DISCRETE LOGARITHMS IN QUASI-POLYNOMIAL TIME IN FINITE FIELDS OF FIXED CHARACTERISTIC

THORSTEN KLEINJUNG AND BENJAMIN WESOLOWSKI

Abstract. We prove that the discrete logarithm problem can be solved in quasi-polynomial expected time in the multiplicative group of finite fields of fixed characteristic. More generally, we prove that it can be solved in the field of cardinality p^n in expected time $(pn)^{2\log_2(n)+O(1)}$.

1. Introduction

In this article we prove the following theorem.

Theorem 1.1. *Given any prime number p and any positive integer n, the discrete logarithm problem in the group $\mathbf{F}_{p^n}^\times$ can be solved in expected time $(pn)^{2\log_2(n)+O(1)}$.*

Fixing the characteristic p, the complexity of solving the discrete logarithm problem in the family of groups $\mathbf{F}_{p^n}^\times$ is then $n^{2\log_2(n)+O(1)}$. Therefore the discrete logarithm problem in finite fields of fixed characteristic can be solved in quasi-polynomial expected time. This result significantly improves upon the complexity $L_{p^n}(1/2)$ proved by Pomerance in 1987 [Pom87]. The quasi-polynomial complexity has been conjectured to be reachable since [BGJT14], where a first heuristic algorithm was proposed. More generally, Theorem 1.1 implies that for any parameter $\alpha \in (0, 1/2)$, discrete logarithms can be computed in expected time $L_{p^n}(\alpha + o(1))$ in any family of fields where $p = L_{p^n}(\alpha)$.

Following the first heuristic algorithm of [BGJT14], a new one was proposed in [GKZ18]. The latter algorithm is proven to terminate in quasi-polynomial expected time for finite fields of fixed characteristic that admit a suitable model. Heuristically, it seems to be easy to compute such a model for any given field, but attempts to prove that it always exists have failed [Mic19]. Nevertheless, the approach of [GKZ18] has been perceived as the most promising way towards a fully rigorous algorithm. Our approach in the present article is similar, and we take advantage of the geometric insights developed in [KW18]. The main difference with all previous work is that we rely on a different model for the field: one that can be proven to exist, eliminating the need for heuristics. This model is introduced in Section 2. The main difficulty is then to construct an algorithm that provably works in this model. The general strategy is similar to that of [GKZ18], yet their algorithm does not immediately translate to the new model. An overview of the new algorithm is presented in Section 3. The remainder of the article is dedicated to the proof.

2. A suitable model for the finite field

The recent algorithms to compute discrete logarithms in small characteristic all exploit properties of a very particular model for the field. It is assumed that the field is of the form $\mathbf{F}_{q^{d\ell}}$, for a prime power q and integers d and ℓ, and there exist two polynomials h_0 and h_1 in $\mathbf{F}_{q^d}[x]$ of degree at most 2, and an irreducible factor I of $h_1 x^q - h_0$ of degree ℓ. The field is then represented as $\mathbf{F}_{q^{d\ell}} \cong \mathbf{F}_{q^d}[x]/(I)$, and the relation

$$x^q \equiv \frac{h_0}{h_1} \mod I \tag{1}$$

is the key ingredient leading to heuristic quasi-polynomial algorithms, assuming that such a model of $\mathbf{F}_{q^{d\ell}}$ can be found where q and d are small enough. A proof that such a model can always be found seems out of reach, therefore we propose to use another one. All we need is a property similar to Equation (1): applying Frobenius is equivalent to a small degree rational function.

Definition 2.1 (Elliptic curve model)**.** Consider a prime power q and an integer $n > 1$. Suppose there is an ordinary elliptic curve E defined over $\mathbf{F}_q$, a rational point $Q \in E(\mathbf{F}_q)$ and an irreducible divisor $\mathscr{I}$ of degree n over $\mathbf{F}_q$ such that for any $f \in \overline{\mathbf{F}}_q(E)$, one has $f \circ \phi_q \equiv f \circ \tau_Q \mod \mathscr{I}$, where ϕ_q is the q-Frobenius and τ_Q is the translation by Q. Then, $\mathbf{F}_q[\mathscr{I}] \cong \mathbf{F}_{q^n}$, and we call $(E, Q, \mathscr{I})$ a (q, n)-*elliptic curve model* of the field $\mathbf{F}_{q^n}$.

We now show how to construct such a model. Consider a prime power q and an integer $n > 1$. Let E be an elliptic curve defined over the finite field $\mathbf{F}_q$, and let ϕ_q be its q-Frobenius. Suppose that $E(\mathbf{F}_q)$ contains a point Q of order n. Let

$$\mathscr{Q} = \{P \in E(\overline{\mathbf{F}}_q) \mid \phi_q(P) = P + Q\}.$$

The kernel of the isogeny $\phi_q - \mathrm{id}_E$ is $E(\mathbf{F}_q)$, and $\mathscr{Q} = (\phi_q - \mathrm{id}_E)^{-1}(Q)$ is a translation of $E(\mathbf{F}_q)$. In particular, $|\mathscr{Q}| = |E(\mathbf{F}_q)|$. Let $P \in \mathscr{Q}$ and i any positive integer. Since $\phi_q(P) = P + Q$ and

$$\phi_{q^i}(P) = \phi_{q^{i-1}}(P + Q) = \phi_{q^{i-1}}(P) + Q,$$

a simple induction yields $\phi_{q^i}(P) = P + iQ$. Also, since Q is of order n, the isogeny ϕ_{q^n} is the first Frobenius fixing P. The orbit of P under the action of ϕ_q is a place of degree n over $\mathbf{F}_q$. Therefore $\mathscr{Q}$ consists of $|E(\mathbf{F}_q)|/n$ irreducible components of degree n over $\mathbf{F}_q$. If $\mathscr{I}$ is one of these components, then $\mathbf{F}_q[\mathscr{I}] \cong \mathbf{F}_{q^n}$. Therefore, a (q, n)-elliptic curve model can be constructed from an elliptic curve E containing an $\mathbf{F}_q$-rational point Q of order n.

Given a finite field of the form $\mathbf{F}_{p^n}$, for a prime number p and an integer n, there does not necessarily exist an elliptic curve model for $\mathbf{F}_{p^n}$, but we show in the following that one can find an extension of that field of degree logarithmic in n which does admit an elliptic curve model. The construction relies on the following theorem.

Theorem 2.2 ([Wat69, Theorem 4.1, condition (I)])**.** *For any integer t coprime to q such that $|t| \leq 2q^{1/2}$, there is an ordinary elliptic curve E defined over $\mathbf{F}_q$ such that $|E(\mathbf{F}_q)| = q + 1 - t$.*

We deduce the following proposition.

Proposition 2.3. *Let $n \leq \sqrt{2}q^{1/4}$ be a non-negative integer. There exists an ordinary elliptic curve defined over $\mathbf{F}_q$ containing an $\mathbf{F}_q$-rational point of order n.*

Proof. We first prove that there is an elliptic curve E over $\mathbf{F}_q$ such that n^2 divides $|E(\mathbf{F}_q)|$. Since $n^2 \leq 2q^{1/2}$, there exists an integer m such that $|q+1-mn^2| \leq 2q^{1/2}$ and $|q+1-(m+1)n^2| \leq 2q^{1/2}$. Either $q + 1 - mn^2$ or $q + 1 - (m + 1)n^2$ is coprime to p, so by Theorem 2.2, there is an ordinary elliptic curve over $\mathbf{F}_q$ with either mn^2 or $(m + 1)n^2$ rational points.

We have shown that there is an elliptic curve E defined over $\mathbf{F}_q$ such that n^2 divides $|E(\mathbf{F}_q)|$. From [Sil86, Corollary 6.4], there are two integers a and b such that the group of rational points $E(\mathbf{F}_q)$ is isomorphic to $\mathbf{Z}/a\mathbf{Z} \oplus \mathbf{Z}/ab\mathbf{Z}$. Then, n^2 divides a^2b, so n divides ab. Therefore $E(\mathbf{F}_q)$ contains a point of order n. □

Theorem 2.4. *For any prime number p and integer n, one can find in deterministic polynomial time in p and n an integer $r = O(\log(n))$ and a (p^r, n)-elliptic curve model of the finite field $\mathbf{F}_{p^{rn}}$.*

Proof. Let r be a positive integer and $q = p^r$. From Proposition 2.3, the existence of an elliptic curve model is ensured whenever $n \leq \sqrt{2}q^{1/4}$, i.e., $n \leq \sqrt{2}p^{r/4}$, which holds whenever $r \geq (4\log(n) - \log(4))/\log(p)$. Therefore, the construction of the elliptic curve model is as follows: let

$$r = \left\lceil \frac{4\log(n) - \log(4)}{\log(p)} \right\rceil,$$

and $q = p^r$. Find an elliptic curve E defined over $\mathbf{F}_q$ and a point $Q \in E(\mathbf{F}_q)$ of order n. As q is polynomial in p and n, these can be found in deterministic polynomial time by an exhaustive search. Finally, let $\mathscr{I}$ be any irreducible component of $\mathscr{Q} = \{P \in E(\overline{\mathbf{F}}_q) : \phi_q(P) = P + Q\}$. □

In the rest of this article, we suppose that the elliptic curve E is in (generalised) Weierstrass form, so that we naturally have coordinates x and y such that x is of degree 2 and y of degree 3, and for any $P \in E$, we have $x(P) = x(-P)$.

3. Overview

The following theorem, summarising a series of refinements [EG02, Die11, GKZ18], shows that to obtain an algorithm to compute discrete logarithms, it is sufficient to have a descent procedure.

Theorem 3.1 ([Wes18, Theorem 1.4]). *Consider a finite cyclic group G of order n. Assume we are given a set $\mathfrak{F} = \{f_1, \dots, f_m\} \subset G$ (called the* factor base*), for some integer m, and an algorithm* Descent *that on input $f \in G$ outputs a sequence $(e_j)_{j=1}^m$ such that $f = \prod_{j=1}^m f_j^{e_j}$. Then, there is a probabilistic algorithm that computes discrete logarithms in G at the expected cost of $O(m \log\log n)$ calls to the descent procedure* Descent*, and an additional $O(m^3 \log\log n)$ operations in $\mathbf{Z}/n\mathbf{Z}$.*

Therefore, to prove Theorem 1.1, it is sufficient to devise an efficient descent algorithm. Fix a (q, n)-elliptic curve model $(E, Q, \mathscr{I})$ for the finite field $\mathbf{F}_{q^n}$.

3.1. **Logarithms of divisors.** The notion of logarithm can be extended from field elements to divisors of the elliptic curve as follows. Let $N = |E(\mathbf{F}_q)|$, and let $\mathrm{Div}^0_{\mathbf{F}_q}(E, \mathscr{I})$ be the subset of $\mathrm{Div}^0_{\mathbf{F}_q}(E)$ of degree zero divisors which do not intersect $\mathscr{I}$. Given a point $P \in E$, the corresponding divisor is written $[P]$. Thanks to the Pohlig-Hellman method, we fix a prime ℓ dividing $q^n - 1$, and focus on the problem of computing discrete logarithms modulo ℓ. We denote by log the logarithm function modulo ℓ, with respect to an arbitrary generator of the multiplicative group of the finite field. We can suppose that N and ℓ are coprime (indeed, since $N = O(q)$, any prime divisor of N can be handled by the baby-step giant-step method in polynomial time in q). We have the following commutative diagram where each line is exact

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbf{F}_q^\times & \longrightarrow & \mathbf{F}_q(E)^\times_{\mathscr{I}} & \xrightarrow{\mathrm{div}} & \mathrm{Div}^0_{\mathbf{F}_q}(E, \mathscr{I}) & \xrightarrow{\sigma} & E(\mathbf{F}_q) \longrightarrow 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \log} & & \vdots{\scriptstyle \mathrm{Log}} & & \\
0 & \longrightarrow & 0 & \longrightarrow & \mathbf{Z}/\ell\mathbf{Z} & \xrightarrow{\mathrm{id}} & \mathbf{Z}/\ell\mathbf{Z} & \longrightarrow & 0,
\end{array}$$

where $\mathbf{F}_q(E)^\times_{\mathscr{I}}$ is the multiplicative group of rational functions on E defined over $\mathbf{F}_q$ whose divisors do not intersect $\mathscr{I}$. The function Log sends any divisor $D \in \mathrm{Div}^0_{\mathbf{F}_q}(E, \mathscr{I})$ to the element $\log(f)/N$, where f is any function with divisor ND (which is principal). Given an effective divisor D of degree n not intersecting $\mathscr{I}$, we also define $\mathrm{Log}(D) = \mathrm{Log}(D - n[0_E])$.

Let $\mathscr{D}_i = E^i/\mathfrak{S}_i$ be the variety of degree i effective divisors on E, where $\mathfrak{S}_i$ is the i-th symmetric group. Let $\mathscr{P}_i \subset \mathscr{D}_i$ be the subvariety of principal divisors. Given two subvarieties $\mathscr{A} \subset \mathscr{D}_n$ and $\mathscr{B} \subset \mathscr{D}_m$, we write $\mathscr{A} + \mathscr{B} = \{A + B \mid A \in \mathscr{A}, B \in \mathscr{B}\} \subset \mathscr{D}_{m+n}$. Given a point $P \in E$, we write $\mathscr{P}_2(P) = \{[P_0] + [P_1] \mid P_0 + P_1 = P\} \subset \mathscr{D}_2$.

