k$ be a field extension and let $F(T) = cT^{q+1} + dT^q + aT + b$ be a polynomial with coefficients in k such that, $ad-bc \neq 0$ and $a^q c - d c^q \neq 0$. By [23, Theorem 4.3 and Lemma 2.3], the polynomial F splits in linear factors over k if and only if there exists an element $z \in k$ such that

$$(d^q c - a c^q)^{q+1}(z^q - z)^{q^2-q} = c^{q^2+1}(ad-bc)^q \left((z^{q^2} - z)/(z^q - z)\right)^{q+1} .$$

In particular, in the notation of the proof of Lemma 4.6.6, we have $\Sigma = k(\mathcal{B})(z_{i,j,m})$ for any choice of integers $0 \leq i < j < m \leq q$. In particular, the map $\phi_{i,j,m}$ is injective, hence it is a birational equivalence between $\mathcal{E}$ and an irreducible component of $\mathcal{C}$. In other words the field of rational functions of an irreducible component of $\mathcal{C}$ is the splitting field of F over $k(\mathcal{B})$.

4.7 Descent 3-to-2

In this section we prove Proposition 4.5.3 for a good irreducible divisor D. Following the notation of Section 4.5 when $\varepsilon = 3$, let k be a finite extension of $\mathbb{F}_q$ of degree at least 80, let Q be a good point on E such that $[k(Q) : k] = 3$, and let σ be a generator of $\mathrm{Gal}(k(Q)/k)$. Then, we look for a function $f \in k(E)$ and a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(k)$ satisfying properties (I), (II), (III), (IV): we describe a curve $\mathcal{C}$ whose k-points give such pairs $(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$, and we prove that there are many k-points on $\mathcal{C}$.

4.7.1 The definition of $\mathcal{C}$

Property (I) requires that $f \in k(E)$ has at most two poles: we look for f of the form

$$f_P := \frac{y - y(P)}{x - x(P)} \tag{4.7.1.1}$$

for some P in $E(k) \setminus \{O_E\}$, since such f_P has exactly two simple poles, namely O_E and $-P$. As explained in Remark 4.6.7, in order to ensure condition (II), it is sufficient imposing that $d^q c \neq a c^q$ and that there exists z in k such that

$$(d^q c - a c^q)^{q+1} (z^q - z)^{q^2-q} = c^{q^2+1} (ad - bc)^q \left((z^{q^2} - z)/(z^q - z) \right)^{q+1} . \tag{4.7.1.2}$$

Notice that definition (4.7.1.1) makes sense for $P \in E(\overline{\mathbb{F}_q}) \setminus \{O_E\}$ and that we have the following symmetry: for any $P, P' \in E(\overline{\mathbb{F}_q}) \setminus O_E$, we have $f_P(P') = f_{P'}(P)$. Using this and the fact that $h^\phi(\phi(P)) = h(P)^q$ for all $h \in \overline{\mathbb{F}_q}(E)$ and $P \in E(\overline{\mathbb{F}_q})$, we have

$$f_P(\sigma^i Q) = f_{\sigma^i Q}(P) , \quad f_P^\phi(\sigma^i Q + P_0) = f_P^\phi(\phi(\sigma^i R)) = f_P(\sigma^i R)^q = f_{\sigma^i R}(P)^q ,$$

where R is the unique point on E such that $\phi(R) = Q + P_0$. Hence (III) is equivalent to

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f_{\sigma_i Q}(P) = -f_{\sigma^i R}(P)^q \quad \text{for each } i = 0, 1, 2 . \tag{4.7.1.3}$$

We now impose (IV). Let B be a point on E such that $\phi(B) = B + P_0$. If the rational function $c f_P^{q+1} + d f_P^q + a f_P + b$ vanishes on B, then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f_B(P) = -f_B(P)^q$. This and Equation (4.7.1.3), when $f_{\sigma^i Q}$ are distinct, imply that the cross ratio of $f_Q(P)$, $f_{\sigma Q}(P)$, $f_{\sigma^2 Q}(P)$, $f_B(P)$ equals the cross ratio of $f_R(P)^q, f_{\sigma R}(P)^q, f_{\sigma^2 R}(P)^q$, $f_B(P)^q$. The poles of f_P are O_E and $-P$. Hence, assuming (4.7.1.3) and the distinctness of $f_{\sigma^i Q}(P)$, condition (IV) is implied by

(4.7.1.4)

$$\text{for all } B \text{ such that } \phi(B) = B + P_0 : \qquad P \neq -B \quad \text{and}$$

$$\mathrm{CrRat}\big(f_Q(P), f_{\sigma Q}(P), f_{\sigma^2 Q}(P), f_B(P)\big) \neq \mathrm{CrRat}\big(f_R(P)^q, f_{\sigma R}(P)^q, f_{\sigma^2 R}(P)^q, f_B(P)^q\big) ,$$

where, given four elements $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{P}^1(\overline{\mathbb{F}_q})$, we write

$$\mathrm{CrRat}(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = \frac{(\lambda_3 - \lambda_1)(\lambda_4 - \lambda_2)}{(\lambda_2 - \lambda_1)(\lambda_4 - \lambda_3)} \in \mathbb{P}^1(\overline{\mathbb{F}_q}),$$

for their cross-ratio, which is defined unless three of the λ_i's are equal.

Finally we define $E' := E \setminus \{O_E, -Q, -R, \dots, -\sigma^2 Q, -\sigma^2 R\}$, so that $f_{\sigma^i R}$ and $f_{\sigma^i Q}$ are regular on E', and we define $\mathcal{C} \subset E' \times \mathrm{PGL}_2 \times \mathbb{A}^1$ as the curve made of points $(P, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z)$ that satisfy Equations (4.7.1.3), (4.7.1.2) and (4.7.1.4), and such that $d^q c - a c^q \neq 0$ and the $f_{\sigma^i Q}(P)$ are distinct.

Notice that $\mathcal{C}$ is defined over k: even though the equations $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) f_{\sigma^i Q}(P) = -f^q_{\sigma^i R}(P)$ on $E' \times \mathrm{PGL}_2$ have coefficients in the field $k(Q)$, the Galois group of $k \subset k(Q)$ permutes these equations. We constructed $\mathcal{C}$ so that, for any point $(P, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z) \in \mathcal{C}(k)$, the pair $(f_P, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$ satisfies properties (I), (II), (III) and (IV).

4.7.2 The irreducible components of $\mathcal{C}$

In this subsection we prove that all the geometrically irreducible components of $\mathcal{C}$ are defined over k. We can leave out (4.7.1.4) from the definition of $\mathcal{C}$. Our strategy is applying Lemma 4.6.6 to the variety $\mathcal{B} = E'$, using the rational functions $u_i = f_{\sigma^{i-1} Q}$, $w_i = -f_{\sigma^{i-1} R}$ and the irreducible divisor Z equals to the point $-Q - \sigma Q \in \mathcal{B}(\overline{\mathbb{F}_q}) \subset E(\overline{\mathbb{F}_q})$.

Notice that, given distinct points $P', P'' \in E(\overline{\mathbb{F}_q}) \setminus \{O_E\}$, the function $f_{P'} - f_{P''}$ is regular at O_E and moreover $(f_{P'} - f_{P''})(O_E) = 0$. Since the sum of zeroes and poles of a rational function is equal to O_E in the group $E(\overline{\mathbb{F}_q})$, we deduce that, given distinct points $P', P'' \in E(\overline{\mathbb{F}_q}) \setminus \{O_E\}$,

(4.7.2.1)

$f_{P'} - f_{P''}$ has two simple poles, namely $-P'$ and $-P''$
and two zeroes counted with multiplicity, namely O_E and $-P' - P''$.

Let $Z := -Q - \sigma Q$. By (4.7.2.1) and the fact that Q is not a trap, the point Q is not a pole of any of the u_i and the w_i and it is not a zero of any of the functions $u_2 - u_3$, $w_3 + u_i$ and $w_i - w_j$ for $i \neq j$: if, for example, $-f_{\sigma R}$ is not regular on Z, then $Z = -R$. Hence, using that σ acts as ϕ^l on $E(\overline{\mathbb{F}_q})$ for $l := [k : \mathbb{F}_q]$, we have

$$Q + P_0 = \phi(R) = \phi(-Z) = \phi^{l+1}(Q) + \phi(Q) \quad \Longrightarrow \quad \phi^{l+1}(Q) = (1 - \phi)(Q) + P_0,$$

hence

(4.7.2.2)

$$\begin{aligned} \phi^3(Q) &= \phi^{3l+3}(Q) = \phi^{2l+2}\left((1-\phi)(Q) + P_0\right) = \left((1-\phi) \circ \phi^{2l+2}\right)(Q) + P_0 \\ &= \left((1-\phi) \circ \phi^{l+1}\right)\left((1-\phi)(Q) + P_0\right) + P_0 = \left((1-\phi) \circ (1-\phi)\right)(\phi^{l+1}(Q)) + P_0 \\ &= (1-\phi)^2\left((1-\phi)(Q) + P_0\right) + P_0 = (1-\phi)^3(Q) + P_0, \end{aligned}$$

implying that

$$((2\phi-1)\circ(\phi^2-\phi+1))(Q) = (\phi^3+(\phi-1)^3)(Q) = P_0\,,$$

which contradicts the hypothesis that Q was not a trap point. Moreover, by (4.7.2.1), the function $f_Q - f_{\sigma Q}$ has a simple zero in Z. Hence, by Lemma 4.6.6, all the geometrically irreducible components of $\mathcal{C}$ are defined over k and disjoint.