3.2. **Elimination and zigzag.** Consider a field extension $k/\mathbf{F}_q$ and a divisor $D \in \mathscr{D}_n(k)$. A *degree n–to–m elimination* is an algorithm that finds a list $(D_i)_{i=1}^t$ of divisors over E of degrees at most m and integers $(\alpha_i)_{i=1}^t$ such that

$$\mathrm{Log}(N_{k/\mathbf{F}_q}(D)) = \sum_{i=1}^{t} \alpha_i \cdot \mathrm{Log}(N_{k/\mathbf{F}_q}(D_i)).$$

The integer t is called the *expansion factor* of the elimination. To build a descent algorithm, we first construct degree 4–to–3 and 3–to–2 elimination algorithms (in Propositions 6.14 and 6.6 respectively) with expansion factors at most some value C. Combining these two eliminations, we obtain a degree 4–to–2 elimination algorithm with expansion factor at most C^2. A descent can then be constructed following the *zigzag* approach developed in [GKZ18], as done in Proposition 7.2. The idea is the following. The logarithm of the finite field element that we wish to descend is first represented as the logarithm of an irreducible divisor D over $\mathbf{F}_q$ of degree a power of two, say 2^{e+2}. Over the field $\mathbf{F}_{q^{2^e}}$, the divisor D splits as 2^e irreducible divisors of degree 4. If D' is any of these, then $D = N_{\mathbf{F}_{q^{2^e}}/\mathbf{F}_q}(D')$. Applying the degree 4–to–2 elimination to D', the value $\mathrm{Log}(D)$ can be rewritten as a linear combination of logarithms $\mathrm{Log}(N_{\mathbf{F}_{q^{2^e}}/\mathbf{F}_q}(D_i))$ where each D_i

has degree 2. Now, taking the norm of each D_i to the subfield $\mathbf{F}_{q^{2^{e-1}}}$, we obtain divisors of degree 4 again, but over a smaller field. One can apply the degree 4–to–2 elimination recursively, until all the divisors involved are of small degree, over a small field $\mathbf{F}_{q^{2^c}}$ (with $c = O(1)$). These small divisors form the set

$$\widetilde{\mathfrak{F}} = \{N_{\mathbf{F}_{q^{2^c}}/\mathbf{F}_q}(D) \mid D \in \mathrm{Div}_{\mathbf{F}_{q^{2^c}}}(E, \mathscr{I}), D > 0, \deg(D) \leq 2\}.$$

We can finally rewrite our logarithm as a combination of logarithms of elements of the factor base

$$\mathfrak{F} = \{f \in \mathbf{F}_q[E] \mid \exists D \in \widetilde{\mathfrak{F}} \text{ such that } \mathrm{div}(f) = ND\}.$$

One difficulty in this approach is that the elimination algorithms might fail for certain divisors, which we call *traps*. We show that traps are rare, in the sense that they form a proper sub-variety of $\mathscr{D}_4$ or $\mathscr{D}_3$ of bounded degree. The descent must then carefully avoid traps. In particular, we show that given a divisor that is not a trap, an elimination allows to rewrite it in terms of smaller degree divisors that are themselves not traps — otherwise the descent could reach a dead end.

3.3. **Degree 3–to–2 elimination.** Consider an extension $k/\mathbf{F}_q$ and a divisor $D \in \mathscr{D}_3(k)$. Let $V = \mathrm{span}(x^{q+1}, x^q, x, 1)$. We define the morphisms φ_P for any $P \in E$ as

$$\varphi_P : V \longrightarrow \overline{\mathbf{F}}_q(E) : \begin{cases} x^{q+1} & \longmapsto (x \circ \tau_{Q+P^{(q)}}) \cdot (x \circ \tau_P), \\ x^q & \longmapsto x \circ \tau_{Q+P^{(q)}}, \\ x & \longmapsto x \circ \tau_P, \\ 1 & \longmapsto 1. \end{cases}$$

These linear morphisms are chosen so that for any vector $f \in V$ and point $P \in E$, we have the relation $\varphi_P(f) \equiv f \circ \tau_P \mod \mathscr{I}$. Now, define the algebraic variety

$$X_0 = \{(f, P) \mid \varphi_P(f) \equiv 0 \mod D\} \subset \mathbf{P}(V) \times E.$$

We will see that it is a curve. Let $(f, P) \in X_0(k)$ be one of its k-rational points. We will prove that there are many such rational points where the polynomial f splits into linear factors over k, i.e., $f = \prod_{i=1}^{q+1} L_i$ with L_i linear over k. Assuming this is the case, then we have a 3–to–2 elimination. Indeed, on one hand,

$$\log(\varphi_P(f)) = \log(f \circ \tau_P) = \sum_{i=1}^{q+1} \log(L_i \circ \tau_P).$$

On the other hand, from the definition of X_0 and the fact that $\varphi_P(f)$ has degree 4, we have $\mathrm{div}(\varphi_P(f)) = D + [P'] - 2[-P] - 2[-Q - P^{(q)}]$, where P' is a point of $E(k)$. We deduce

$$\begin{aligned} \mathrm{Log}(N_{k/\mathbf{F}_q}(D)) = {} & \log(N_{k/\mathbf{F}_q}(\varphi_P(f))) - \mathrm{Log}(N_{k/\mathbf{F}_q}([P'] - 2[-P] - 2[-Q - P^{(q)}])) \\ = {} & \sum_{i=1}^{q+1} \log(N_{k/\mathbf{F}_q}(L_i \circ \tau_P)) - \mathrm{Log}(N_{k/\mathbf{F}_q}([P'])) \\ & + 2 \cdot \mathrm{Log}(N_{k/\mathbf{F}_q}([-P])) + 2 \cdot \mathrm{Log}(N_{k/\mathbf{F}_q}([-Q - P^{(q)}])). \end{aligned}$$

The right-hand side is a sum of logarithms of divisors of degree 1 or 2 over k. Therefore, the 3–to–2 elimination algorithm simply consists in constructing X_0, and pick uniformly at random rational points $(f, P) \in X_0(k)$ until f splits as a product of linear terms. It remains to prove that this happens with good probability. This is formalised in Proposition 6.6.

3.4. **On the action of PGL_n and splitting probabilities.** For the 3–to–2 elimination sketched above to work, we rely on the idea that for $(f, P) \in X_0(k)$, the polynomial f splits into linear factors over k with good probability. This polynomial f has degree $q+1$, so at first glance it seems it should split with very small probability $1/(q+1)!$. However, and this is the key of previous (heuristic) quasi-polynomial algorithms, the polynomials in V have a very particular structure and a fraction $1/O(q^3)$ of them split over k. This high splitting probability can be understood from

the action of PGL_2 on $\mathbf{P}(V)$. We denote by $\star$ the action of invertible 2×2 matrices on univariate polynomials defined as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \star f(x) = (cx+d)^{\deg f} f\left(\frac{ax+b}{cx+d}\right).$$

It induces an action of PGL_2 on $\mathbf{P}(V)$, also written $\star$. The space $\mathbf{P}(V)$ is the closure of the orbit $\mathrm{PGL}_2 \star (x^q - x)$, and if $m \in \mathrm{PGL}_2(k)$, then $m \star (x^q - x)$ splits as a product of linear polynomials over k, which allows to deduce that a significant portion of the polynomials in $\mathbf{P}(V)(k)$ split over k.

This idea is sufficient for the previous heuristic algorithms and for our 3–to–2 elimination, but to obtain a rigorous 4–to–3 elimination algorithm, we need to work with higher dimensional objects. Let $V_n = \mathrm{span}(x_i^q x_j \mid i, j \in \{0, 1, \ldots, n-1\})$. Then, $n \times n$ matrices naturally act on these polynomials by substituting x_i with the scalar product of the i-th row with $(x_0, x_1, \ldots, x_{n-1})^t$. This induces an action of PGL_n on $\mathbf{P}(V_n)$, written $\star$. Let $\mathfrak{d}_n = x_0^q x_1 - x_1^q x_0 \in \mathbf{P}(V_n)$. The orbit $\mathrm{PGL}_n \star \mathfrak{d}$ is a subvariety of $\mathbf{P}(V_n)$, but as soon as $n > 2$, this orbit is not dense anymore. However, as illustrated in the following lemma, it remains the relevant subvariety to consider as we wish to find polynomials that split into linear factors.

Lemma 3.2. *The only polynomials in V_n with 3 distinct linear factors are in the orbit $\mathrm{PGL}_n \star \mathfrak{d}_n$. The only polynomials with a double linear divisor are in the orbits $\mathrm{PGL}_n \star (x_0^q x_1)$ and $\mathrm{PGL}_n \star x_0^{q+1}$.*

Proof. For the first part, suppose that the three factors are not collinear, and apply the action of a matrix sending them to x_0, x_1 and x_2. The resulting polynomial is divisible by $x_0 x_1 x_2$, a contradiction. So the three factors must be collinear, and send them to x_0, x_1 and $x_0 + x_1$. For the second part, send the double divisor to x_0^2. □

As in the PGL_2 case, we have that for any $m \in \mathrm{PGL}_n(k)$, the polynomial $m \star \mathfrak{d}_n$ splits into linear factors over k. Before sketching how to use these observations to build a 4–to–3 elimination algorithm, we note that the closure of $\mathrm{PGL}_n \star \mathfrak{d}_n$ is well understood: it consists of $\mathrm{PGL}_n \star \mathfrak{d}_n$ itself and the closure of $\mathrm{PGL}_n \star (x_0^q x_1)$, described in the following lemma. Consider the vector space $\Lambda_n = \mathrm{span}(x_i \mid i \in \{0, \ldots, n-1\})$ of linear polynomials.

Lemma 3.3. *The closure of $\mathrm{PGL}_n \star (x_0^q x_1)$ is the image of the morphism*

$$\Xi : \mathbf{P}(\Lambda_n) \times \mathbf{P}(\Lambda_n) \longrightarrow \mathbf{P}(V_n) : (u, v) \longmapsto v^q u,$$

which is just the Segre embedding of $\mathbf{P}(\Lambda_n) \times \mathbf{P}(\Lambda_n) \cong \mathbf{P}^{n-1} \times \mathbf{P}^{n-1}$ into $\mathbf{P}(V_n) \cong \mathbf{P}^{n^2-1}$.

The points in $\mathrm{PGL}_n \star (x_0^q x_1)$ are called the *exceptional points* of the closure of $\mathrm{PGL}_n \star \mathfrak{d}_n$, and they play a crucial role in our analysis of the descents. In particular, a divisor being a trap or not is closely related to the properties of the exceptional points that appear in X_0.

3.5. **Degree 4–to–3 elimination algorithm.** Consider an extension $k/\mathbf{F}_q$ and a divisor $D \in \mathscr{D}_4(k)$. Consider the vector space $V = V_3$ as defined above, the element $\mathfrak{d} = x_0^q x_1 - x_0 x_1^q \in V$, and its orbit $\mathrm{PGL}_3 \star \mathfrak{d} \subset \mathbf{P}(V)$. Define the morphism $\psi : V \to \overline{\mathbf{F}}_q[E]$ which substitutes x_0, x_1 and x_2 with 1, x, and y respectively. Now, define the morphism $\varphi : V \to \overline{\mathbf{F}}_q[E]$ with $\varphi(x_i^q x_j) = (\psi(x_i) \circ \tau_Q) \cdot \psi(x_j)$. Observe that $\varphi(f) \equiv \psi(f) \mod \mathscr{I}$ for any $f \in V$. Define

$$X_0 = \{f \in \overline{\mathrm{PGL}_3 \star \mathfrak{d}} \mid \varphi(f) \equiv 0 \mod D\}.$$

Let $f \in X_0(k)$. As briefly justified in the previous paragraph, when f is in the orbit $\mathrm{PGL}_3 \star \mathfrak{d}$, we can expect it to split into linear factors over k with good probability, i.e., $f = \prod_{i=1}^{q+1} L_i$ with $L_i \in \Lambda_3 = \mathrm{span}(x_j \mid j \in \{0, 1, 2\})$. When this happens, we have a 4–to–3 elimination. Indeed, on one hand,

$$\log(\varphi(f)) = \log(\psi(f)) = \sum_{i=1}^{q+1} \log(\psi(L_i)).$$

On the other hand,

$$\mathrm{div}(\varphi(f)) = D + D' - 3[0_E] - 3[-Q],$$

where D' is an effective divisor of degree 2 defined over the field k. We deduce

$$\begin{aligned}\mathrm{Log}(N_{k/\mathbf{F}_q}(D)) &= \log(N_{k/\mathbf{F}_q}(\varphi(f))) - \mathrm{Log}(N_{k/\mathbf{F}_q}(D')) + 3\cdot\mathrm{Log}(N_{k/\mathbf{F}_q}([Q]))\\ &= \sum_{i=1}^{q+1}\log(N_{k/\mathbf{F}_q}(\psi(L_i))) - \mathrm{Log}(N_{k/\mathbf{F}_q}(D')) + 3\cdot[k:\mathbf{F}_q]\cdot\mathrm{Log}([Q]).\end{aligned}$$

The right-hand side is a sum of logarithms of divisors of degree 1, 2 of 3 over k. Therefore, the 4–to–3 elimination algorithm consists in constructing X_0 and pick uniformly at random rational points $f \in X_0(k)$ until f splits as a product of linear terms. We need to prove that this happens with good probability. This is formalised in Proposition 6.14.

3.6. **Traps.** The two types of elimination sketched above work for 'most' degree 3 and degree 4 divisors. There are however certain divisors for which we cannot guarantee that the elimination succeeds: these *trap divisors* form subvarieties $\mathscr{T}_3 \subset \mathscr{D}_3$ and $\mathscr{T}_4 \subset \mathscr{D}_4$. When D is not a trap divisor, we can prove that the elimination succeeds, but another problem might arise: it could be that all possible eliminations of this divisor involve traps, so the descent cannot be iteratively applied. We deal with this issue in Section 6.