4.7.3 k-rational points on $\mathcal{C}$

We now prove that $\#\mathcal{C}(k)$ is larger than $\frac{1}{2}\#k$. The curve $\mathcal{C}$ is contained in the open subset of $(E\setminus\{O_E\})\times \mathrm{PGL}_2\times\mathbb{A}^1$ made of points $((x,y),\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right),z)$ such that $c\neq 0$. Hence $\mathcal{C}$ is contained in $\mathbb{A}^6$, with variables x, y, a, b, d, z and it is defined by the following equations:

- $0 = p_1 := W(x,y)$, the Weierstrass equation defining E;
- $0 = p_2 := (d^q-a)^{q+1}(z^q-z)^{q^2-q} - (ad-b)^q(\frac{z^{q^2}-z}{z^q-z})^{q+1}$, the dehomogenization of (4.7.1.2) in c;
- $0 = p_i(x,y,a,b,d)$ for $i=3,4,5$, obtained by (4.7.1.3) after dehomogenizing in c, substituting $f_{\sigma^i Q}(P)$ and $f_{\sigma^i R}(P)$ by their expressions in x, y and clearing denominators;
- a number of conditions $0\neq q_j$ ensuring that $P\neq -\sigma^i Q$, $P\neq -\sigma^i R$, $d^q-a\neq 0$, $ad-b\neq 0$, that $f_{\sigma^i Q}(P)$ are pairwise distinct and that (4.7.1.4) is satisfied.

In particular, $\mathcal{C}$ can be seen as a closed subvariety of $\mathbb{A}^7$, with variables x, y, a, b, d, z and t defined by the equations $p_1=0,\dots,p_5=0$ and $0=p_6 := tq_1\cdots q_r - 1$.

Let $\mathcal{C}_1,\dots,\mathcal{C}_s$ be the irreducible components of $\mathcal{C}$. By [46, Remark 11.3], we have

$$\#\mathcal{C}(k) \geq \#\mathcal{C}_1(k) \geq \#k - (\delta-1)(\delta-2)(\#k)^{\frac{1}{2}} - K(\mathcal{C}_1)\,, \tag{4.7.3.1}$$

where δ is the degree of $\mathcal{C}_1$ and $K(\mathcal{C}_1)$ is the sum of the Betti numbers of $\mathcal{C}$ relative to the compact ℓ-adic cohomology. Since $\mathcal{C}_1$ is a component of $\mathcal{C}$ then

$$\delta \leq \deg(p_1)\cdots\deg(p_6)\,. \tag{4.7.3.2}$$

Since $\mathcal{C}$ is the disjoint union of the $\mathcal{C}_i$, the Betti numbers of $\mathcal{C}$ are the sums of the Betti numbers of the $\mathcal{C}_i$ and using [58, Corollary of Theorem 1] we deduce that

$$K(\mathcal{C}_1) \leq K(\mathcal{C}) \leq 6\cdot 2^6\cdot\left(3+7\max_{i=1,\dots,6}\{\deg(p_i)\}\right)^8\,. \tag{4.7.3.3}$$

Since $\deg p_1\leq 3$, $\deg p_2\leq q^3+q$, $\deg p_3,\dots,\deg p_5\leq q+2$, $\deg p_7\leq 8q^2+29q+29$, then Equations (4.7.3.1), (4.7.3.2) and (4.7.3.3) imply that $\#\mathcal{C}(k) > \frac{1}{2}(\#k)$ when $\#k\geq q^{80}$ and $q\geq 3$.

4.8 Descent 4-to-3

In this section we prove Proposition 4.5.2 for a good irreducible divisor D. Following the notation of section 4.5 when $\varepsilon = 4$, let k be a finite extension of $\mathbb{F}_q$ of degree at least 80, let Q be a good point on E such that $[k(Q) : k] = 4$, and let σ be a generator of $\mathrm{Gal}(k(Q)/k)$. Then, we look for a function $f \in k(E)$ and a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(k)$ satisfying properties (I), (II), (III), (IV): we describe a surface $\mathcal{C}$ whose k-points give such pairs $(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$, and we prove that there are many k-points on $\mathcal{C}$.

4.8.1 The definition of $\mathcal{C}$

Property (I) requires that $f \in k(E)$ has at most 3 poles: we look for f of the form

$$f = f_{\alpha,\beta,P} := \frac{f_P + \alpha}{f_{\widetilde{P}} + \beta}\,. \tag{4.8.1.1}$$

where α, β are elements of k, the points $P, \widetilde{P}$ lie in $E(k) \setminus \{O_E\}$ and f_P is the rational function defined in (4.7.1.1). For the rest of the article we let α, β and P vary and we fix $\widetilde{P}$ so that

$$f_Q(\widetilde{P}), f_{\sigma Q}(\widetilde{P}), f_{\sigma^2 Q}(\widetilde{P}), f_{\sigma^3 Q}(\widetilde{P}), f_R(\widetilde{P}), f_{\sigma R}(\widetilde{P}), f_{\sigma^2 R}(\widetilde{P}), f_{\sigma^3 R}(\widetilde{P}) \text{ are pairwise distinct.}$$

There is at least one such point $\widetilde{P}$ because $\#(E(k) \setminus \{O_E\}) > \binom{8}{2}$ and by (4.7.2.1) for each $P' \neq P'' \in E(\overline{\mathbb{F}_q}) \setminus \{O_E\}$ there is at most one point $\widetilde{P} \in (E(k) \setminus \{O_E\})$ such that $f_{P'}(P) = f_{P''}(P)$. Notice that the above definition makes sense for any $P \in E(\overline{\mathbb{F}_q})$ and $\alpha, \beta \in \overline{\mathbb{F}_q}$ and that, for any such choice, the function $f_{\alpha,\beta,P}$ has at most three poles counted with multiplicity, namely $-P$ and the zeroes of $f_{\widetilde{P}}+\beta$. Hence condition (I) is automatically satisfied. We write f for $f_{\alpha,\beta,P}$, unless we want to stress the dependence on α, β, P, like in the equations defining $\mathcal{C}$.

As explained in Remark 4.6.7, when $d^q c - a c^q \neq 0$, condition (II), is satisfied if and only if there exists $z \in k$ such that

$$(d^q c - a c^q)^{q+1}(z^q - z)^{q^2-q} = c^{q^2+1}(ad - bc)^q \left((z^{q^2} - z)/(z^q - z)\right)^{q+1}\,. \tag{4.8.1.2}$$

Since $h^\phi(\phi(P)) = h(P)^q$ for all $h \in \overline{\mathbb{F}_q}(E)$ and $P \in E(\overline{\mathbb{F}_q})$, we have

$$-f^\phi(\sigma^i Q + P_0) = -f^\phi(\phi(\sigma^i R)) = -f(\sigma^i R)^q\,,$$

where $R \in E(\overline{\mathbb{F}_q})$ is the unique point such that $\phi(R) = Q + P_0$. Hence property (III) is equivalent to

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f_{\alpha,\beta,P}(\sigma^i Q) = -f_{\alpha,\beta,P}(\sigma^i R)^q \quad \text{for } i = 0, 1, 2, 3\,. \tag{4.8.1.3}$$

Since cross-ratio is invariant under the action of PGL_2 on $\mathbb{P}^1$, the above equation implies that either the cross-ratio of $f(\sigma^0 Q), \ldots, f(\sigma^3 Q)$ is equal to the cross ratio of $f(\sigma^0 R), \ldots$, $f(\sigma^3 R)$, or one of the two cross-ratios is not defined. Hence, assuming that $f(\sigma^i Q)$ are distinct and that $f(\sigma^i R)$ are distinct, Equation (4.8.1.3) implies

(4.8.1.4)
$$\mathrm{CrRat}\big(f_{\alpha,\beta,P}(\sigma^0 Q), \ldots, f_{\alpha,\beta,P}(\sigma^3 Q)\big) = \mathrm{CrRat}\big(f_{\alpha,\beta,P}(\sigma^0 R)^q, \ldots, f_{\alpha,\beta,P}(\sigma^3 R)^q\big).$$

Moreover, supposing that $f(\sigma^i Q)$ and $f(\sigma^i R)$ are distinct, the properties of cross-ratio imply that Equation (4.8.1.3) is equivalent to Equation (4.8.1.4) together with