4. Degree 3–to–2 elimination

In this section, we consider a degree 3 divisor D on E, defined over k. Note however that the main ideas, and notably the roadmap presented in Section 4.1, also apply to the degree 4–to–3 elimination. We suppose D does not belong to a set of exceptional divisors, the *traps* $\mathscr{T}_3 \subset \mathscr{D}_3$, defined in Section 4.2. Consider the vector space $V = \mathrm{span}(x^{q+1}, x^q, x, 1)$ in the algebra $\overline{\mathbf{F}}_q[x]$. As explained in 3.3, we can associate to the divisor D a variety

$$X_0 = \{(f,P) \mid \varphi_P(f) \equiv 0 \mod D\} \subset \mathbf{P}(V)\times E,$$

and our goal in this section is to prove that for a significant proportion of the pairs $(f,P) \in X_0(k)$, the polynomial f splits into linear terms over k. The general strategy is similar to that of [KW18]: we define a curve C and a morphism $C \to X_0$ such that the image of any k-rational point of C is a pair (f,P) such that f splits into linear terms over k. Such a curve C can be defined in $\mathbf{P}(V)\times E\times\mathbf{P}^1\times\mathbf{P}^1\times\mathbf{P}^1$ as

$$C = \{(f,P,r_1,r_2,r_3) \mid (f,P)\in X_0, \text{ and the } r_i\text{-values are three distinct roots of } f\}.$$

Similarly to [KW18, Proposition 4.1], Lemma 3.2 implies that if $(f,P,r_1,r_2,r_3)\in C(k)$, then f splits into linear factors over k (and therefore leads to an elimination, as explained in Section 3.3).

4.1. **Roadmap.** We need to show that C has a lot of k-rational points. It is sufficient to prove that C has at least one absolutely irreducible component defined over k, then apply Hasse-Weil bounds. There again, our strategy draws inspiration from [KW18]. Instead of considering directly C, whose points encode triples of roots, we start with the following variety which considers a single root at a time:

$$X_1 = \{(f,P,r) \mid (f,P)\in X_0, \text{ and } f(r)=0\} \subset \mathbf{P}(V)\times E\times\mathbf{P}^1.$$

We can then increase the number of roots by considering fibre products over the projection $\theta : X_1 \to X_0$. Indeed, we have

$$\begin{aligned}X_1\times_{X_0}X_1 &= \{((f_1,P_1,r_1),(f_2,P_2,r_2)) \mid (f_1,P_1)=(f_2,P_2)\in X_0, \text{ and } f_1(r_1)=f_2(r_2)=0\}\\ &\cong \{(f,P,r_1,r_2) \mid (f,P)\in X_0, \text{ and } f(r_1)=f(r_2)=0\}.\end{aligned}$$

This product contains a *diagonal* component Δ_{X_1} isomorphic to X_1, which corresponds to quadruples (f,P,r,r). The other components $X_2 = X_1\times_{X_0}X_1\setminus\Delta_{X_1}$ encode pairs of distinct roots (points of the form (f,P,r,r) can still appear in X_2, but they imply that r is a double root of f). We can iterate this construction, and consider the product $X_2\times_{X_1}X_2$ over the projection $X_1\times_{X_0}X_1\to X_1$ to the first factor. This product encodes triples of roots, and the curve C embeds into the non-diagonal part $X_3 = X_2\times_{X_1}X_2\setminus\Delta_{X_2}$. In the rest of this section, we prove sequentially that X_0,

X_1, X_2, X_3 and C contain absolutely irreducible components defined over k.

The following lemma allows us to prove irreducibility results through fibre products.

Lemma 4.1. *Let Y and Z be two absolutely irreducible, complete curves over k, and consider a cover $\eta : Z \to Y$. Suppose there is a point $s \in Y$ and two distinct points $a, b \in Z$ such that $\eta^{-1}(s) = \{a, b\}$. If s, a and b are analytically irreducible, and the normalisation of η is unramified at a, then $Z \times_Y Z \setminus \Delta_Z$ is absolutely irreducible, where Δ_Z is the diagonal component.*

Proof. The same proof as [KW18, Lemma 4.2] implies this result, where smoothness is replaced by analytic irreducibility (both imply that a point belongs to a single irreducible component). □

Remark 1. The term *analytically* refers to properties of the completion of the local ring. A point is *analytically irreducible* if the completion of the corresponding local ring has no zero divisors (equivalently, a single branch passes through this point: it desingularises as a single point).

The following proposition defines our strategy: the rest of our analysis of the 3–to–2 elimination consists in showing that our cover $\theta : X_1 \to X_0$ satisfies the necessary conditions to apply Proposition 4.2.

Proposition 4.2. *Let X_0 and X_1 be complete curves over k, and suppose X_0 is absolutely irreducible. Let $\theta : X_1 \to X_0$ be a cover of degree at least 3. Let $X_2 = (X_1 \times_{X_0} X_1) \setminus \Delta_{X_1}$, and $X_3 = (X_2 \times_{X_1} X_2) \setminus \Delta_{X_2}$ (for the projection $X_2 \to X_1$ to the first factor). Suppose that*

1. *there is a point $s \in X_0$ and two distinct points $a, b \in X_1$ such that $\theta^{-1}(s) = \{a, b\}$,*
2. *the points $a, b \in X_1$ and $(b, b) \in X_2$ are analytically irreducible,*
3. *the normalisation of the cover θ is unramified at a.*

Then, either

1. *the curve X_1 is absolutely irreducible, and so is X_3, or*
2. *the curve X_1 is the union of two absolutely irreducible components A and B, with $a \in A$ and $b \in B$, and*

$$(B \times_{X_0} A) \times_B ((B \times_{X_0} B) \setminus \Delta_B)$$

is an absolutely irreducible components of X_3 defined over k.

Remark 2. Applied to the cover $\theta : X_1 \to X_0$ defined above, we choose $s \in X_0$ to be one of the exceptional points in $X_0 \cap S$, which have the form $((x-\alpha)(x-\beta)^q, P)$. Then,

$$a = ((x-\alpha)(x-\beta)^q, P, \alpha), \text{ and } b = ((x-\alpha)(x-\beta)^q, P, \beta).$$

We then prove that all the conditions of the proposition are satisfied, which imply that X_3 contains an absolutely irreducible component defined over k, which by Hasse-Weil bounds implies that X_3 has a lot of rational points.

Proof. First, we prove that either the curve X_1 is absolutely irreducible, or it splits into two absolutely irreducible components A and B defined over k. Since X_1 is complete and X_0 is absolutely irreducible, each of the absolutely irreducible components of X_1 surjects to X_0 through θ. The points a and b are the only two preimages of s, and since they are analytically irreducible, each belongs to exactly one absolutely irreducible component of X_1. Therefore, X_1 has at most two components. Assuming X_1 is not absolutely irreducible, let A be the component containing a, and B the component containing b. Since the normalisation of θ is not ramified at a, the cover θ restricts to a birational morphism $A \to X_0$. Yet, θ is of degree at least 3, so it *does not* restrict to a birational morphism $B \to X_0$. Since θ is defined over k, the components A and B are not $\mathrm{Gal}(\overline{k}/k)$-conjugate, so they are each defined over k.

Next, we prove Point 1. If X_1 is absolutely irreducible, then X_2 is absolutely irreducible from Lemma 4.1, and we deduce that X_3 is absolutely irreducible from Lemma 4.1 again. Note that we need here that $X_2 \to X_1$ is unramified at $(b, a) \in X_2$, a consequence of the fact that θ is unramified at a.

We now prove Point 2. Assume that X_1 decomposes as $A \cup B$. We first show that X_2 is the union of the absolutely irreducible components $A \times_{X_0} B$, $B \times_{X_0} A$, and $(B \times_{X_0} B) \setminus \Delta_B$, each defined over k. We have

$$\begin{aligned}(X_1 \times_{X_0} X_1) \setminus \Delta_{X_1} &= ((A \times_{X_0} A) \cup (A \times_{X_0} B) \cup (B \times_{X_0} A) \cup (B \times_{X_0} B)) \setminus \Delta_{X_1} \\ &= (A \times_{X_0} B) \cup (B \times_{X_0} A) \cup ((B \times_{X_0} B) \setminus \Delta_B).\end{aligned}$$

Both $A \times_{X_0} B$ and $B \times_{X_0} A$ are birational to B, so they are absolutely irreducible. The point $(b, b) \in (B \times_{X_0} B) \setminus \Delta_B$ is analytically irreducible (so it can only be in one component), and is the only preimage of the point $b \in B$ through the projection to the first factor. Therefore $B \times_{X_0} B$ is absolutely irreducible. Finally, we prove that X_3 contains an absolutely irreducible component defined over k. Consider the component of X_3 of the form

$$Y = (B \times_{X_0} A) \times_B ((B \times_{X_0} B) \setminus \Delta_B),$$

with respect to the projections to the first factor $B \times_{X_0} A \to B$ and $B \times_{X_0} B \to B$. The projection $Y \to (B \times_{X_0} B) \setminus \Delta_B$ is an isomorphism, so Y is absolutely irreducible. □

4.2. **Traps.** Recall that we need D not to be a trap: we now define what this means. Let

$$\begin{aligned}\mathscr{T}_3^0 &= \{[D_1] + [D_1] + [D_2] \mid D_1, D_2 \in E\} \subset \mathscr{D}_3, \\ \mathscr{T}_3^1 &= \{[D_1] + [D_2] + [D_3] \mid (D_1 + D_2)^{(q)} = (D_1 + D_i) + 2Q \text{ for some } i \neq 1\} \subset \mathscr{D}_3, \\ \mathscr{T}_3^2 &= \{[D_1] + [D_2] + [D_3] \mid D_1^{(q)} = D_i + Q \text{ for some } i\} \subset \mathscr{D}_3.\end{aligned}$$

In addition, a fourth kind of traps $\mathscr{T}_3^3$ is defined in Proposition 4.4. The set of traps is $\mathscr{T}_3 = \bigcup_{i=0}^3 \mathscr{T}_3^i$, and we suppose that $D \notin \mathscr{T}_3$. The following lemma allows us to prove that traps can always be avoided in the descent algorithm (in particular, not every divisor is a trap).

Lemma 4.3. *Let $P_0 \in E$. If $P_0^{(q)} \notin \{P_0 - Q, P_0 + 2Q\}$, then $\mathscr{P}_2(P_0) + [-P_0] \not\subset \mathscr{T}_3$.*

Proof. This easily follows from the above definitions, and Proposition 4.4. □

4.3. **Exceptional points of X_0.** Let S be the image of the morphism Ξ from Lemma 3.3. In this section we give an explicit list of the 24 points in $X_0 \cap (S \times E)$ (or only 12 points in characteristic 2). Let $f = (x - \beta)^q (x - \alpha) \in S$, and suppose $(f, P) \in X_0$. Then, D divides the positive part of

$$\operatorname{div}(\varphi_P(f)) = [P_\alpha - P] + [-P_\alpha - P] + [P_{\beta^q} - Q - P^{(q)}] + [-P_{\beta^q} - Q - P^{(q)}] - 2[-P] - 2[-Q - P^{(q)}],$$

where P_γ is any of the two points such that $x(P_\gamma) = \gamma$. There are three ways to split $D = D' + [D_3]$ where D' is of degree 2 and D_3 is a point. Each such splitting induces two possible ways for D to divide $\operatorname{div}(\varphi_P(f))$: either D' divides $\operatorname{div}(\varphi_P(x - \alpha))$ and $[D_3]$ divides $\operatorname{div}(\varphi_P((x - \beta)^q))$, or the reverse. Let c be the number of two-torsion points on E; it is 2 in characteristic 2 (recall that E is ordinary) and 4 otherwise. Each of these 6 configurations gives rise to c possible values of f, and we find that $X_0 \cap S \times E$ contains a total of $6c$ points (we observe below that they project to $6c$ distinct points in E). Indeed, if $D' = [D_1] + [D_2]$, D' divides $\operatorname{div}(\varphi_P(x - \alpha))$ and $[D_3]$ divides $\operatorname{div}(\varphi_P((x - \beta)^q))$, we get that P is any of the c points such that $2P = -(D_1 + D_2)$. Then, $\alpha = x(P + D_1)$ and $\beta^q = x(P^{(q)} + Q + D_3)$. Similarly, if $[D_3]$ divides $\operatorname{div}(\varphi_P(x - \alpha))$ and D' divides $\operatorname{div}(\varphi_P((x - \beta)^q))$, we get that P is any of the c points such that $2P^{(q)} = -(D_1 + D_2 + 2Q)$. Then, $\alpha = x(P + D_3)$ and $\beta^q = x(P^{(q)} + Q + D_1)$.

Assuming that $D_i \neq D_j$ for $i \neq j$ and $(D_i + D_j)^{(q)} \neq (D_i + D_k) + 2Q$ for any i, j, k (with $i \neq j$ and $i \neq k$), then the $6c$ points are distinct. Therefore, since D is not in $\mathscr{T}_3^0 \cup \mathscr{T}_3^1$, the intersection $X_0 \cap (S \times E)$ projects to $6c$ distinct points in E.

4.4. **Irreducibility of X_0.** Let $P \in E$. Since $\dim(V) = 4$ and $\dim(\overline{\mathbf{F}}_q(E)/D) = 3$, we generically expect the kernel of

$$\overline{\varphi}_P : V \longrightarrow \overline{\mathbf{F}}_q(E)/D : f \longmapsto \varphi_P(f) \mod D$$

to be a line, in which case there is exactly one $f \in \mathbf{P}(V)$ such that $(f, P) \in X_0$. If this is indeed the case for all $P \in E$, then the projection $X_0 \to E$ is a bijection, so X_0 is absolutely irreducible.