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f_{\alpha,\beta,P}(\sigma^i Q) = -f_{\alpha,\beta,P}(\sigma^i R)^q \quad \text{for } i = 0, 1, 2\,. \tag{4.8.1.5}$$

We now impose (IV). Let B be a point on E such that $\phi(B) = B + P_0$. If the rational function $cf^{q+1} + df^q + af + b$ vanishes on B, then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) f(B) = -f(B)^q$. This, together with Equation (4.8.1.5) and the fact that $f(\sigma^i Q)$ are all distinct, implies that the cross-ratio of $f(Q), f(\sigma Q), f(\sigma^2 Q), f(B)$ is equal to the cross-ratio of $f^q(R), f^q(\sigma R), f^q(\sigma^2 R)$, $f^q(B)$. A pole of $f_{\alpha,\beta,P}$ is either equal to $-P$ or to a zero of $f_{\widetilde{P}} + \beta \in \overline{\mathbb{F}_q}(E)$. Hence, assuming Equation (4.8.1.5) and the distinctness of $f(\sigma^i Q)$, condition (IV) is implied by

(4.8.1.6)
$$\text{for all } B \text{ such that } \phi(B) = B + P_0 : \qquad P \neq -B\,, \quad \beta + f_{\widetilde{P}}(B) \neq 0 \quad \text{and}$$
$$\mathrm{CrRat}\big(f(Q), f(\sigma Q), f(\sigma^2 Q), f(B)\big) \neq \mathrm{CrRat}\big(f(R)^q, f(\sigma R)^q, f(\sigma^2 R)^q, f(B)^q\big)\,.$$

Let $E' := E \setminus \{O_E, -\sigma^0 Q, -\sigma^0 R, \ldots, -\sigma^3 Q, -\sigma^3 R\}$ and let $\mathcal{C} \subset \mathbb{A}^2 \times E' \times \mathrm{PGL}_2 \times \mathbb{A}^1$ be the surface made of points $(\alpha, \beta, P, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z)$ that satisfy Equations (4.8.1.4), (4.8.1.5), (4.8.1.2) and (4.8.1.6), and such that $\beta + f_{\widetilde{P}}(\sigma^i Q) \neq 0$, $\beta + f_{\widetilde{P}}(\sigma^i R) \neq 0$, $d^q c - a c^q \neq 0$, the $f(\sigma^i Q)$ are distinct and the $f(\sigma^i R)$ are distinct.

The definition of E' and the conditions $\beta + f_{\widetilde{P}}(\sigma^i Q) \neq 0$, $\beta + f_{\widetilde{P}}(\sigma^i R) \neq 0$, ensure that $f(\sigma^i Q)$ and $f(\sigma^i R)$ are well defined. As in subsection 4.7.1, the surface $\mathcal{C}$ is defined over k. If $(\alpha, \beta, P, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z)$ is a k-point on $\mathcal{C}$, then $(f_{\alpha,\beta,P}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$ satisfies (I), (II) and (III) and (IV).

4.8.2 Irreducibility of a projection of $\mathcal{C}$

Before studying the irreducible components of $\mathcal{C}$, we study the closure in $\mathbb{P}^2 \times E$ of the projection of $\mathcal{C}$ in $\mathbb{A}^2 \times E$. Let $\mathcal{B}' \subset \mathbb{A}^2 \times E'$ be the surface whose points are the tuples (α, β, P) such that

$$f_{\alpha,\beta,P}(\sigma^i Q) \text{ are pairwise distinct}\,, \quad f_{\alpha,\beta,P}(\sigma^i R) \text{ are pairwise distinct},$$
$$f_{\widetilde{P}}(\sigma^i Q) + \beta \neq 0\,, \quad f_{\widetilde{P}}(\sigma^i R) + \beta \neq 0\,,$$
$$\mathrm{CrRat}\big(f_{\alpha,\beta,P}(\sigma^0 Q), \ldots, f_{\alpha,\beta,P}(\sigma^3 Q)\big) = \mathrm{CrRat}\big(f_{\alpha,\beta,P}(\sigma^0 R)^q, \ldots, f_{\alpha,\beta,P}(\sigma^3 R)^q\big)\,,$$

and let $\mathcal{B}$ be the closure of $\mathcal{B}'$ inside $\mathbb{P}^2 \times E$. Since the action of PGL_2 on $\mathbb{P}^1$ is triply transitive, the projection $\mathbb{A}^2 \times E \times \mathrm{PGL}_2 \times \mathbb{A}^1 \to \mathbb{A}^2 \times E$ gives a dominant morphism $\mathcal{C} \to \mathcal{B}$ (this is the same argument used in the proof of Lemma 4.6.6 to show that $\mathcal{B}_0 \to \mathcal{B}$ is dominant). Since $\mathcal{C}$ is defined over k, the variety $\mathcal{B}$ is defined over k. In the rest of the subsection we prove that for all but a few choices of $P \in E(k)$ the curve $\mathcal{B}_P := \mathcal{B} \cap (\{P\} \times \mathbb{P}^2)$ is reduced and geometrically irreducible. In other words, we think of P as fixed and we let α and β vary.

We first write an equation for $\mathcal{B}_P$ in $\mathbb{P}^2$. Using the definition of $f_{\alpha,\beta,P}$ we get

$$f_{\alpha,\beta,P}(\sigma^i Q) - f_{\alpha,\beta,p}(\sigma^j Q) = \frac{L_{i,j}(\alpha,\beta,1)}{\big(l_i+\beta\big)\big(l_j+\beta\big)}, \quad f_{\alpha,\beta,P}(\sigma^i R) - f_{\alpha,\beta,P}(\sigma^j R) = \frac{R_{i,j}(\alpha,\beta,1)}{\big(r_i+\beta\big)\big(r_j+\beta\big)},$$

where $l_i := f_{\widetilde{P}}(\sigma^i Q)$, $r_i := f_{\widetilde{P}}(\sigma^i R)$ and $L_{i,j}, R_{i,j} \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ are the linear polynomials

$$\begin{aligned} L_{i,j} &:= \big(l_j - l_i\big)\alpha + \big(f_{\sigma^i Q}(P) - f_{\sigma^j Q}(P)\big)\beta + \big(f_{\sigma^i Q}(P) l_j - f_{\sigma^j Q}(P) l_i\big)\gamma, \\ R_{i,j} &:= \big(r_j - r_i\big)\alpha + \big(f_{\sigma^i R}(P) - f_{\sigma^j R}(P)\big)\beta + \big(f_{\sigma^i R}(P) r_j - f_{\sigma^j R}(P) r_i\big)\gamma\,. \end{aligned} \tag{4.8.2.1}$$

Then, for a fixed P, Equation (4.8.1.4) is equivalent to

$$(L_{0,2} L_{1,3} R_{0,1}^q R_{2,3}^q)(\alpha,\beta,1) = (L_{0,1} L_{2,3} R_{0,2}^q R_{1,3}^q)(\alpha,\beta,1)\,,$$

and $\mathcal{B}_P$ is the vanishing locus of the homogenous polynomial

$$M(\alpha,\beta,\gamma) := L_{0,2} L_{1,3} R_{0,1}^q R_{2,3}^q - L_{0,1} L_{2,3} R_{0,2}^q R_{1,3}^q \quad \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]\,. \tag{4.8.2.2}$$

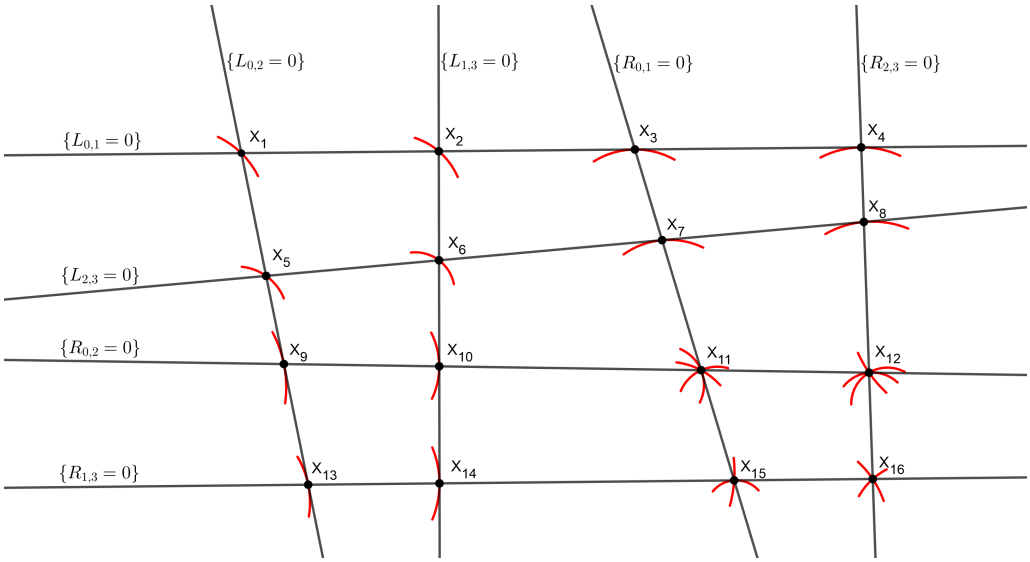
Notice that for each pair $(i,j) \in \{(0,1),(0,2),(1,3),(2,3)\}$ the varieties $\{L_{i,j} = 0\}$ and $\{R_{i,j} = 0\}$ are lines inside $\mathbb{P}^2$ and that it is easy to determine the intersections $\mathcal{B}_P \cap \{L_{i,j}{=}0\}$ and $\mathcal{B}_P \cap \{R_{i,j}{=}0\}$: such divisors are linear combinations of the points X_k's defined in Figure 4.1 as intersections between lines in $\mathbb{P}^2$. The following proposition says that the points X_k are well-defined and distinct.