By contradiction, suppose there is a point $P \in E$ such that $L = \mathbf{P}(\ker \overline{\varphi}_P)$ has dimension at least 1. From Section 4.3, the variety L intersects S only at one point, so it must be a line tangent to S at that point. Write $D = \sum_{i=1}^{3}[D_i]$, $u_i = x(D_i + P)$ and $v_i = x(D_i + Q + P^{(q)})$. Without loss of generality, the intersection point is $(x^q - v_3)(x - u_1)$. There are two cases to distinguish: either $u_1 = u_2$, or $v_3 = v_2$ (corresponding to the two cases exhibited in Section 4.3). The points $a_{q+1}x^{q+1} + a_q x^q + a_1 x + a_0$ on the line L satisfy (by construction) the three equations

$$a_{q+1}u_i v_i + a_q v_i + a_1 u_i + a_0 = 0, i \in \{1, 2, 3\}.$$

Also, since L is tangent to S at $(x^q - v_3)(x - u_1)$, it also satisfies the equation

$$a_{q+1}u_1 v_3 + a_q v_3 + a_1 u_1 + a_0 = 0.$$

These linear equations can be represented in the matrix

$$M = \begin{pmatrix} v_1u_1 & v_1 & u_1 & 1 \\ v_2u_2 & v_2 & u_2 & 1 \\ v_3u_3 & v_3 & u_3 & 1 \\ v_3u_1 & v_3 & u_1 & 1 \end{pmatrix}.$$

Since L has dimension at least 1, the rank of this matrix is at most 2. We now show that when D is not a trap, M is of rank 3, a contradiction (implying that $X_0 \to E$ is a bijection and X_0 is absolutely irreducible). In the case where $u_1 = u_2$, we have $u_1 \neq u_3$ (because $D \notin \mathscr{T}_3^0$), so

$$\operatorname{rank}(M) = 1 + \operatorname{rank}\begin{pmatrix} v_1u_1 & v_1 & 1 \\ v_2u_1 & v_2 & 1 \\ v_3u_1 & v_3 & 1 \end{pmatrix} = 1 + \operatorname{rank}\begin{pmatrix} v_1 & 1 \\ v_2 & 1 \\ v_3 & 1 \end{pmatrix}.$$

Since $D \notin \mathscr{T}_3^0$, the values v_i are not all equal, so the rank of M is 3. The case $v_3 = v_2$ is similar.

4.5. **Local analysis of X_1.** Let us compute some equations for X_1. We see it as a subvariety of $\mathbf{P}^3 \times E \times \mathbf{P}^1$, parameterized by the (affine) variables $a_q, a_1, a_0, x_E, y_E, r$ (where the corresponding polynomial is $x^{q+1} + a_q x^q + a_1 x + a_0$, the point is $P = (x_P, y_P) \in E$, and the root is r). As above, let $D = \sum_{i=1}^{3}[D_i]$, $u_i = x(P + D_i)$ and $v_i = x(P^{(q)} + D_i + Q)$. The defining polynomials of X_1 are the equation $e \in \mathbf{F}_q[x_P, y_P]$ of the elliptic curve E and the four polynomials

$$\begin{aligned} F_1 &= v_1u_1 + a_q v_1 + a_1 u_1 + a_0, \\ F_2 &= v_2u_2 + a_q v_2 + a_1 u_2 + a_0, \\ F_3 &= v_3u_3 + a_q v_3 + a_1 u_3 + a_0, \\ G &= r^{q+1} + a_q r^q + a_1 r + a_0. \end{aligned}$$

Recall that for any $P_0 \in E$, we have $\mathscr{P}_2(P_0) = \{[R] + [T] \mid R + T = P_0\} \subset \mathscr{D}_2$.

Proposition 4.4. *There is a point $s \in X_0 \cap (S \times E)$ of which both preimages through θ in X_1 are smooth, unless D belongs to a strict subvariety $\mathscr{T}_3^3$ of $\mathscr{D}_3$. For any $P_0 \in E$, we have $\mathscr{P}_2(P_0) + [-P_0] \not\subset \mathscr{T}_3^3$.*

Proof. The Jacobian matrix associated to the given defining polynomials of X_1 is

$$\begin{pmatrix} 0 & 0 & 0 & \frac{\partial e}{\partial x_P} & \frac{\partial e}{\partial y_P} & 0 \\ v_1 & u_1 & 1 & \frac{\partial u_1}{\partial x_P}(v_1 + a_1) & \frac{\partial u_1}{\partial y_P}(v_1 + a_1) & 0 \\ v_2 & u_2 & 1 & \frac{\partial u_2}{\partial x_P}(v_2 + a_1) & \frac{\partial u_2}{\partial y_P}(v_2 + a_1) & 0 \\ v_3 & u_3 & 1 & \frac{\partial u_3}{\partial x_P}(v_3 + a_1) & \frac{\partial u_3}{\partial y_P}(v_3 + a_1) & 0 \\ r^q & r & 1 & 0 & 0 & r^q + a_1 \end{pmatrix}$$

Since X_0 is smooth, the top-left 5×4 submatrix has rank 4. Therefore the above matrix has rank 5 at any point where $r^q + a_1 \neq 0$. Therefore, the only points that could be singular on X_1 correspond to polynomials of the form $(x - \beta)^q(x - \alpha) = x^{q+1} - \alpha x^q - \beta^q x + \beta^q \alpha$, together with

the elliptic curve point (x_0, y_0) and the root β. In terms of the coordinates $(a_q, a_1, a_0, x_E, y_E, r)$, such a point is given by $(-\alpha, -\beta^q, \beta^q\alpha, x_0, y_0, \beta)$. It is non-singular if and only if the matrix

$$\begin{pmatrix} 0 & 0 & \frac{\partial e}{\partial x_P} & \frac{\partial e}{\partial y_P} \\ v_1 - r^q & u_1 - r & \frac{\partial u_1}{\partial x_P}(v_1 + a_1) & \frac{\partial u_1}{\partial y_P}(v_1 + a_1) \\ v_2 - r^q & u_2 - r & \frac{\partial u_2}{\partial x_P}(v_2 + a_1) & \frac{\partial u_2}{\partial y_P}(v_2 + a_1) \\ v_3 - r^q & u_3 - r & \frac{\partial u_3}{\partial x_P}(v_3 + a_1) & \frac{\partial u_3}{\partial y_P}(v_3 + a_1) \end{pmatrix}$$

has rank 4 at this geometric point.

Let $\mathscr{T}_3^3$ be the subvariety of $\mathscr{D}_3$ of divisors D for which this matrix is singular at all the corresponding 24 exceptional points (or 12 in characteristic 2). Fix $P_0 \in E$, and let us show that $\mathscr{P}_2(P_0) + [-P_0] \not\subset \mathscr{T}_3^3$. Let $P \in E$, and

$$D = [D_1] + [D_2] + [D_3] = [-P_0] + [P_0 - 2P] + [2P] \in \mathscr{P}_2(P_0) + [-P_0].$$

The point $((x-\beta)^q(x-\alpha), P)$ is on the induced X_0 for $\alpha = x(P + D_1) = x(P + D_2)$ and $\beta^q = x(P^{(q)} + D_3 + Q)$. At this exceptional point, the matrix simplifies to

$$\begin{pmatrix} 0 & 0 & \frac{\partial e}{\partial x_P} & \frac{\partial e}{\partial y_P} \\ v_1 - \beta^q & u_1 - \beta & \frac{\partial u_1}{\partial x_P}(v_1 - \beta^q) & \frac{\partial u_1}{\partial y_P}(v_1 - \beta^q) \\ v_2 - \beta^q & u_2 - \beta & \frac{\partial u_2}{\partial x_P}(v_2 - \beta^q) & \frac{\partial u_2}{\partial y_P}(v_2 - \beta^q) \\ 0 & u_3 - \beta & 0 & 0 \end{pmatrix}$$

It is easy to see that $v_1 - v_2$ and $u_3 - \beta$ are non-zero rational functions of P. Then, the matrix is singular if and only if the following matrix is singular:

$$\begin{pmatrix} \frac{\partial e}{\partial x_P} & \frac{\partial e}{\partial y_P} \\ \frac{\partial u_1}{\partial x_P} - \frac{\partial u_2}{\partial x_P} & \frac{\partial u_1}{\partial y_P} - \frac{\partial u_2}{\partial y_P} \end{pmatrix}$$

An explicit computation shows that for any D_1, this determinant is a non-zero rational function of P. Indeed, using the addition formula for the short Weierstrass equation $y^2 = x^3 + Ax + B$ in characteristic larger than 3, we get that the numerator of this determinant divides a rational function in which the two leading terms are

$$y(D_1)x_P^{30} - (A + 3x(D_1)^2)x_P^{28}y_P.$$

The explicit computations being cumbersome, we provide a Magma script[1]. This numerator is a non-zero rational function of P if $y(D_1) \neq 0$ or $A \neq -3x(D_1)^2$. If $y(D_1) = 0$ and $A = -3x(D_1)^2$, then $B = 2x(D_1)^3$, and the discriminant of the short Weierstrass equation is zero, a contradiction. The cases of characteristic 2 and 3 are similar (and the arguments are indeed simpler since the exhibited leading coefficients are x^{27} and $x^{39}y$ respectively). We deduce that for any D_1, all but finitely many points P correspond to a non-singular point. With $D_1 = -P_0$, we have shown that $\mathscr{P}_2(P_0) + [-P_0] \not\subset \mathscr{T}_3^3$. □

In the rest of this section, we fix the point s from Proposition 4.4. With $s = ((x-\beta)^q(x-\alpha), P_0)$, let $a = ((x-\beta)^q(x-\alpha), P_0, \alpha)$ and $b = ((x-\beta)^q(x-\alpha), P_0, \beta)$, the two preimages of s through θ. These points s, a and b are the ones that will allow us to apply Proposition 4.2. Since these points are smooth, they are analytically irreducible.

Lemma 4.5. *The morphism $X_1 \to X_0$ is unramified at a.*

Proof. In terms of the coordinates $(a_q, a_1, a_0, x_E, y_E, r)$, the point $a = ((x-\beta)^q(x-\alpha), P_0, \alpha) \in X_1$ is the tuple $(-\alpha, -\beta^q, \beta^q\alpha, x_0, y_0, \alpha)$. With a linear change of variables, send this point to the origin, and to avoid heavy notation, we still write $(a_q, a_1, a_0, x_E, y_E, r)$ for the translated variables. Since X_0 is non-singular, it admits a local parameterisation $a_q, a_1, a_0, x, y \in k[[t]]$ at s. Then, the curve X_1 is given analytically at a by the equation

$$G = r^{q+1} + a_q r^q + (a_1 + \alpha^q - \beta^q)r + (a_q\alpha^q + a_1\alpha + a_0) \in k[[r, t]].$$

[1] `https://github.com/Calodeon/dlp-proof/blob/master/3to2elimination.m`

The induced morphism between the completions of the local rings is then given by

$$\begin{aligned} f : k[[t]] &\longrightarrow k[[t,r]]/(G) \\ t &\longmapsto t, \end{aligned}$$

Since $\alpha^q - \beta^q \neq 0$, the variable t does not divide the linear term of G, and the morphism is therefore unramified at a. □

4.6. **Local analysis of X_2.** In this section, we show that the point $(b,b) \in X_2$ is analytically irreducible.

Lemma 4.6. *Consider a morphism of smooth curves $\eta : Z \to Y$ over some field k. Suppose that at some point $z \in Z$, the induced morphism between the completions of the local rings is given by*

$$\begin{aligned} \eta_z^* : k[[t]] &\longrightarrow k[[t,r]]/(t - r^q B(t,r)) \\ t &\longmapsto t, \end{aligned}$$

where $B(0,0) \neq 0$ and $B(0,r)$ has a non-zero linear term. Then, the point $(z,z) \in (Z \times_Y Z) \setminus \Delta_Z$ is analytically irreducible.

Proof. Up to isomorphism, η_z^* can be written as

$$\eta_z^* : k[[t]] \to k[[r]] : t \mapsto r^q U(r),$$

where $U(0) \neq 0$ and $U(r)$ has a non-zero linear term. Then, the completion of the local ring at $(z,z) \in (Z \times_Y Z) \setminus \Delta_Z$ is $k[[r,r']]/C(r,r')$ where

$$C(r,r') = \frac{r^q U(r) - r'^q U(r')}{r - r'}.$$

Unsurprisingly, (z,z) is singular: this corresponds to the fact that η is ramified at z, with ramification index $q > 2$. Let us blow up the equation $C(r,r')$ by introducing a variable s and the equation $r' = rs$ (the case $r = r's$ is symmetric). Substituting in C, we obtain

$$C(r,rs) = \frac{r^q(U(r) - s^q U(rs))}{r(1-s)} = r^{q-1}\frac{U(r) - s^q U(rs)}{1-s}.$$

The equation of the blowup is $H(r,s) = C(r,rs)/r^{q-1}$. The only solution of $H(0,s) = 0$ is at $s = 1$, so there is only one point in the blowup, and it remains to see that it is smooth. Write $U(r) = u_0 + u_1 r + r^2\tilde{U}(r)$, and $s' = s - 1$. We have

$$\begin{aligned} U(r) - s^q U(rs) &= U(r) - U(rs) - s'^q U(rs) \\ &= u_0 + u_1 r + r^2\tilde{U}(r) - u_0 - u_1 rs - r^2 s^2 \tilde{U}(rs) - s'^q U(rs) \\ &= -u_1 rs' + r^2\tilde{U}(r) - r^2 s^2 \tilde{U}(rs) - s'^q U(rs). \end{aligned}$$

Therefore, $u_1 \neq 0$ is the coefficient of the monomial r in $H(r,s)$, so $H(r,s)$ has a non-zero linear term, implying that the point at $r = 0$ and $s = 1$ is smooth. □

Proposition 4.7. *The point $(b,b) \in X_2$ is analytically irreducible.*

Proof. Recall that $s \in X_0$ is the point from Proposition 4.4, and $a, b \in X_1$ are its two preimages through θ. We start as in the proof of Lemma 4.5. In terms of the coordinates $(a_q, a_1, a_0, x_E, y_E, r)$, the point $b = ((x-\beta)^q(x-\alpha), P_0, \beta) \in X_1$ is the tuple $(-\alpha, -\beta^q, \beta^q\alpha, x_0, y_0, \beta)$, and we send this point to the origin via a linear change of variables (again, to avoid heavy notation, we still write $(a_q, a_1, a_0, x_E, y_E, r)$ for the translated variables). Let $a_q, a_1, a_0, x, y \in k[[t]]$ be the local parameterisation of X_0 at s. The curve X_1 is given analytically at b by the equation

$$G = r^{q+1} + (a_q + \beta - \alpha)r^q + a_1 r + (a_q\beta^q + a_1\beta + a_0) \in k[[r,t]].$$

Since b is non-singular, $a_q\beta^q + a_1\beta + a_0 = tF(t)$ with $F(0) \neq 0$. Writing $a_1 = tH(t)$, we get

$$G = t(F(t) + H(t)r) + r^q(r + a_q + \beta - \alpha) \in k[[r,t]].$$

Since $D \notin \mathscr{T}_3^2$, we have $\alpha \neq \beta$, so up to multiplication by a unit, G is of the form $t - r^q B(t,r)$ for some $B(t,r)$ such that $B(0,0) \neq 0$. We would like to show that $B(0,r)$ has a non-zero linear term. Write $v_3 = v_3' + \beta^q$. From equation F_3 (defined on page 9), we have

$$\begin{aligned} 0 &= v_3 u_3 + (a_q - \alpha)v_3 + (a_1 - \beta^q)u_3 + a_0 + \beta^q \alpha \\ &= (v_3' + \beta^q)u_3 + (a_q - \alpha)(v_3' + \beta^q) + (a_1 - \beta^q)u_3 + a_0 + \beta^q \alpha \\ &= a_1 u_3 - v_3'(\alpha - u_3 - a_q) + a_q \beta^q + a_0 \\ &= a_1(u_3 - \beta) - v_3'(\alpha - u_3 - a_q) + tF(t) \end{aligned}$$

Since v_3 is a q-th power, we get that $H(0) = \frac{a_1}{t}(0) = -\frac{F(0)}{u_3(0)-\beta}$. We deduce that the linear term of $B(0,r)$ is $-F(0)^{-1}(1 - \frac{\alpha-\beta}{u_3(0)-\beta})$. Since $D \notin \mathscr{T}_3^0$, $u_3(0) \neq \alpha$, so $B(0,r)$ has a non-zero linear term. We conclude with Lemma 4.6. □

4.7. **Irreducibility of X_3.** We are finally ready to prove the main result of this section.

Proposition 4.8. *For any divisor $D \in (\mathscr{D}_3 \setminus \mathscr{T}_3)(k)$, the curve X_3 contains an absolutely irreducible component defined over k.*

Proof. We have shown that $\theta : X_1 \to X_0$ satisfies all the conditions of Proposition 4.2, so the result follows. □

5. Degree 4–to–3 elimination

As for the degree 3–to–2 elimination, we are going to apply Proposition 4.2. Consider an extension $k/\mathbf{F}_q$ and a divisor $D \in \mathscr{D}_4(k)$. Recall from Section 3.5 that we work with the vector space $V = \operatorname{span}(x_i^q x_j \mid i,j \in \{0,1,2\})$, the morphism $\psi : V \to \overline{\mathbf{F}}_q[E]$ which substitutes x_0, x_1 and x_2 with 1, x, and y respectively, and the morphism $\varphi : V \to \overline{\mathbf{F}}_q[E]$ with $\varphi(x_i^q x_j) = (\psi(x_i) \circ \tau_Q) \cdot \psi(x_j)$. Let $\overline{\varphi} : V \to \overline{\mathbf{F}}_q[E]/D$ be the composition of φ with the projection to $\overline{\mathbf{F}}_q[E]/D$. We then have

$$X_0 = \{f \in \overline{\mathrm{PGL}_3 \star \mathfrak{d}} \mid \varphi(f) \equiv 0 \mod D\} = \overline{\mathrm{PGL}_3 \star \mathfrak{d}} \cap \mathbf{P}(\ker \overline{\varphi}),$$

where $\mathfrak{d} = x_0^q x_1 - x_1^q x_0 \in V$. The space $\mathbf{P}(\ker \overline{\varphi})$ is a hyperplane in $\mathbf{P}(V)$, which we denote by H. We prove in Lemma 5.5 that X_0 is a curve. Let us represent the elements of V (or $\mathbf{P}(V)$) as column vectors

$$\sum_{ij} a_{ij} x_i^q x_j = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{10} & a_{11} & a_{12} & a_{20} & a_{21} & a_{22} \end{pmatrix}^t = a_{\mathrm{vec}}$$

The hyperplane H is the kernel of the matrix

$$\begin{pmatrix} H_{00} & H_{01} & H_{02} & H_{10} & H_{11} & H_{12} & H_{20} & H_{21} & H_{22} \end{pmatrix},$$

where each H_{ij} is a column vector of dimension 4. With $\Lambda = \operatorname{span}(x_i \mid i \in \{0,1,2\})$, the curve X_1 is defined as

$$X_1 = \{(f,u) \mid f \in X_0 \text{ and } u \text{ is a factor of } f\} \subset \mathbf{P}(V) \times \mathbf{P}(\Lambda).$$

and we set $X_2 = X_1 \times_{X_0} X_1 \setminus \Delta_{X_1}$ and $X_3 = X_2 \times_{X_1} X_2 \setminus \Delta_{X_2}$ as in Section 4.1.

5.1. **Exceptional points of X_0.** Let $D = \sum_{i=1}^4 [D_i] \in \mathscr{D}_4(k)$ be the divisor of E to be eliminated, and let H be the induced hyperplane. Suppose that D is not divisible by a principal divisor of degree 3 (being divisible by a principal divisor would correspond to the traps of type $\mathscr{T}_4^4$ defined in Section 5.2). Let $uv^q \in S \cap H$ be an exceptional point of X_0. We have $\varphi(uv^q) = u \cdot (v^{(q)} \circ \tau_Q)$ (where $v^{(q)}$ is v with coefficients raised to the power q), which is of degree 6 since u and $v^{(q)} \circ \tau_Q$ are each of degree 3. Since D divides $\varphi(uv^q)$ and D is not divisible by a principal divisor of degree 3, we have a permutation $\sigma \in \mathfrak{S}_4$ such that

$$\operatorname{div}(u) = [D_{\sigma(1)}] + [D_{\sigma(2)}] + \left[-D_{\sigma(1)} - D_{\sigma(2)}\right] - 3[0_E],$$

and

$$\operatorname{div}(v^{(q)} \circ \tau_Q) = [D_{\sigma(3)}] + [D_{\sigma(4)}] + \left[-D_{\sigma(3)} - D_{\sigma(4)} - 3Q\right] - 3[-Q].$$

The second equality implies

$$\operatorname{div}(v^{(q)}) = [D_{\sigma(3)} + Q] + [D_{\sigma(4)} + Q] + \left[-D_{\sigma(3)} - D_{\sigma(4)} - 2Q\right] - 3[0_E].$$

Note that, as should be expected, the number of ways to split D into two parts of 2 points is exactly the degree of S, the image of the Segre embedding Ξ from Lemma 3.3. We found an exhaustive description of the set of exceptional points $S \cap H$.

There are 6 exceptional points $U^i V^{iq}$ in the intersection of X_0 with S. Up to reindexing, we necessarily have the following triples of aligned points:

$$(V^1, V^2, V^3), (V^1, V^4, V^5), (V^2, V^5, V^6), (V^3, V^4, V^6),$$
$$(U^4, U^5, U^6), (U^2, U^3, U^6), (U^1, U^3, U^4), (U^1, U^2, U^5),$$

They arise as follows. Consider the 6 pairs of distinct points dividing $D = \sum_{i=1}^4 [D_i]$,

$$\{a_1, \dots, a_6\} = \{(D_3, D_4), (D_2, D_3), (D_2, D_4), (D_1, D_4), (D_1, D_3), (D_1, D_2)\}.$$

For each i, if $a_i = (D_j, D_k)$, then U^i defines the line passing through D_j and D_k, while $V^{i(q)}$ defines the line passing through $D_m + Q$ and $D_n + Q$, where $\{j, k, m, n\} = \{1, 2, 3, 4\}$. With this indexing, we can see that U^4, U^5, and U^6 are aligned because they all have a root at D_1 (i.e., the corresponding lines intersect at the point D_1). All the alignments listed above arise in this way.

As in the 3–to–2 case, we follow the strategy outlined in Section 4.1, so we fix a point $s \in X_0$, say $s = (V^1)^q U^1$, and its two preimages $a = ((V^1)^q U^1, U_1)$ and $b = ((V^1)^q U^1, V^1)$ in X_1.

5.2. **Summary of the traps.** As long as D is not a trap, there should be no other alignement between the points U^i and V^i than the ones listed above. Hence we define the following varieties of traps, where $\ell(R, S)$ denotes the line passing through R and S :

$$\mathscr{T}_4^0 = \left\{ \sum_{k=1}^4 [D_k] \;\middle|\; \begin{array}{l} \ell(D_i, D_j) \cap \ell(D_m, D_n) \cap \ell(D_r, D_s) \neq \emptyset, \\ \{i,j\}, \{m,n\}, \{r,s\} \text{ all distinct, and } \{i,j\} \cap \{m,n\} \cap \{r,s\} = \emptyset \end{array} \right\}$$

$$\mathscr{T}_4^1 = \left\{ \sum_{k=1}^4 [D_k] \;\middle|\; \begin{array}{l} \ell(D_i + Q, D_j + Q) \cap \ell(D_m + Q, D_n + Q) \cap \ell(D_r + Q, D_s + Q) \neq \emptyset, \\ \{i,j\}, \{m,n\}, \{r,s\} \text{ all distinct, and } \{i,j\} \cap \{m,n\} \cap \{r,s\} = \emptyset \end{array} \right\}$$

$$\mathscr{T}_4^2 = \left\{ \sum_{k=1}^4 [D_k] \;\middle|\; \begin{array}{l} \ell(D_i, D_j)^{(q)} \cap \ell(D_m, D_n)^{(q)} \cap \ell(D_r + Q, D_s + Q) \neq \emptyset, \\ \text{and } \{i,j\} \neq \{m,n\} \end{array} \right\}$$

$$\mathscr{T}_4^3 = \left\{ \sum_{k=1}^4 [D_k] \;\middle|\; \begin{array}{l} \ell(D_i + Q, D_j + Q) \cap \ell(D_m + Q, D_n + Q) \cap \ell(D_r, D_s)^{(q)} \neq \emptyset, \\ \text{and } \{i,j\} \neq \{m,n\} \end{array} \right\}$$

$$\mathscr{T}_4^4 = \{F + [D_4] \mid \; F \in \mathscr{P}_3, D_4 \in E\}.$$

The conditional statements are to be understood as "*there exist indices i, j, m, n, r, s such that $i \neq j$, $m \neq n$, $r \neq s$, and...* ". Let $\mathscr{T}_4' = \bigcup_{i=0}^3 \mathscr{T}_4^i$. Note that the full variety of traps $\mathscr{T}_4$ (rather than $\mathscr{T}_4'$) requires an additional component, studied in Section 5.9.

Lemma 5.1. *For any points $P_0, P_1 \in E$ such that either $P_0 \neq P_1$ or $P_0^{(q)} \neq P_0 + 2Q$, we have $\mathscr{P}_2(P_0) + \mathscr{P}_2(P_1) \not\subset \mathscr{T}_4'$.*

Proof. Let $R, T \in E$, and $D = \sum_{i=1}^4 [D_i] \in \mathscr{P}_2(P_0) + \mathscr{P}_2(P_1)$, where

$$(D_1, D_2, D_3, D_4) = (R, P_0 - R, T, P_1 - T).$$

We simply need to show that $D \notin \mathscr{T}_4$ except for certain pairs (R, T) that belong to some strict subvariety of E^2. There are many conditions to check in order to verify whether or not $D \in \mathscr{T}_4$; we use symmetries (exchanging R and T, replacing R with $P_0 - R$, or some permutations of the three sets $\{i,j\}, \{m,n\}, \{r,s\}$) to significantly reduce this number.

First, let us characterise the cases where $D \notin \mathscr{T}_4^0$. Up to symmetry, we can assume that 1 belongs to two of the pairs of indices, and even that $(i,j) = (1,3)$, $m = 1$ and $n \in \{2,4\}$. As

long as $D_2 = P_0 - R$ and $D_4 = P_1 - T$ are not on the line $\ell(R,T)$ (which corresponds to a strict subvariety of E^2), we have $\ell(D_i, D_j) \cap \ell(D_m, D_n) = \{R\}$. The condition for $D \in \mathscr{T}_4^0$ is then

$$R \in \ell(D_r, D_s),$$

and for each allowable (r,s), it corresponds to (R,T) belonging to a strict subvariety of E^2. This implies that $\mathscr{P}_2(P_0) + \mathscr{P}_2(P_1) \not\subset \mathscr{T}_4^0$. The fact that $\mathscr{P}_2(P_0) + \mathscr{P}_2(P_1) \not\subset \mathscr{T}_4^1$ follows from the observation that $\mathscr{T}_4^1$ is a translation by $-Q$ of $\mathscr{T}_4^0$, and that $\mathscr{P}_2(P_0 + 2Q) + \mathscr{P}_2(P_0 + 2Q) \not\subset \mathscr{T}_4^0$.