Claim 4.8.2.3. *We consider the lines $\{L_{i,j} = 0\}$ and $\{R_{i,j} = 0\}$ for (i,j) in the set $\{(0,1),(2,3),(0,2),(1,3)\}$ and the points X_i defined in Figure 4.1 as intersections of some of these lines. For all but at most 450 choices of $P \in E(k)$, this lines are distinct and the points X_i are distinct.*

Proof. Since Q is not a trap, we have $\phi^4(Q) \neq Q + 4P_0$. Hence the points $\sigma^0 Q, \sigma^0 R, \ldots, \sigma^3 Q, \sigma^4 R$ are pairwise distinct: clearly $\sigma^0 Q, \ldots, \sigma^3 Q$ are distinct and $\sigma^0 R, \ldots, \sigma^3 R$ are distinct and if we had $\sigma^i Q = \sigma^j R$, then, for $l := [k : \mathbb{F}_q]$ and $m := i - j$, we would have

$$\begin{aligned} Q + P_0 = \phi(R) = \phi(\sigma^{i-j} Q) = \phi(\phi^{l(i-j)} Q) = \phi^{lm+1}(Q) \\ \implies \quad \phi^4(Q) = \phi^{4(lm+1)}(Q) = Q + 4P_0\,. \end{aligned}$$

Figure 4.1: The intersections X_i of the curve $\mathcal{B}_P$ with certain lines $L_{i,j}, R_{i,j}$.



This implies that for any point $P \in \{\sigma^0 Q, \sigma^0 R, \ldots, \sigma^3 Q, \sigma^4 R\}$ there is exactly one of the rational functions $f_{\sigma^0 Q}, f_{\sigma^0 R}, \ldots, f_{\sigma^3 Q}, f_{\sigma^4 R}$ that has a pole in $-P$, namely f_P.

If the lines $\{L_{0,2} = 0\}$ and $\{L_{1,3} = 0\}$ are equal, then the matrix of their coefficients

$$n(P) = \begin{pmatrix} l_2 - l_0 & (f_Q - f_{\sigma^2 Q})(P) & (l_2 f_Q - l_0 f_{\sigma^2 Q})(P) \\ l_3 - l_1 & (f_{\sigma Q} - f_{\sigma^3 Q})(P) & (l_3 f_{\sigma Q} - l_1 f_{\sigma^3 Q})(P) \end{pmatrix}$$

has rank 1 hence, computing the deteminant of a submatrix of n, P is a zero of the rational function $(l_0 - l_2)(f_{\sigma^3 Q} - f_{\sigma Q}) - (l_1 - l_3)(f_{\sigma^2 Q} - f_Q)$. We have chosen $\widetilde{P}$ so that $l_0 \neq l_2$ and $l_1 \neq l_3$ hence this rational function is non-zero and has five poles counted with multiplicity. So it has at most five zeroes. Hence for all but at most five choices of $P \in E(k)$, the matrix $n(P)$ has rank 2 and consequently the lines $\{L_{0,2} = 0\}$ and $\{L_{1,3} = 0\}$ are distinct.

For any other pair of lines Λ, Λ' in Figure 4.1, one can prove with similar arguments that $\Lambda \neq \Lambda'$ for all but at most five choices of $P \in E(k)$. We prove that, for all $i \neq j$, we have $X_i \neq X_j$, for all but six choices of $P \in E(k)$. We treat only a couple of cases here.

If $X_9 = X_{12}$, then the lines $\{R_{1,3} = 0\}$, $\{R_{2,3} = 0\}$ and $\{L_{0,2} = 0\}$ are concurrent,

hence the following matrix, that contains their coefficients, is not invertible

$$M = M(P) = \begin{pmatrix} r_2 - r_0 & (f_R - f_{\sigma^2 R})(P) & (r_2 f_R - r_0 f_{\sigma^2 R})(P) \\ r_3 - r_2 & (f_{\sigma^2 R} - f_{\sigma^3 R})(P) & (r_3 f_{\sigma^2 R} - r_2 f_{\sigma^3 R})(P) \\ l_2 - l_0 & (f_Q - f_{\sigma^2 Q})(P) & (l_2 f_Q - l_0 f_{\sigma^2 Q})(P) \end{pmatrix},$$

implying that P is a zero of the rational function $\det(M)$. Writing out the $\det(M)$ we see that there is a rational function g, regular in $-\sigma^2 R$, such that

$$\det(M) = (l_2 - l_0)(r_0 - r_3) f_{\sigma^2 R}^2 + f_{\sigma^2 R}\, g\,,$$

and since $l_0 \neq l_2$ and $r_0 \neq r_3$ we deduce that $\det(M)$ has a pole of order 2 in $-\sigma^2 R$ and in particular $\det(M)$ is a non-zero rational function with at most 6 poles counted with multiplicity. Hence $\det(M)$ has at most 6 zeroes, implying that $X_9 \neq X_{12}$, for all but 6 choices of $P \in E(k)$.

If $X_3 = X_4$, then the lines $\{L_{0,1} = 0\}$, $\{L_{2,3} = 0\}$ and $\{R_{0,1} = 0\}$ are concurrent, hence the following matrix, that contains the coefficients of $L_{0,1}$, $L_{2,3}$ and $R_{0,1}$, is not invertible

$$N = N(P) = \begin{pmatrix} l_1 - l_0 & (f_Q - f_{\sigma Q})(P) & (l_1 f_Q - l_0 f_{\sigma Q})(P) \\ l_3 - l_2 & (f_{\sigma^2 Q} - f_{\sigma^3 Q})(P) & (l_3 f_{\sigma^2 Q} - l_2 f_{\sigma^3 Q})(P) \\ r_1 - r_0 & (f_R - f_{\sigma R})(P) & (r_1 f_R - r_0 f_{\sigma R})(P) \end{pmatrix}.$$

As before, in order to prove that $X_3 \neq X_4$ for all but at most 6 choices of $P \in E(k) \setminus \{O_E\}$ it is enough proving that $\det(N(P))$, considered as a rational function of P, is not identically zero. We suppose by contradiction that $\det(N)$ is identically zero and for each $i, j \in \{1, 2, 3\}$ we denote $N_{i,j}$ the (i, j)-minor of $N(P)$, considered as a rational function. Since $l_1 \neq l_0$, then $N_{3,3}$ has a simple pole in $\sigma^3 Q$ and consequently $N_{3,3} \neq 0$. Analogously $N_{1,3} \neq 0$ and $N_{2,3} \neq 0$, hence there are rational functions $A, B \in \overline{\mathbb{F}_q}(E)$ such that

$$\begin{cases} (l_1 - l_0) \cdot A + (f_Q - f_{\sigma Q}) \cdot B = l_1 f_Q - l_0 f_{\sigma Q} \\ (l_3 - l_2) \cdot A + (f_{\sigma^2 Q} - f_{\sigma^3 Q}) \cdot B = l_3 f_{\sigma^2 Q} - l_2 f_{\sigma^3 Q} \\ (r_1 - r_0) \cdot A + (f_R - f_{\sigma R}) \cdot B = r_1 f_R - r_0 f_{\sigma R} \end{cases} \tag{4.8.2.4}$$

and, using Cramer's rule, we have

$$B = \frac{N_{1,2}}{N_{1,3}} = \frac{N_{2,2}}{N_{2,3}} = \frac{N_{3,2}}{N_{3,3}}\,.$$