The condition $D \notin \mathscr{T}_4^2$ enjoys fewer symmetries and is therefore more cumbersome. First assume that $\{i,j\} \cap \{m,n\} \neq \emptyset$. Then, up to symmetry, we can assume $i = m = 1$, and apart from a strict subvariety of E^2, we have $\ell(D_i, D_j)^{(q)} \cap \ell(D_m, D_n)^{(q)} = \{R^{(q)}\}$. The conditions for $D \in \mathscr{T}_4^2$ become

$$R^{(q)} \in \ell(D_r + Q, D_s + Q),$$

for any allowable $r \neq s$. None of them is satisfied as long as

$$R^{(q)} \notin \{D_r + Q \mid r = 1,2,3,4\} \cup \{-(D_r + Q) - (D_s + Q) \mid r \neq s\},$$

which for any fixed T corresponds to finitely many values of R to be avoided.

It remains to consider the cases where $\{i,j\} \cap \{m,n\} = \emptyset$. To continue the proof, let us work in E^4 instead of $\mathscr{D}_4$. More precisely, write

$$T_4^2(i,j,m,n,r,s) = \left\{ (D_k)_{k=1}^4 \mid \ell(D_i, D_j)^{(q)} \cap \ell(D_m, D_n)^{(q)} \cap \ell(D_r + Q, D_s + Q) \neq \emptyset \right\},$$

such that $\mathscr{T}_4^2$ is the union of the varieties $\pi(T_4^2(i,j,m,n,r,s))$ for all allowable indices, where $\pi : E^4 \to \mathscr{D}_4$ is the natural projetion. It is then sufficient to show that for each allowable (i,j,m,n,r,s), we have $\pi^{-1}(\mathscr{P}_2(P_0) + \mathscr{P}_2(P_1)) \not\subset \pi^{-1}(\pi(T_4^2(i,j,m,n,r,s)))$. This is equivalent to showing that $\pi^{-1}(\mathscr{P}_2(P_0)) \times \pi^{-1}(\mathscr{P}_2(P_1)) \not\subset T_4^2(i,j,m,n,r,s)$ for any allowable indices; this follows from the facts that $\pi^{-1}(\mathscr{P}_2(P_0)) \times \pi^{-1}(\mathscr{P}_2(P_1))$ is absolutely irreducible, and that for any permutation $\sigma \in \mathfrak{S}_4$, we have

$$(D_k)_{k=1}^4 \in T_4^2(i,j,m,n,r,s) \iff (D_{\sigma(k)})_{k=1}^4 \in T_4^2(\sigma(i), \sigma(j), \sigma(m), \sigma(n), \sigma(r), \sigma(s)).$$

Up to symmetry, it is sufficient to consider $(i,j,m,n) = (1,2,3,4)$ or $(i,j,m,n) = (1,3,2,4)$.

First, suppose that $(i,j,m,n) = (1,2,3,4)$. Again up to symmetries, it is sufficient to consider $(r,s) = (2,3)$ or $(3,4)$. Suppose $(r,s) = (3,4)$, and let

$$(D_1, D_2, D_3, D_4) = (R, P_0 - R, T, P_1 - T) \in \pi^{-1}(\mathscr{P}_2(P_0)) \times \pi^{-1}(\mathscr{P}_2(P_1)).$$

First, if $P_0 = P_1$, then $\ell(D_1, D_2)^{(q)} \cap \ell(D_3, D_4)^{(q)} = -P_0^{(q)}$, and $\ell(D_3 + Q, D_4 + Q) \cap E = \{T + Q, P_0 - T + Q, -P_0 - 2Q\}$ does not contain $-P_0^{(q)}$ for almost all points R and T (as long as $P_0^{(q)} \neq P_0 + 2Q$). If $P_0 \neq P_1$, let $R = T$. Then, $\ell(D_1, D_2)^{(q)} \cap \ell(D_3, D_4)^{(q)} = R^{(q)}$. The condition becomes $R^{(q)} \in \ell(D_3 + Q, D_4 + Q)$. But $R^{(q)}$ is on E, and

$$\ell(D_3 + Q, D_4 + Q) \cap E = \{R + Q, P_1 - R + Q, -P_1 - 2Q\}.$$

For all but finitely many points R, we have that $R^{(q)}$ does not belong to this intersection.

The case $(r,s) = (2,3)$ is similar. The same reasoning allows to conclude for the remaining cases $(i,j,m,n,r,s) \in \{(1,3,2,4,1,2), (1,3,2,4,1,3)\}$, at least for $P_0 \neq P_1$; for $P_0 = P_1$, one should choose T to be one of the points such that $2T = P_0$ and $T^{(q)} \neq -P_0 - 2Q$, then observe that for almost all R, the condition for $\mathscr{T}_4^2$ is not satisfied. The proof for $\mathscr{T}_4^3$ is similar, and the proof for $\mathscr{T}_4^4$ is easy. □

Lemma 5.2. *Suppose D is not a trap. Pick a matrix in* PGL_3 *sending U^1 to x_0, V^1 to x_1, and V^2 to x_2, and let it act on $\mathbf{P}(V)$. In the matrix defining the transformation of H, the submatrices*

$$\begin{pmatrix} H_{00} & H_{01} & H_{02} & H_{20} \end{pmatrix}, \begin{pmatrix} H_{00} & H_{01} & H_{11} & H_{12} \end{pmatrix}, \text{ and } \begin{pmatrix} H_{00} & H_{02} & H_{11} & H_{12} \end{pmatrix}.$$

each have full rank 4.

Proof. Using a matrix of PGL_3 as described, we can suppose that $U^1 = x_0$, $V^1 = x_1$, and $V^2 = x_2$. Since $(V^1)^q U^1 = x_1^q x_0 \in H$, we have that H_{10} is the zero vector. Suppose by contradiction that $\operatorname{rank}\begin{pmatrix} H_{00} & H_{01} & H_{02} & H_{20}\end{pmatrix} \leq 3$. Then, a non-trivial linear-combination of the rows has the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 & D_{11} & D_{12} & 0 & D_{21} & D_{22}\end{pmatrix}$$

Applied to U^2 and $V^2 = x_2$, we get that U^2 is on the line $(0 : D_{21} : D_{22})$. But $U^1 = x_0$ also lies on this line, therefore so does U^5. The relation applied to (U^5, V^5) implies that U^5 lies on the line $(0 : D_{11} : D_{12})$ (unless V^5 is on the line $u_1 = 0$, which already contains $U^1 = x_0$ and $V^2 = x_2$, a contradiction). But U^1 also does, so $(0 : D_{21} : D_{22}) = (0 : D_{11} : D_{12})$. The relation becomes

$$(\alpha v_1^q + \beta v_2^q)(D_{11}u_1 + D_{12}u_2),$$

where $(\alpha, \beta) \neq (0, 0)$ are coefficient such that $\alpha(D_{21}, D_{22}) = \beta D_{21}(D_{11}, D_{12})$. We conclude that $(0 : \alpha : \beta)$ is the line passing through $(V^3)^{(q)}$,$(V^4)^{(q)}$ and $(V^6)^{(q)}$, and it also contains $x_0 = (U^1)^{(q)}$, a contradiction.

Now, suppose by contradiction that $\operatorname{rank}\begin{pmatrix} H_{00} & H_{01} & H_{11} & H_{12}\end{pmatrix} \leq 3$. We get a non-trivial linear combination of the rows of the form

$$\begin{pmatrix} 0 & 0 & C_{02} & 0 & 0 & 0 & C_{20} & C_{21} & C_{22}\end{pmatrix}$$

First, we cannot have $C_{02} = 0$, otherwise the above line gives the relation $v_2^q(C_{20}u_0 + C_{21}u_1 + C_{22}u_2)$: since no more that three of the U^i-points can be on the line $(C_{20} : C_{21} : C_{22})$, at least three of the V^i-points must be on the line $(0 : 0 : 1)$, which also contains U^1, a contradiction. We can therefore assume that $C_{02} = 1$. We deduce that the line through U^2 and U^3 is $(C_{20} : C_{21} : C_{22})$. This line contains U^6. We get that

$$0 = (V_0^6)^q U_2^6 + (V_2^6)^q (C_{20}U_0^6 + C_{21}U_1^6 + C_{22}U_2^6) = (V_0^6)^q U_2^6.$$

We get that either $V_0^6 = 0$, implying that V^6 is aligned with V^1, V^2, V^3, or $U_2^6 = 0$, implying that U^6 is aligned with U^1 and V^1. Both cases are a contradiction. The same proof leads to $\operatorname{rank}\begin{pmatrix} H_{00} & H_{02} & H_{11} & H_{12}\end{pmatrix} = 4$. □

5.3. **Irreducibility of X_0.** In this section, we prove that X_0 has an absolutely irreducible component defined over k. To do so, we first find an equation for X_0 in the plane. Recall that $\mathbf{P}(\Lambda)$ has coordinates u_0, u_1 and u_2, and each point $(u_0 : u_1 : u_2)$ represents the linear polynomial $u_0x_0 + u_1x_1 + u_2x_2$. Its dual space $\mathbf{P}(\Lambda)^\vee$ has coordinates t_0, t_1 and t_2, and any element $(t_0 : t_1 : t_2) \in \mathbf{P}(\Lambda)^\vee$ represents the line in $\mathbf{P}(\Lambda)$ with equation $u_0t_0 + u_1t_1 + u_2t_2 = 0$. Define a subvariety $\mathscr{O}$ of $\mathbf{P}(V) \times \mathbf{P}(\Lambda)^\vee$ by the six polynomials $e_k = \sum_{j=0}^2 a_{kj}t_j$ and $f_k = \sum_{i=0}^2 a_{ik}t_i^q$ for $k = 0, 1, 2$, where a_{ij} are the coordinates of $\mathbf{P}(V)$.

Lemma 5.3. *The variety $\mathscr{O}$ is the closure of the orbit $\mathrm{PGL}_3 \star \mathfrak{d}$. Furthermore, for any point $(f, \ell) \in \mathscr{O}$, any linear factor of f is on the line $\ell \subseteq \mathbf{P}(\Lambda)$.*

Proof. Notice that PGL_3 acts on both $\mathscr{O}$ and $\mathbf{P}(\Lambda)^\vee$, and the projection $\mathscr{O} \to \mathbf{P}(\Lambda)^\vee$ is PGL_3-equivariant. The group PGL_3 acts faithfully on $\mathbf{P}(\Lambda)^\vee$, and the fibre of $(0 : 0 : 1)$ through $\mathscr{O} \to \mathbf{P}(\Lambda)^\vee$ is the subvariety $\mathbf{P}(V_2) \subset \mathbf{P}(V)$ where $V_2 = \operatorname{span}(x_i^q x_i \mid i, j \in \{0, 1\})$. Any $f \in \mathbf{P}(V_2)$ is a polynomial in x_0 and x_1, so its linear factors necessarily lie on the line in $\mathbf{P}(\Lambda)$ defined by $\ell = (0 : 0 : 1)$ (i.e., by the equation $u_2 = 0$), proving the second part of the lemma. The group PGL_2 acts on this fibre through the embedding into PGL_3 as the 2×2 upper-left minor. We conclude from [KW18, Lemma 2.2], which implies that the fibre $\mathbf{P}(V_2)$ is the closure of the action of PGL_2, proving the first part of the lemma. □

Let $h_1, \ldots, h_4$ be the linearly independent linear polynomials in the a_{ij}-coordinates which define the hyperplane $H \subset \mathbf{P}(V)$ of codimension 4, and let $C = \mathscr{O} \cap (H \times \mathbf{P}(\Lambda)^\vee)$, so that X_0 is a subvariety of C. Let $C' \subset \mathbf{P}(\Lambda)^\vee$ be the projection of C to the second factor of $\mathbf{P}(V) \times \mathbf{P}(\Lambda)^\vee$. In the remainder of this section, we prove that all the absolutely irreducible components of C' (and therefore also of X_0) are defined over k.

Lemma 5.4. *The projection $C \to C'$ is an injective map on the geometric points.*

Lemma 5.5. *The plane curve C' is defined by the polynomial (in projective coordinates t_0, t_1, t_2)*

$$t_2^{-1} \cdot \det \begin{pmatrix} t_0^q & & & t_1^q & & & t_2^q & & \\ & t_0^q & & & t_1^q & & & t_2^q & \\ t_0 & t_1 & t_2 & & & & & & \\ & & & t_0 & t_1 & t_2 & & & \\ & & & & & & t_0 & t_1 & t_2 \\ H_{00} & H_{01} & H_{02} & H_{10} & H_{11} & H_{12} & H_{20} & H_{21} & H_{22} \end{pmatrix},$$

where H_{ij} denotes the 4-dimensional vector whose entries are the coefficients of a_{ij} in $h_1, \dots, h_4$. The curve C' has degree $2q+2$.

Proof. The six polynomials e_k, f_k, $k = 0, 1, 2$, as well as $h_1, \dots, h_4$ are linear polynomials in the a_{ij}-coordinates, thus they can be written as Ma_{vec} where M is the 10×9-matrix of coefficients and

$$a_{vec} = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{10} & a_{11} & a_{12} & a_{20} & a_{21} & a_{22} \end{pmatrix}^t.$$

Pick a row of M corresponding to one of the six polynomials e_k, f_k, $k = 0, 1, 2$, add a column to M containing zeros except at the chosen row where the entry is t_k^{-q} if e_k was chosen and t_k^{-1} if f_k was chosen, denote the resulting 10×10-matrix by M' and let $f = \det(M')$. If two rows (of the six above) are chosen and the corresponding entries are set in the adjoined column (with a possible sign change of one of them), it follows from the relation $\sum_{k=0}^2 t_k^q e_k - \sum_{k=0}^2 t_k f_k = 0$ that the determinant of the matrix is zero. Then Laplace expansion with respect to the adjoined column shows that the definition of f is independent (up to sign) of the choice of one of the six rows. By choosing f_2, deleting the adjoined column as well as the row corresponding to f_2 and setting $t_2 = 0$ it follows from $\sum_{k=0}^1 t_k^q e_k - \sum_{k=0}^1 t_k f_k = 0$ that the determinant of the resulting matrix is zero which implies that f is a polynomial. Therefore f defines the variety C'.