Using the same argument we used for $N_{3,3}$, we see that $N_{1,2}, N_{2,2}, N_{3,2} \neq 0$. Moreover it is easy to compute the poles of $N_{1,2}$, $N_{2,2}$, $N_{3,2}$, $N_{1,3}$, $N_{2,3}$, $N_{3,3}$ and check that they all vanish in $\widetilde{P}$ and O_E, using that for each $P \in E(\overline{\mathbb{F}_q}) \setminus \{O_E\}$ we have $(f_P - \frac{y}{x})(O_E) = 0$. Hence there are positive divisors $D_{l,m}$ of degree 2 on E such that, for each $j = 2, 3$

$$\begin{aligned}
\operatorname{div}(N_{1,j}) &= D_{1,j} + \widetilde{P} + O_E - (-R) - (-\sigma R) - (-\sigma^2 Q) - (-\sigma^3 Q)\,,\\
\operatorname{div}(N_{2,k}) &= D_{2,j} + \widetilde{P} + O_E - (-Q) - (-\sigma Q) - (-R) - (-\sigma R)\,,\\
\operatorname{div}(N_{3,j}) &= D_{3,j} + \widetilde{P} + O_E - (-Q) - (-\sigma Q) - (-\sigma^2 Q) - (-\sigma^3 Q)\,,
\end{aligned}$$

and consequently

$$\operatorname{div}(B) = D_{1,2} - D_{1,3} = D_{2,2} - D_{2,3} = D_{3,2} - D_{3,3}\,.$$

The functions f_Q, $f_{\sigma Q}$, $f_{\sigma^2 Q}$ and $f_{\sigma^3 Q}$ are $\overline{\mathbb{F}_q}$-linearly independent, hence $N_{1,2}$ and $N_{1,3}$ are not $\overline{\mathbb{F}_q}$-multiples. Hence B is not constant. Since every non-constant rational function on E has at least two poles, we deduce that $D_{1,3} = D_{2,3} = D_{3,3}$ is the divisor of poles of B. This implies that the sum, in the group $E(\overline{\mathbb{F}_q})$, of the poles of $N_{1,3}$ is equal to the sum of the poles of $N_{2,3}$ and is also equal to the sum of the poles of $N_{3,3}$. This implies that, in the group $E(\overline{\mathbb{F}_q})$, we have

$$Q + \sigma Q = \sigma^2 Q + \sigma^3 Q = R + \sigma R\,.$$

Hence, using (4.7.2.1), $-Q - \sigma Q$ is a zero of $N_{3,3}$ and consequently the two poles of B are $-Q - \sigma Q$ and $-Q - \sigma Q - \widetilde{P}$. By looking at (4.8.2.4) we deduce that A has exactly one simple pole, namely $-Q - \sigma Q - \widetilde{P}$, which is absurd. Hence $\det(N(P))$ is not identically zero. □

We now study the geometrically irreducible components of $\mathcal{B}_P$ assuming the conclusions of Claim 4.8.2.3. In other words, we avoid the small (compared to q) number of points $P \in E(k)$ such that the lines $L_{i,j}, R_{i,j}$ or the points X_i in Figure 4.1 are not distinct.

Using the equation defining $\mathcal{B}_P$, we can compute the divisor-theoretic intersection

$$\mathcal{B}_P \cap \{L_{0,2} = 0\} = X_1 + X_5 + qX_9 + qX_{13}\,. \tag{4.8.2.5}$$

This intersection contains the point X_1 with multiplicity 1, hence X_1 is a smooth point of $\mathcal{B}_P$. With analogous arguments we can prove that all the points X_i in the figure except the ones of the shape $\{R_{i,j} = 0\} \cap \{R_{l,m} = 0\}$ are smooth points. This helps us studying the geometrically irreducible components of $\mathcal{B}_P$, as in the following Claim.

Claim 4.8.2.6. *Assume the conclusions of Claim 4.8.2.3 hold. The curve $\mathcal{B}_P$ does not contain any conic defined over k.*

Proof. Suppose $F \in k[\alpha, \beta, \gamma]$ is a quadratic equation defining a conic contained in $\mathcal{B}_P$. Since X_9 is a smooth point of $\mathcal{B}_P$, if the conic $\{F = 0\}$ contains X_9, then $\{F = 0\}$ is the only component of $\mathcal{B}_P$ passing through X_9, hence X_9 appears in $\mathcal{B}_P \cap \{L_{0,2} = 0\}$ with multiplicity at most $2 < q$, contradicting Equation (4.8.2.5). Hence $\{F = 0\}$ does not contain X_9 nor, by a similar argument, X_{13}.

This, together with Equation (4.8.2.5), implies that X_1 and X_5 belong to $\{F = 0\}$. Analogously X_2 and X_6 belong to $\{F = 0\}$. Both the conics $\{L_{0,1}L_{2,3} = 0\}$ and $\{L_{0,2}L_{1,3} = 0\}$ pass through the points X_1, X_2, X_5, X_6, hence, using that X_1, X_2, X_5, X_6 are in general position, there are $\lambda_0, \lambda_1 \in \overline{\mathbb{F}_q}$ such that

$$F = \lambda_0 L_{0,1}L_{2,3} + \lambda_1 L_{0,2}L_{1,3}\,.$$

We extend σ to an element in $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$ and we look at the action of σ on $\overline{\mathbb{F}_q}[\alpha, \beta, \gamma]$. For each $i, j \in \{0, 1, 2, 3\}$ we have $\sigma L_{i,j} = L_{i+1,j+1} = -L_{j+1,i+1}$, considering the indices modulo 4, hence

$$\lambda_0 L_{0,1}L_{2,3} + \lambda_1 L_{0,2}L_{1,3} = F = \sigma F = \sigma(\lambda_0)L_{2,3}L_{3,0} + \sigma(\lambda_1)L_{0,2}L_{1,3}\,.$$

Some cumbersome computations imply that the line $\{L_{1,2} = 0\}$ is the line through X_2 and X_5 and the line $\{L_{3,0} = 0\}$ is the line through X_1 and X_6. In particular the lines $\{L_{i,j} = 0\}$ appearing in the above equation are pairwise distinct. Hence $\lambda_0 = \sigma(\lambda_0) = 0$, and consequently $\{F = 0\} = \{L_{0,2}L_{1,3} = 0\}$, which is not contained in $\mathcal{B}_P$. Contradiction. □

Claim 4.8.2.6 implies that $\mathcal{B}_P$ does not contain a line of $\mathbb{P}^2$. Suppose that Λ is a line contained in $\mathcal{B}_P$. Neither X_9 nor X_{13} are contained in Λ since they are smooth points of $\mathcal{B}_P$ and, by Equation (4.8.2.5, the unique components of $\mathcal{B}_P$ passing through them must have degree at least q inside $\mathbb{P}^2$. Hence $\Lambda \cap \{L_{0,2} = 0\} \in \{X_1, X_5\}$ and consequently

$$(\Lambda \cup \sigma^2\Lambda) \cap \{L_{0,2} = 0\} = X_1 + X_5\,. \tag{4.8.2.7}$$

This implies that $\sigma^2\Lambda \neq \Lambda$ and that $\sigma^2\Lambda$ and Λ are all the $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$-conjugates of Λ: since $\mathcal{B}_P$ is defined over k, then all the $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$-conjugates of Λ are components of $\mathcal{B}_P$ and if Λ has a conjugate $\Lambda' \neq \Lambda, \sigma^2\Lambda$, then, by the same argument as before, $\Lambda' \cap \{L_{0,2} = 0\} \in \{X_1, X_5\}$ and this, together with Equation (4.8.2.7) contradicts the smoothness of X_1 and X_5. We deduce that $\Lambda \cup \sigma^2\Lambda$ is a conic defined over k and contained in $\mathcal{B}_P$, contradicting Claim 4.8.2.6.

By a similar argument, no conic $\mathcal{Q}$ is a component of $\mathcal{B}_P$: if this happens, since conics have degree $2 < q$ in $\mathbb{P}^2$, then X_9, X_{13} do not belong to any of the $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$-conjugates of $\mathcal{Q}$, thus, by Equation (4.8.2.5), for all $\tau \in \mathrm{Gal}(\overline{\mathbb{F}_q}/k)$ we have

$$\tau(\mathcal{Q}) \cap \{L_{0,2} = 0\} = X_1 + X_5 = \mathcal{Q} \cap \{L_{0,2} = 0\}$$

hence, by the smoothness of X_1 and X_5, $\mathcal{Q}$ is defined over k, contradicting Claim 4.8.2.6.

We now suppose that $\mathcal{B}_P$ is not geometrically irreducible. Let $\mathcal{B}_1, \ldots, \mathcal{B}_r$ be the geometrically irreducible components of $\mathcal{B}_P$. As we already proved, each $\mathcal{B}_i$ has degree at least 3, hence the intersection $\mathcal{B}_i \cap \{L_{0,2} = 0\}$ is a sum of at least 3 points counted with multiplicity. By Equation (4.8.2.5), this implies that $\mathcal{B}_i$ is passing through X_9 or X_{13} hence each $\mathcal{B}_i$ has degree at least q. Since the sum of the degrees of the $\mathcal{B}_i$'s is equal to $2q+2 < 3q$, we deduce that $r = 2$ and that either $\deg(\mathcal{B}_1) = \deg(\mathcal{B}_2) = q+1$ or, up to reordering, $\deg(\mathcal{B}_1) = q$ and $\deg(\mathcal{B}_2) = q+2$.

If $\deg(\mathcal{B}_1) = \deg(\mathcal{B}_2) = q+1$, Equation (4.8.2.5) implies that, up to reordering, $X_1 \in \mathcal{B}_1(\overline{\mathbb{F}_q})$ and $X_5 \in \mathcal{B}_2(\overline{\mathbb{F}_q})$. Since $\mathcal{B}_P$ is defined over k, then $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$ acts on $\{\mathcal{B}_1, \mathcal{B}_2\}$ and because of the cardinality of such a set, then σ^2 acts trivially. In particular $X_5 = \sigma^2 X_1$ belongs to $\sigma^2\mathcal{B}_1(\overline{\mathbb{F}_q}) = \mathcal{B}_1(\overline{\mathbb{F}_q})$, hence $X_5 \in \mathcal{B}_1(\overline{\mathbb{F}_q}) \cap \mathcal{B}_2(\overline{\mathbb{F}_q})$, contradicting the smoothness of X_5. This contradiction implies that

$$\deg(\mathcal{B}_1) = q, \quad \deg(\mathcal{B}_2) = q+2\,.$$

For each linear polynomial $L = l_\alpha\alpha + l_\beta\beta + l_\gamma\gamma$ such that $l_\alpha \neq 0$ and for each polynomial $F(\alpha,\beta,\gamma) \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ we define

$$F|_L = F\left(-\frac{l_\beta\beta + l_\gamma\gamma}{l_\alpha}, \beta, \gamma\right),$$

so that $F|_L$ is the unique element of $\overline{\mathbb{F}_q}[\beta,\gamma]$ such that $F \equiv F|_L \bmod L$. If F is homogenous, then $F|_L$ is also homogenous. Notice that the hypothesis $l_\alpha \neq 0$ is true for $L = L_{i,j}$ when $i \neq j$, because, by the definition (4.8.2.1), the coefficient of α in $L_{i,j}$ is $f_{\sigma^i Q}(\tilde{P}) - f_{\sigma^j Q}(\tilde{P})$ and we have chosen $\tilde{P}$ so that $f_{\sigma^i Q}(\tilde{P}) \neq f_{\sigma^j Q}(\tilde{P})$.

For each $i \in \{1,2\}$ let $M_i \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ be a homogeneous polynomial defining $\mathcal{B}_i$.

Claim 4.8.2.8. *There exists homogenous polynomials $F_1, F_2, G_2, N_1, N_2 \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ of respective degree $1,1,1,q-4,q-2$ such that*

$$M_1 = F_1^q + L_{0,1}L_{2,3}L_{0,2}L_{1,3}N_1, \tag{4.8.2.9}$$

$$M_2 = F_2^q L_{0,1}L_{2,3} + G_2^q L_{0,2}L_{1,3} + L_{0,1}L_{2,3}L_{0,2}L_{1,3}N_2 \tag{4.8.2.10}$$

Proof. We start from the first part. Since $\deg \mathcal{B}_1 = q$ and since X_1, X_5, X_9 and X_{13} are smooth, Equation (4.8.2.5 implies that $\mathcal{B}_1 \cap \{L_{0,2} = 0\}$ is either qX_{13} or qX_9, hence $M_1|_{L_{0,2}}$ is the q-th power of a linear polynomial. We deduce the existence of polynomials $A_1, B_1 \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ such that A_1 is linear homogenous and

$$M_1 = A_1^q + B_1 L_{0,2}\,.$$

Similarly to $\mathcal{B}_1 \cap \{L_{0,2} = 0\}$, we have that $\mathcal{B}_1 \cap \{L_{1,3} = 0\}$ is either qX_{14} or qX_{10}, hence there exists a linear polynomial $A_2 \in \overline{\mathbb{F}_q}[\beta, \gamma]$ such that

$$A_2^q = M_1|_{L_{1,3}} = A_1|_{L_{1,3}}^q + B_1|_{L_{1,3}} L_{0,2}|_{L_{1,3}} \quad \Longrightarrow \quad B_1|_{L_{1,3}} L_{0,2}|_{L_{1,3}} = (A_2 - A_1|_{L_{1,3}})^q.$$

In the last equation either both sides are zero or the right hand side gives the prime factorization of the left hand side (we use that $A_2 - A_1$ has degree at most 1 and that $\overline{\mathbb{F}_q}[\beta, \gamma]$ is a UFD). In both cases there exists $\lambda_1 \in \overline{\mathbb{F}_q}$ such that $B_1|_{L_{1,3}} = \lambda_1 L_{0,2}|_{L_{1,3}}^{q-1}$, hence

$$B_1 = \lambda_1 L_{0,2}^{q-1} + B_2 L_{1,3} \quad \Longrightarrow M_1 = (A_1 + \lambda_1 L_{0,2})^q + B_2 L_{0,2} L_{0,3} = A_3^q + B_2 L_{0,2} L_{0,3}$$

for certain homogenous polynomials $A_3, B_2 \in \overline{\mathbb{F}_q}[\alpha, \beta, \gamma]$, with A_3 linear. Similarly to $\mathcal{B}_1 \cap \{L_{0,2} = 0\}$, we have that $\mathcal{B}_1 \cap \{L_{0,1} = 0\}$ is either qX_3 or qX_4. Hence, using the piece of notation $l = L_{0,1}$, there exists a linear polynomial $A_4 \in \overline{\mathbb{F}_q}[\beta, \gamma]$ such that

$$A_4^q = M_1|_l = A_3|_l^q + B_2|_l \, L_{0,2}|_l \, L_{1,3}|_l \quad \Longrightarrow \quad B_2|_l \, L_{0,2}|_l \, L_{1,3}|_l = (A_4 - A_3|_l)^q.$$

Again, in the last equation either both sides are zero or the right hand side gives the prime factorization of the left hand side. The latter is not possible, since the points $X_1 = \{L_{0,1} = 0\} \cap \{L_{0,2} = 0\}$ and $X_2 = \{L_{0,1} = 0\} \cap \{L_{1,3} = 0\}$ are distinct and consequently $L_{0,2}|_l$ and $L_{1,3}|_l$ are relatively prime. We deduce that $B_2|_l = 0$, or equivalently B_2 is divisible by $L_{0,1}$. A similar argument proves that B_2 is also divisible by $L_{2,3}$, implying Equation (4.8.2.9).

Since $\deg \mathcal{B}_2 = q + 2$ and since X_1, X_5, X_9 and X_{13} are smooth, Equation (4.8.2.5) implies that $\mathcal{B}_2 \cap \{L_{0,2}\}$ is either $X_1 + X_5 + qX_{13}$ or $X_1 + X_5 + qX_9$, hence

$$M_1|_{L_{0,2}} = L_{0,1}|_{L_{0,2}} L_{2,3}|_{L_{0,2}} A_5^q \quad \Longrightarrow \quad M_2 = A_5^q L_{0,1} L_{2,3} + B_3 L_{0,2},$$

for some homogenous polynomials $A_5, B_3 \in \overline{\mathbb{F}_q}[\alpha, \beta, \gamma]$, with A_5 linear. In a similar fashion we have $\mathcal{B}_2 \cap \{L_{1,3}\}$ is either $X_2 + X_6 + qX_{14}$ or $X_2 + X_6 + qX_{10}$, hence, using the piece of notation $r = L_{1,3}$, we have

$$\begin{aligned} L_{0,1}|_r L_{2,3}|_r A_6^q = M_1|_r = L_{0,1}|_r L_{2,3}|_r A_5|_r^q + B_3|_r L_{0,2}|_r \\ \Longrightarrow \quad B_3|_r L_{0,2}|_r = L_{0,1}|_r L_{2,3}|_r (A_6 - A_5)|_r^q \end{aligned}$$

Again, in the last equation either both sides are zero or the right hand side gives the prime factorization of the left hand side. In both cases $B_3|_{L_{1,3}}$ is a scalar multiple of $L_{0,1}|_r L_{2,3}|_r L_{0,2}|_r^{q-1}$: in the last case this is obvious, in the first case we use that, since X_1, X_2, X_5 and X_6 are distinct, the polynomials $L_{0,1}|_r$, $L_{2,3}|_r$ and $L_{0,2}|_r$ are relatively

prime. Hence there exist homogenous polynomials $A_7, B_4 \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ such that A_7 is linear and

$$M_2 = A_7^q L_{0,2} L_{1,3} + B_4 L_{0,1} L_{2,3}.$$

Iterating similar arguments we prove Equation 4.8.2.10. □

Let F_1, F_2, G_1, N_1 and N_2 as in Claim 4.8.2.8. Up to multiplying M_1 with an element of $\overline{\mathbb{F}_q}^\times$, we can suppose that $M = M_1 M_2$. Reducing this equality modulo $L_{0,2}L_{1,3}$ we see that

$$L_{0,2}L_{1,3} \text{ divides } L_{0,1}L_{2,3}(F_1F_2 + R_{0,2}R_{1,3})^q.$$

The linear polynomials $L_{i,j}$ in the above equation are coprime since they define distinct lines. Hence $L_{0,2}L_{1,3}$ divides $F_1F_2+R_{0,2}R_{1,3}$. Since $F_1F_2+R_{0,2}R_{1,3}$ is homogenous of degree at most 2, then it is a scalar multiple of $L_{0,2}L_{1,3}$. Using a similar argument with $L_{0,1}L_{2,3}$ we prove that there exist $\lambda, \mu \in \mathbb{F}_q$ such that

$$F_1F_2 + R_{0,2}R_{1,3} = \lambda L_{0,2}L_{1,3}, \quad F_1G_2 - R_{0,1}R_{2,3} = \mu L_{0,1}L_{2,3}\,. \tag{4.8.2.11}$$