It remains to show that f has degree $2q+2$. Choose an arbitrary point $P \in C \cap (S \times \mathbf{P}(\Lambda)^\vee)$. There is an element $g \in \mathrm{PGL}_3$ which maps P to $(x_1^q x_0, (0 : 0 : 1))$. Since this element is a linear transformation of $\mathbf{P}(\Lambda)^\vee$, it does not change the degree of the curve, and we can simply assume that $(x_1^q x_0, (0 : 0 : 1)) \in C$. This implies that in each equation h_i, the coefficient of a_{10} is zero. Now, an simple computation shows that the coefficient of the monomial $t_2^{2q} t_0 t_2$ is $\det \begin{pmatrix} H_{00} & H_{01} & H_{11} & H_{12} \end{pmatrix}$. From Lemma 5.2, it is not zero, so the degree of the equation is $2q+2$. □

Lemma 5.6. *Let N be the matrix from Lemma 5.5, such that $f = t_2^{-1} \det(N)$ is an equation defining C'. We have*

$$\frac{\partial f}{\partial t_0} = t_2^{-1}(m_{31} + m_{44} + m_{57}), \text{ and } \frac{\partial f}{\partial t_1} = t_2^{-1}(m_{32} + m_{45} + m_{58}),$$

where m_{ij} is the (i,j)-minor of N.

Proof. This is an elementary application of Jacobi's formula $d\det(N) = \mathrm{tr}(\mathrm{adj}(N) dN)$, where $\mathrm{adj}(N)$ is the adjoint matrix, and dN is the differential of N. □

Corollary 5.7. *The image in C' of any point in $C \cap S$ is smooth.*

Proof. Let $P \in C \cap S$. There is an element $g \in \mathrm{PGL}_3$ which maps P to $(x_1^q x_0, (0 : 0 : 1))$. This transformation will map the 4-codimensional hyperplane $\tilde{H} \subset \mathbf{P}(V)$ used in the definition of X_0 to a 4-codimensional hyperplane H with defining polynomials $h_1, \dots, h_4$, for each of which the coefficient of a_{10} is zero. From Lemma 5.6, and the fact that $m_{31}(0 : 0 : 1) = m_{57}(0 : 0 : 1) = 0$, we get that

$$\frac{\partial f}{\partial t_0}(0 : 0 : 1) = m_{44}(0 : 0 : 1) = \pm \det \begin{pmatrix} H_{00} & H_{01} & H_{11} & H_{12} \end{pmatrix}.$$

From Lemma 5.2, the latter determinant is non-zero, hence the image of P on C' is smooth. □

Let us now study the singularities of C' away from S. As above, up to a transformation by a matrix $g \in \mathrm{PGL}_3$, it is sufficient to study the point $(x_1^q x_0 - x_0 x_1^q, (0 : 0 : 1)) \in \mathscr{O} \cap H$ with $H_{01} = H_{10}$. Note that with this transformation, the H_{ij}-columns change, and they do not have,

for instance, the properties of Lemma 5.2. We now have that the minors $m_{31}, m_{57}, m_{45}, m_{58}$ are all zero at $(0:0:1)$, and

$$\frac{\partial f}{\partial t_0}(0:0:1) = m_{44}(0:0:1) = \pm \det \begin{pmatrix} H_{00} & H_{01} & H_{11} & H_{12} \end{pmatrix}, \text{ and}$$
$$\frac{\partial f}{\partial t_1}(0:0:1) = m_{32}(0:0:1) = \pm \det \begin{pmatrix} H_{00} & H_{02} & H_{10} & H_{11} \end{pmatrix}.$$

The point is singular if and only if both determinants are zero, i.e.,

$$\operatorname{rank} \begin{pmatrix} H_{00} & H_{01} & H_{02} & H_{11} & H_{12} \end{pmatrix} \leq 3.$$

From now on, suppose that the point is indeed singular, so there is a linear combination of the linear equations h_i that has the form $\alpha a_{20} + \beta a_{21} + \gamma a_{22}$, corresponding to the row vector

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \alpha & \beta & \gamma \end{pmatrix}.$$

One must have $(\alpha, \beta) \neq (0,0)$, otherwise all the points in $X_0 \cap S$ satisfy the equation $v_2^q u_2 = 0$, meaning that among all the linear functions U^i and V^i, at least six of them are on the line $(0:0:1) \in \mathbf{P}(V)^\vee$, a trap. Let us show that the singularity has multiplicity q. From the curve equation given in Lemma 5.5, we derive that the quadratic terms at our point $(x_1^q x_0 - x_0 x_1^q, (0:0:1))$ are

$$\pm \det \begin{pmatrix} H_{01} & H_{02} & H_{11} & H_{12} \end{pmatrix} t_0^2,$$
$$\pm \det \begin{pmatrix} H_{00} & H_{02} & H_{11} & H_{12} \end{pmatrix} t_0 t_1,$$
$$\pm \det \begin{pmatrix} H_{00} & H_{02} & H_{10} & H_{12} \end{pmatrix} t_1^2,$$

which are all zero since $\operatorname{rank} \begin{pmatrix} H_{00} & H_{01} & H_{02} & H_{11} & H_{12} \end{pmatrix} \leq 3$. Now, the terms of degree q are

$$\pm \det \begin{pmatrix} H_{00} & H_{10} & H_{11} & H_{21} \end{pmatrix} t_0^q,$$
$$\pm \det \begin{pmatrix} H_{00} & H_{01} & H_{11} & H_{20} \end{pmatrix} t_1^q,$$

which are not both zero, as that would imply $(\alpha, \beta) = (0,0)$. So the multiplicity is q.

We now show that the blowup of this singularity is either a single smooth point or a node. Without loss of generality, assume $h_1 = \alpha a_{20} + \beta a_{21} + \gamma a_{22}$, and denote by $\tilde{H}_{ij}$ the 3-dimensional vector whose entries are the coefficients of a_{ij} in h_2, h_3 and h_4. Then, restricting to the affine plane $\mathbf{A}^2 \subset \mathbf{P}(\Lambda)^\vee$ defined by $t_2 = 1$, and considering one affine chart of the blowup at $P_0 = (0,0)$ obtained by setting $t_1 = st_0$, one obtains the equation

$$\det \begin{pmatrix} t_0^q & & & s^q t_0^q & & & 1 & & \\ & t_0^q & & & s^q t_0^q & & & 1 & \\ t_0 & st_0 & 1 & & & & & & \\ & & & t_0 & st_0 & 1 & & & \\ & & & & & & t_0 & st_0 & 1 \\ & & & & & & \alpha & \beta & \gamma \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{02} & \tilde{H}_{10} & \tilde{H}_{11} & \tilde{H}_{12} & \tilde{H}_{20} & \tilde{H}_{21} & \tilde{H}_{22} \end{pmatrix} = t_0^q \det(M_2),$$

where

$$M_2 = \begin{pmatrix} 1 & & & s^q & & & 1 & & \\ & 1 & & & s^q & & & 1 & \\ t_0 & st_0 & 1 & & & & & & \\ & & & t_0 & st_0 & 1 & & & \\ & & & & & & t_0 & st_0 & 1 \\ & & & & & & \alpha & \beta & \gamma \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{02} & \tilde{H}_{10} & \tilde{H}_{11} & \tilde{H}_{12} & t_0^q \tilde{H}_{20} & t_0^q \tilde{H}_{21} & t_0^q \tilde{H}_{22} \end{pmatrix}$$

for the pre-image (the equality follows by multiplying the last three columns by t_0^q as well as multiplying the first, second, fifth and sixth row by t_0^{-q}). At $t_0 = 0$, the determinant of M_2

becomes, up to sign,

$$\det\begin{pmatrix} 1 & & s^q & & 1 & \\ & 1 & & s^q & & 1 \\ & & & & \alpha & \beta \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{10} & \tilde{H}_{11} & & \end{pmatrix} = \pm(\alpha s^q - \beta)\det\begin{pmatrix}\tilde{H}_{00} & \tilde{H}_{10} & \tilde{H}_{11}\end{pmatrix}.$$

So the preimage P_1 of P_0 in the blowup of C' is the single point at $t_0 = 0$ and $s = (\beta/\alpha)^{1/q}$. Note that if $\alpha = 0$, then $\beta \neq 0$ and one can simply consider another affine patch of the blowup.

Let $\delta = (\beta/\alpha)^{1/q}$, and set $v = s - \delta$ so that P_1 is given by $t_0 = v = 0$. We now show that either P_1 is non-singular, or it is a singular point of multiplicity 2 with two branches with distinct tangents. To do so, we compute the linear and quadratic terms of $\det(M_2)$. It is sufficient to compute $\det(M_2)$ modulo the ideal (t_0^q, v^q) in $k[t_0, v]$. Up to sign, it is equal to the determinant of M_3 with

$$M_3 = \begin{pmatrix} 1 & & & \delta^q & & & 1 & & \\ & 1 & & & \delta^q & & & 1 & \\ t_0 & \delta t_0 + vt_0 & 1 & & & & & & \\ & & & t_0 & \delta t_0 + vt_0 & 1 & & & \\ & & & & & & t_0 & \delta t_0 + vt_0 & 1 \\ & & & & & & \alpha & \beta & \gamma \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{02} & \tilde{H}_{10} & \tilde{H}_{11} & \tilde{H}_{12} & & & \end{pmatrix},$$

and by subtracting the second column from the fourth one, subtracting δ^q times the seventh column from the fourth one as well as adding the eighth column to the fourth one, it follows that $\det(M_3) = t_0 \det(M_4)$ with

$$M_4 = \begin{pmatrix} 1 & & & & & & 1 & & \\ & 1 & & & \delta^q & & & 1 & \\ t_0 & \delta t_0 + vt_0 & 1 & -\delta - v & & & & & \\ & & & 1 & \delta t_0 + vt_0 & 1 & & & \\ & & & -\delta^q + \delta + v & & & t_0 & \delta t_0 + vt_0 & 1 \\ & & & & & & \alpha & \beta & \gamma \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{02} & & \tilde{H}_{11} & \tilde{H}_{12} & & & \end{pmatrix}.$$

From $\det(M_3) = t_0 \det(M_4)$, we deduce that the constant term of $\det(M_4)$ gives the linear term of the equation, and the linear term in v for $\det(M_4)$ gives us the quadratic term in $t_0 v$ in $\det(M_3)$. In order to find these two terms, we can set $t_0 = 0$ in M_4. Subtracting the eighth column from the second, subtracting δ^q times the eighth from the fifth one, and removing the second row as well as the eighth one, one obtains that $\det(M_4) = \pm\det(M_5)$ with

$$M_5 = \begin{pmatrix} 1 & & & & & & 1 & \\ & & 1 & -\delta - v & & & & \\ & & & 1 & & 1 & & \\ & & & -\delta^q + \delta + v & & & & 1 \\ & -\beta & & & -\delta^q\beta & & \alpha & \gamma \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{02} & & \tilde{H}_{11} & \tilde{H}_{12} & & \end{pmatrix}.$$

By subtracting the seventh column from the first one and removing the first row as well as the seventh column, one obtains $\det(M_5) = \pm\det(M_6)$ with

$$M_6 = \begin{pmatrix} & & 1 & -\delta - v & & & \\ & & & 1 & & 1 & \\ & & & -\delta^q + \delta + v & & & 1 \\ -\alpha & -\beta & & & -\delta^q\beta & & \gamma \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{02} & & \tilde{H}_{11} & \tilde{H}_{12} & \end{pmatrix}.$$

By subtracting the fourth column from the sixth one and removing the second row as well as the fourth column, one obtains $\det(M_6) = \pm\det(M_7)$ with

$$M_7 = \begin{pmatrix} & & 1 & & \delta+v & \\ & & & & \delta^q-\delta-v & 1 \\ -\alpha & -\beta & & -\delta^q\beta & & \gamma \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{02} & \tilde{H}_{11} & \tilde{H}_{12} & \end{pmatrix},$$

and by subtracting $\delta + v$ times the third column from the fifth one, subtracting $\delta^q - \delta - v$ times the sixth column from the fifth one and removing the first two rows as well as the third and sixth column, one obtains $\det(M_7) = \pm\det(M_8)$ with

$$M_8 = \begin{pmatrix} \alpha & \beta & \delta^q\beta & \gamma(-\delta^q+\delta+v) \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{11} & (\delta+v)\tilde{H}_{02} - \tilde{H}_{12} \end{pmatrix},$$

Finally, we have $\det(M_8) = \delta\det(M_9) - \det(M_{10}) + v\det(M_9)$ with

$$M_9 = \begin{pmatrix} \alpha & \beta & \delta^q\beta & \gamma \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{11} & \tilde{H}_{02} \end{pmatrix}, \text{ and } M_{10} = \begin{pmatrix} \alpha & \beta & \delta^q\beta & \delta^q\gamma \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{11} & \tilde{H}_{12} \end{pmatrix}.$$

Therefore the linear terms of the equation of the blowup of C' consist only of $\pm(\delta\det(M_9) - \det(M_{10}))t_0$, implying that P_1 is non-singular if $\delta\det(M_9) \neq \det(M_{10})$.

If $\delta\det(M_9) = \det(M_{10})$, then P_1 is singular, and the quadratic term of the equation is of the form $t_0(\epsilon t_0 + \det(M_9)v)$ for some coefficient ϵ. As long as $\det(M_9) \neq 0$, P_1 is a singularity of multiplicity 2, with 2 distinct tangents.