We have $\lambda \neq 0$, otherwise F_1 would be a scalar multiple of either $R_{0,2}$ or $R_{1,3}$: in the first case Equation 4.8.2.9 would imply that $\mathcal{B}_1$ contains X_9 but not $X_{14} = \tau(X_9)$, implying that $\tau(\mathcal{B}_1)$ is a component of $\mathcal{B}$ different from $\mathcal{B}_1$, that is $\tau(\mathcal{B}_1) = \mathcal{B}_2$ which contradicts the inequality $\deg(\mathcal{B}_2) > \deg(\mathcal{B}_1)$; in the second case Equation 4.8.2.9 would imply that $\mathcal{B}_1$ contains X_{13} but not $X_{10} = \tau(X_{13})$, leading to the same contradiction.

Using Equations (4.8.2.9), (4.8.2.10) and (4.8.2.11) and the equality $M_1M_2{=}M$, we see that

$$\begin{aligned} 0 &= \frac{M_1M_2 - M}{L_{0,1}L_{2,3}L_{0,2}L_{1,3}} = \\ &= \mu^q L_{0,1}^{q-1}L_{2,3}^{q-1} + \lambda^q L_{0,2}^{q-1}L_{1,3}^{q-1} + F_1^q N_2 + F_2^q N_1 L_{0,1}L_{2,3} + G_2^q N_1 L_{0,2}L_{1,3} + N_1N_2L_{0,1}L_{2,3}L_{0,2}L_{1,3} \\ &\equiv \lambda^q (L_{0,2}L_{1,3})^{q-1} + F_1^q N_2 + G_2^q N_1 L_{0,2}L_{1,3} \pmod{L_{0,1}}. \end{aligned}$$

For any $F \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ we define $\tilde{F} := F_{L_{0,1}}$ and we rewrite the above congruence as

$$\lambda^q \tilde{L}_{0,2}^{q-1}\tilde{L}_{1,3}^{q-1} + \tilde{F}_1^q \tilde{N}_2 + \tilde{G}_2^q \tilde{N}_1 \tilde{L}_{0,2}\tilde{L}_{1,3} = 0. \tag{4.8.2.12}$$

Since then $\mathcal{B}_1 \cap L_{0,1}$ does not contain the point $X_1 = \{L_{0,2}{=}0\} \cap \{L_{0,1}{=}0\}$ nor the point $X_3 = \{L_{1,3}{=}0\} \cap \{L_{0,1}{=}0\}$, then $\tilde{F}_1$ is relatively prime with both $\tilde{L}_{0,2}$ and $\tilde{L}_{1,3}$. Hence both $\tilde{L}_{0,2}$ and $\tilde{L}_{1,3}$ divide $\tilde{N}_2$. Since $X_1 = \{L_{0,2}{=}0\} \cap \{L_{0,1}{=}0\}$ and $X_3 = \{L_{1,3}{=}0\} \cap \{L_{0,1}{=}0\}$ are distinct, then $\tilde{L}_{0,2}$ is relatively prime with $\tilde{L}_{1,2}$ and we can write $\tilde{N}_2 = \tilde{L}_{0,2}\tilde{L}_{1,3}N_3$ for some homogenous polynomial $N_3 \in \overline{\mathbb{F}_q}[\beta,\gamma]$. Substituting in Equation 4.8.2.12 we have

$$\lambda^q \tilde{L}_{0,2}^{q-2}\tilde{L}_{1,3}^{q-2} + \tilde{F}_1^q N_3 + \tilde{G}_2^q \tilde{N}_1 = 0.$$

Since $\lambda \neq 0$, since all the polynomials of the form $\tilde{F}$ are contained in $\overline{\mathbb{F}_q}[\beta,\gamma]$ and since $\tilde{L}_{0,2}$ is relatively prime with $\tilde{L}_{1,2}$, the above equation contradicts Lemma 4.8.2.13 below.

In particular the assumption of the reducibility of $\mathcal{B}$ led to contradiction, together with the conclusions of Claim 4.8.2.3. We deduce that for all but at most 450 choices of $P \in E(k)$ the curve $\mathcal{B}_P$ is geometrically irreducible. Since $\#E(k) > 450$ and since all the components of $\mathcal{B}$ project surjectively to E, we deduce that $\mathcal{B}$ is reduced and geometrically irreducible.

Lemma 4.8.2.13. *Let $L_1, L_2 \in \overline{\mathbb{F}_q}[\beta,\gamma]$ be relatively prime homogenous linear polynomials. Then there exist no homogenous polynomial $A, B, C, D \in \overline{\mathbb{F}_q}[\beta,\gamma]$ such that*

$$L_1^{q-2} L_2^{q-2} = A^q B + C^q D.$$

Proof. The zeroes of L_1 and L_2 in $\mathbb{P}^1$ are distinct, hence, up to a linear transformation we can suppose that their zeroes are 0 and ∞. In particular, up to scalar multiples we can suppose $L_1 = \beta$ and $L_2 = \gamma$, implying that $A^q B + C^q D = \beta^{q-2}\gamma^{q-2}$. This is absurd because any monomial appearing in A^q or in B^q is either a multiple of β^q of a multiple of γ^q, hence the same is true for all the monomials appearing in $A^q B + C^q D$. □

4.8.3 The irreducible components of $\mathcal{C}$

In this subsection we prove that all the geometrically irreducible components of $\mathcal{C}$ are defined over k. To do so, we can ignore (4.8.1.6) in the definition of $\mathcal{C}$. The strategy is applying Lemma 4.6.6 to the variety $\mathcal{B}$, using the rational functions

$$\begin{aligned} u_1, u_2, u_3 \colon \mathcal{B} \dashrightarrow \mathbb{P}^1\,, \qquad & u_i(\alpha,\beta,1,P) = f_{\alpha,\beta,P}(\sigma^{i-1}Q)\,, \\ w_1, w_2, w_3 \colon \mathcal{B} \dashrightarrow \mathbb{P}^1\,, \qquad & w_i(\alpha,\beta,1,P) = -f_{\alpha,\beta,P}(\sigma^{i-1}R)\,, \end{aligned}$$

and the irreducible divisor $Z \subset \mathcal{B}$ being the Zariski closure of

(4.8.3.1)

$$\left\{ (\alpha,\beta,P) \in (\mathbb{A}^2 \times E')(\overline{\mathbb{F}_q}) : \begin{array}{c} P = -Q - \sigma Q - \sigma^3 Q - \widetilde{P}\,, \\ \alpha = \big((f_Q(P) - f_{\sigma Q}(P))\beta + l_1 f_Q(P) - l_0 f_{\sigma Q}(P)\big)/(l_0 - l_1) \end{array} \right\}.$$

Claim 4.8.3.2. *The variety Z is generically contained in the smooth locus of $\mathcal{B}$ and the rational function $u_1 - u_2$ vanishes on Z with multiplicity 1.*

Proof. We restrict to an open subset $U \subset \mathbb{P}^2 \times E$ containing the generic point of Z. Up to shrinking U, the rational functions u_i, w_i can be extended to regular functions on U using the definition (4.8.1.1) of $f_{\alpha,\beta,P}$, and we have

$$u_1 - u_2 = \frac{L_{0,1}(\alpha,\beta,1,P)}{\big(l_0+\beta\big)\big(l_1+\beta\big)}\,,$$

where $L_{i,j}(\alpha,\beta,\gamma,P) \in \overline{\mathbb{F}_q}[U]$ is defined as in (4.8.2.1), as well as $R_{i,j}(\alpha,\beta,\gamma,P)$. Since we can assume that $l_0+\beta, l_1+\beta$ are invertible on U and since Z is generically smooth, it is enough showing that $Z\cap U$ is a component of $(\mathcal{B}\cap U)\cap\{L_{0,1}=0\}$ having multiplicity one. Up to shrinking U, the closed $\mathcal{B}\cap U\subset U$ is the vanishing locus of

$$M(\alpha,\beta,P) := (L_{0,2}L_{1,3}R_{0,1}^qR_{2,3}^q - L_{0,1}L_{2,3}R_{0,2}^qR_{1,3}^q)(\alpha,\beta,1,P) \quad \in \overline{\mathbb{F}_q}[U]\,.$$

Since the restriction of M to $\{L_{0,1}=0\}$ is equal to the restriction of $L_{0,2}L_{1,3}R_{0,1}^qR_{2,3}^q$, it is enough showing that $L_{0,2}$, $R_{0,1}$, $R_{2,3}$ do not vanish on Z and that $\{L_{1,3}=0\}\cap\{L_{0,1}=0\}$ contains $Z\cap U$ with multiplicity 1. We start from the latter. Eliminating the variable α we see that, up to shrinking U, $\{L_{1,3}=0\}\cap\{L_{0,1}=0\}$ is defined by the equations

$$\lambda(P)=0 \quad\text{and}\quad (l_1-l_0)\alpha+(f_Q(P)-f_{\sigma Q}(P))\beta+l_1f_Q(P)-l_0f_{\sigma Q}(P)=0\,, \tag{4.8.3.3}$$

where

$$\lambda(P) := (l_1-l_0)f_{\sigma^3Q}(P)+(l_3-l_1)f_Q(P)+(l_0-l_3)f_{\sigma Q}(P) \quad \in \overline{\mathbb{F}_q}(E)\,.$$

The function λ has three simple poles, namely $-Q,-\sigma Q,-\sigma^3Q$, and we easily verify that $\lambda(\widetilde{P})=\lambda(O_E)=0$. We deduce that $P=-Q-\sigma Q-\sigma^3Q-P_0$ is a simple zero of λ. This, together with the fact that the second equation in (4.8.3.3) is equal to the second equation in the definition (4.8.3.1) of Z, implies that $\{L_{1,3}=0\}\cap\{L_{0,1}=0\}$ contains $Z\cap U$ with multiplicity 1.

We now suppose by contradiction that $R_{0,1}$ vanishes on $Z\cap U$. Substituting α and P in $R_{0,1}$ as in the definition (4.8.3.1) of Z, we see that

$$R_{0,1}(\alpha,\beta,1,P)|_{Z\cap U} = \frac{\lambda_0(-Q-\sigma Q-\sigma^3Q-\widetilde{P})}{l_0-l_1}\beta + \frac{\lambda_1(-Q-\sigma Q-\sigma^3Q-\widetilde{P})}{l_0-l_1}\,,$$

where

$$\begin{aligned}\lambda_0(P) :=& (r_1-r_0)(f_Q-f_{\sigma Q})(P)-(l_1-l_0)(f_R-f_{\sigma R})(P)\,,\\ \lambda_1(P) :=& (r_1-r_0)(l_1f_Q(P)-l_0f_{\sigma Q}(P))-(l_1-l_0)(r_1f_R(P)-r_0f_{\sigma R}(P))\,,\end{aligned}$$

and we deduce that both λ_0 and λ_1 vanish on $P=-Q-\sigma Q-\sigma^3Q-\widetilde{P}$. Both λ_0 and λ_1 have 4 poles and 4 zeroes counted with multiplicity: they have the same poles they share three zeroes, namely $O_E,\widetilde{P}$ and $-Q-\sigma Q-\sigma^3Q-\widetilde{P}$. Since, in the group on $E(\overline{\mathbb{F}_q})$, the sum of the zeroes of an element of $\overline{\mathbb{F}_q}(E)^\times$ is equal to the sum of the poles, then λ_0 and λ_1 also share the fourth zero, hence λ_0 and λ_1 differ by a multiplicative constant in $\overline{\mathbb{F}_q}$. This is absurd because $l_0\neq l_1$ and because the functions f_Q, $f_{\sigma Q}$, f_R, $f_{\sigma R}$ are $\overline{\mathbb{F}_q}$-independent.

A similar argument implies that $R_{2,3}$ does not vanish on $Z \cap U$, while the case of $L_{0,2}$ is easier. Substituting α and P in $L_{0,2}(\alpha, \beta, 1, P)$ as in the definition (4.8.3.1) of Z we get

$$L_{0,2}(\alpha, \beta, 1, P)|_{Z\cap U} = \frac{(\beta + l_0)\lambda_2(-Q-\sigma Q-\sigma^3 Q-\widetilde{P})}{l_0 - l_1},$$

where

$$\lambda_2(P) := (l_2-l_1)f_Q(P) + (l_0-l_2)f_{\sigma Q}(P) + (l_1-l_0)f_{\sigma^2 Q}(P) \quad \in \overline{\mathbb{F}_q}(E).$$

Analogously to λ, we see that the zeroes of λ_2 are $\widetilde{P}, O_E$ and $-Q-\sigma Q-\sigma^2 Q-P_0$, hence λ_2 does not vanish on $-Q-\sigma Q-\sigma^3 Q-P_0$, implying that $L_{0,2}$ does not vanish on $Z \cap U$. □

We can show that u_2-u_3, w_3+u_3, w_3+u_1 and w_i-w_j do not vanish on $Z \cap U$ with similar arguments to the ones used to prove that $R_{0,1}$ and $L_{0,2}$ do not vanish on Z. Hence we can apply Lemma 4.6.6 and deduce that all the components of $\mathcal{C}$ are defined over k.

4.8.4 k-rational points on $\mathcal{C}$

Finally we prove that $\#\mathcal{C}(k)$ is larger than $\frac{1}{2}(\#k)^2$. The surface $\mathcal{C}$ is contained in the open subset of $\mathbb{A}^2 \times (E\backslash\{O_E\}) \times \mathrm{PGL}_2 \times \mathbb{A}^1$ made of points $(\alpha, \beta, (x, y), \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z)$ such that $c \neq 0$. Hence $\mathcal{C}$ is contained in $\mathbb{A}^8$, with variables α, β, x, y, a, b, d, z and it is defined by the following equations:.

- $0 = p_1 := W(x, y)$, the Weierstrass equation defining E;
- $0 = p_2 := (d^q-a)^{q+1}(z^q-z)^{q^2-q} - (ad-b)^q(\frac{z^{q^2}-z}{z^q-z})^{q+1}$, the dehomogenization of (4.8.1.2) in c;
- $0 = p_i(\alpha, \beta, x, y, a, b, d)$ for $i = 3, 4, 5, 6$, obtained by (4.8.1.3) after dehomogenizing in c, substituting $f_{\sigma^i Q}, f_{\sigma^i R}$ by their expressions in α, β, x, y and clearing denominators;
- a number of conditions $0 \neq q_j$ ensuring that $P \neq -\sigma^i Q, P \neq -\sigma^i R$, $\beta + f_{\widetilde{P}}(\sigma^i Q) \neq 0$, $\beta + f_{\widetilde{P}}(\sigma^i R) \neq 0$, $d^q - a \neq 0$, $ad - b \neq 0$, that (4.8.1.6) is satisfied, that $f_{\alpha,\beta,P}(\sigma^i Q)$ are distinct and that $f_{\alpha,\beta,P}(\sigma^i R)$ are distinct.

In particular, $\mathcal{C}$ can be seen as a closed subvariety of $\mathbb{A}^9$, with variables α, β, x, y, b, c, d, z and t defined by the seven equations $p_1 = 0, \ldots, p_6 = 0$ and $0 = p_7 := tq_1 \cdots q_r - 1$. Let $\mathcal{C}_1, \ldots, \mathcal{C}_s$ be the geometrically irreducible components of $\mathcal{C}$. By [46, Remark 11.3], we have

$$\#\mathcal{C}(k) \geq \#\mathcal{C}_1(k) \geq (\#k)^2 - (\delta-1)(\delta-2)(\#k)^{\frac{3}{2}} - K(\mathcal{C}_1)(\#k), \tag{4.8.4.1}$$

where δ is the degree of $\mathcal{C}_1$ and $K(\mathcal{C}_1)$ is the sum of the Betti numbers of $\mathcal{C}$ relative to the compact ℓ-adic cohomology. Since $\mathcal{C}_1$ is a component of $\mathcal{C}$ then

$$\delta \leq \deg(p_1) \cdots \deg(p_7)\,. \tag{4.8.4.2}$$

Since $\mathcal{C}$ is the disjoint union of the $\mathcal{C}_i$, the Betti numbers of $\mathcal{C}$ are the sums of the Betti numbers of the $\mathcal{C}_i$. Hence, using [58, Corollary of Theorem 1]

$$K(\mathcal{C}_1) \leq K(\mathcal{C}) \leq 6 \cdot 2^7 \cdot \left(3 + 7 \max_{i=1,\ldots,7}\{\deg(p_i)\}\right)^{10}\,. \tag{4.8.4.3}$$

Combining Equations (4.8.4.1), (4.8.4.2) and (4.8.4.3) and the inequalities $\deg p_1 \leq 3$, $\deg p_2 \leq q^3{+}q$, $\deg p_3, \ldots, \deg p_6 \leq 2q{+}3$, $\deg p_7 \leq 16q^2{+}37q{+}75$, we deduce that $\#\mathcal{C}(k) > \frac{1}{2}(\#k)^2$ when $\#k \geq q^{80}$ and $q \geq 3$.