Suppose that $\det(M_9) = \det(M_{10}) = 0$. We get that

$$\operatorname{rank}\begin{pmatrix} \alpha & \beta & \gamma & \delta^q\alpha & \delta^q\beta & \delta^q\gamma \\ \tilde{H}_{00} & \tilde{H}_{01} & \tilde{H}_{02} & \tilde{H}_{10} & \tilde{H}_{11} & \tilde{H}_{12} \end{pmatrix} \leq 3.$$

Therefore, there is a linear combination of the equations defining the hyperplane that has the form

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta^q\alpha & \delta^q\beta & \delta^q\gamma & a & b & c \end{pmatrix}.$$

Consider the points $(v_0x_0 + v_1x_1 + v_2x_2)^q(u_0x_0 + u_1x_1 + u_2x_2) \in H \cap S$. First, they must satisfy the equation

$$0 = \alpha v_2u_0 + \beta v_2u_1 + \gamma v_2u_2 = v_2(\alpha u_0 + \beta u_1 + \gamma u_2),$$

so either $v_2 = 0$ or $\alpha u_0 + \beta u_1 + \gamma u_2 = 0$. Second, they must satisfy the equation

$$\begin{aligned} 0 &= \alpha v_0^q u_0 + \beta v_0^q u_1 + \gamma v_0^q u_2 + \delta^q\alpha v_1^q u_0 + \delta^q\beta v_1^q u_1 + \delta^q\gamma v_1^q u_2 + a v_2^q u_0 + b v_2^q u_1 + c v_2^q u_2 \\ &= (v_0 + \delta v_1)^q(\alpha u_0 + \beta u_1 + \gamma u_2) + v_2^q(au_0 + bu_1 + cu_2). \end{aligned}$$

For the points such that $\alpha u_0 + \beta u_1 + \gamma u_2 \neq 0$, one must have $v_2 = 0$, and thereby $v_0 + \delta v_1 = 0$. The only possibility is $(v_0 : v_1 : v_2) = (-\delta : 1 : 0)$. Therefore, there can only be one point such that $\alpha u_0 + \beta u_1 + \gamma u_2 \neq 0$ (two such points would share the factor $-\delta^q x_0^q + x_1^q$, a contradiction). So all the points of $H \cap S$ satisfy $\alpha u_0 + \beta u_1 + \gamma u_2 = 0$, also a contradiction (among the exceptional points, at most 3 can lead to $(u_0 : u_1 : u_2)$ being on a given line).

Corollary 5.8. *The curve C' has four singularities. Each of them has multiplicity q, and is either analytically irreducible, or one blowup results in a node (the intersection of two smooth branches with distinct tangents).*

Proof. We have just shown the last part of the statement: any singular point has multiplicity q, and is either analytically irreducible, or one blowup results in a node. Let us show that there are four singularities. A point is singular if and only if, after the transformation sending its preimage in C to $(x_1^q x_0 - x_0 x_1^q, (0 : 0 : 1))$, we have a relation of the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \alpha & \beta & \gamma \end{pmatrix}.$$

Applied to the points $v^q u = (v_0x_0 + v_1x_1 + v_2x_2)^q(u_0x_0 + u_1x_1 + u_2x_2) \in H \cap S$, we get

$$v_2^q(\alpha u_0 + \beta u_1 + \gamma u_2) = 0.$$

For each $v^q u \in H \cap S$, either $v^{(q)}$ is on the line $(0:0:1)$, or u is on the line $(\alpha:\beta:\gamma)$. There are six such $v^q u$, but no more than three values u or v can lie on any given line. Therefore, for three of the $v^q u \in H \cap S$, the $v^{(q)}$-values are aligned on $(0:0:1)$, and for the other three $v^q u \in H \cap S$, the u-values are aligned. Therefore, a point on $C' \subset \mathbf{P}(V)^\vee$ is singular if and only if it corresponds to one of the lines in $\mathbf{P}(V)$ that contain three $v^{(q)}$-values; since the divisor is not a trap, there are exactly four such lines. □

Proposition 5.9. *All the absolutely irreducible component of the curve X_0 are defined over k.*

Proof. Since it is a plane curve, any two components of C' must intersect, and they can only do so at the singular points $T \subset C'$. Also, a given singular point can be contained in at most 2 of the components (at most one if it is analytically irreducible, and at most 2 if its blowup is a node).

First observe that the number of pairs of irreducible components is at most the number of singularities, so there are at most 3 components. Second, observe that each component is defined over an extension K/k of degree at most 2. Indeed, degree 4 or more would contradict the previous observation. For the degree 3 case, since there are at most three components, there must be exactly 3 Galois-conjugate components. None of the four singularities can be fixed by the Galois action (such a singularity would appear in all three components). Yet, the number of singularities is not divisible by 3, a contradiction.

If there is only one absolutely irreducible component, it is X_0 itself, which is defined over k, and we are done.

If there are two components, either they are both defined over k and we are done, or $C' = A \cup B$, where A and B are two Galois-conjugate absolutely irreducible plane curves. We now deal with the latter case. Since C' has degree $2q+2$, the components each have degree $q+1$, so by Bézout's theorem,

$$(q+1)^2 = A \cdot B = \sum_{P \in A \cap B} I(P, A \cap B) = 4I(P_0, A \cap B),$$

where P_0 is any of the 4 isomorphic singularities of C'. We get $I(P_0, A \cap B) = (q+1)^2/4$. Recall that the multiplicity of each singularity P_0 is q, and their blowups are nodes. Let $f : Z \to \mathbf{P}(V)^\vee$ be the blowup at P_0, let $\tilde{A}$, $\tilde{B}$ and $\tilde{C}'$ be the corresponding blowups of A, B and C' respectively, let E be the exceptional divisor, and let $\tilde{P}_0$ the unique preimage of P_0 in C' (it is a node, at the intersection of $\tilde{A}$ and $\tilde{B}$). Applying the formula [Ful13, Corollary 6.7.1], we get

$$\begin{aligned} I(P_0, A \cap B) &= I(\tilde{P}_0, f^*A \cap f^*B) \\ &= I(\tilde{P}_0, (\tilde{A} + e_{P_0}(A)E) \cap (\tilde{B} + e_{P_0}(B)E)) \\ &= I(\tilde{P}_0, \tilde{A} \cap \tilde{B}) + e_{P_0}(A)e_{P_0}(B), \end{aligned}$$

where $e_{P_0}(A)$ and $e_{P_0}(B)$ are the multiplicities of P_0 on A and B. Since $e_{P_0}(A) + e_{P_0}(B) = q$, we have $e_{P_0}(A)e_{P_0}(B) \leq (q/2)^2$. Since $\tilde{P}_0$ is a node at the intersection of $\tilde{A}$ and $\tilde{B}$, we have $I(\tilde{P}_0, \tilde{A} \cap \tilde{B}) = 1$. Therefore, $I(P_0, A \cap B) \leq (q/2)^2 + 1$, which contradicts the fact that $I(P_0, A \cap B) = (q+1)^2/4$.

Finally, it remains to deal with the case were there are 3 components. If they are all defined over k, we are done, so let us suppose that $C' = A \cup A^\sigma \cup B$, where A is defined over a quadratic extension of k and σ is the corresponding conjugation. Let $a = \deg(A)$ and $b = \deg(B)$. The only possible configuration of the singular points $T = \{P_1, \ldots, P_4\}$ is

$$A \cap A^\sigma = \{P_1\} = \{P_1^\sigma\}, A \cap B = \{P_2\}, A^\sigma \cap B = \{P_3\} = \{P_2^\sigma\}, \text{ and } P_4 = P_4^\sigma \in B.$$

Write $e_i(Z) = e_{P_i}(Z)$ for the multiplicity of P_i on any component Z. We must have $e_1(A) = e_1(A^\sigma)$, and since $e_1(A) + e_1(A^\sigma) = q$, we get $e_1(A) = q/2$. This is a contradiction, unless the characteristic is 2. We have $e_1(A) = q/2$ so $a \geq q/2$, and $e_4(B) = q$, so $b \geq q$. Also, $2a+b = 2q+2$, so either $a = q/2$ and $b = q+2$, or $a = q/2+1$ and $b = q$. From Bézout's theorem, we have

$$I(P_2, A \cap B) = ab = q^2/2 + q.$$

Also, applying the formula [Ful13, Corollary 6.7.1] as in the previous case, we have

$$I(P_2, A \cap B) = 1 + e_2(A)e_2(B) \leq 1 + q^2/4,$$

a contradiction. □

5.4. **Defining equations for X_1.** Consider the action of PGL_3 on $\mathbf{P}(V) \times \mathbf{P}(\Lambda)$, and let W be the closure of the orbit of $(\mathfrak{d}, x_0)$. Suppose $u = u_0x_0 + u_1x_1 + u_2x_2 \in \mathbf{P}(\Lambda)$. We focus on the affine patch $u_0 = 1$, since the rest of the proof is a study of local properties of points on this patch. Consider the matrix

$$m = \begin{pmatrix} 1 & -u_1 & -u_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We have $m^t u = x_0$, so u divides f if and only if x_0 divides $m \star f$, i.e., the coefficient of $x_i^q x_j$ in $m \star f$ is zero for any $i, j \neq 0$. Write $f = \sum_{i,j} a_{ij} x_i^q x_j$. Then,

$$\begin{aligned} m \star f = a_{00}x_0^q x_0 + \sum_{i,j\neq 0} (a_{ij} + a_{00}u_i^q u_j - a_{i0}u_j - a_{0j}u_i^q) x_i^q x_j \\ + \sum_{i\neq 0} (a_{i0} - a_{00}u_i^q) x_i^q x_0 + \sum_{j\neq 0} (a_{0j} - a_{00}u_j) x_0^q x_j. \end{aligned}$$

We deduce that the equations corresponding to the condition that u divides f are

$$E_{ij} : a_{ij} + a_{00}u_i^q u_j - a_{i0}u_j - a_{0j}u_i^q = 0$$

for any indices $i, j \neq 0$. Assuming these hold, we have

$$m \star f = a_{00}x_0^q x_0 + \sum_{i\neq 0} (a_{i0} - a_{00}u_i^q) x_i^q x_0 + \sum_{j\neq 0} (a_{0j} - a_{00}u_j) x_0^q x_j.$$

Furthermore,

$$x_0^q \left(\sum_i b_i x_i \right) - x_0 \left(\sum_i b_i x_i \right)^q = (b_0 - b_0^q) x_0^q x_0 + \sum_i b_i^q x_i^q x_0 + \sum_j b_j x_0^q x_j.$$

So we obtain W by adding the equations

$$F_{ij} : (a_{i0} - a_{00}u_i^q)(a_{0j} - a_{00}u_j)^q - (a_{j0} - a_{00}u_j^q)(a_{0i} - a_{00}u_i)^q = 0.$$

So X_1 is defined by these equations for W and the equations defining the hyperplane $H \subset \mathbf{P}(V)$, in the affine patch $u_0 = 1$.

5.5. **Blowing up $a \in X_1$.** Recall that we have fixed an exceptional point $s = (V^1)^q U^1 \in X_0$, and its two preimages $a = ((V^1)^q U^1, U_1)$ and $b = ((V^1)^q U^1, V^1)$ in X_1. We need to prove that the conditions of Proposition 4.2 are satisfied, starting with the analytic irreducibility of a.

Lemma 5.10. *The point $a \in X_1$ is analytically irreducible.*

Proof. Take a matrix in PGL_3 sending U^1 to x_0, V^1 to x_1, and V^2 to x_2 (in particular, the line passing through V^1, V^2, V^3 is sent to the line $u_0 = 0$). With this transformation, a belongs to the affine patch $u_0 = 1$ of $\mathbf{P}(V) \times \mathbf{P}(\Lambda)$, so we can study it locally through the equations of X_0 derived in Section 5.4. From Lemma 5.2, after applying the action of this matrix, we can rewrite the matrix defining H as

$$\begin{pmatrix} 1 & 0 & 0 & 0 & A_{11} & A_{12} & 0 & A_{21} & A_{22} \\ 0 & 1 & 0 & 0 & B_{11} & B_{12} & 0 & B_{21} & B_{22} \\ 0 & 0 & 1 & 0 & C_{11} & C_{12} & 0 & C_{21} & C_{22} \\ 0 & 0 & 0 & 0 & D_{11} & D_{12} & 1 & D_{21} & D_{22} \end{pmatrix}.$$

with $C_{11}D_{12} - C_{12}D_{11} \neq 0$ and $C_{11}B_{12} - C_{12}B_{11} \neq 0$. Blowing up via $u_2 = u_1t_2$, we get the equations

$$\begin{aligned}
E_{11} &= a_{11} + u_1(a_{00}u_1^q - a_{10} - a_{01}u_1^{q-1}),\\
E_{12} &= a_{12} + u_1(a_{00}u_1^q t_2 - a_{10}t_2 - a_{02}u_1^{q-1}),\\
E_{21} &= a_{21} + u_1(a_{00}u_1^q t_2^q - a_{20} - a_{01}u_1^{q-1}t_2^q),\\
E_{22} &= a_{22} + u_1(a_{00}u_1^q t_2^q t_2 - a_{20}t_2 - a_{02}u_1^{q-1}t_2^q),\\
F_{12} &= (a_{10} - a_{00}u_1^q)(a_{02} - a_{00}u_1t_2)^q - (a_{20} - a_{00}u_1^q t_2^q)(a_{01} - a_{00}u_1)^q.
\end{aligned}$$

For any $Z \in \{A, B, C, D\}$, write $Z_{*i} = Z_{1i} + Z_{2i}t_2^q$, $Z_{i*} = Z_{i1} + Z_{i2}t_2$. We get the relations

$$\begin{pmatrix}
1 + u_1^{q+1}(A_{1*} + A_{2*}t_2^q) & u_1^q A_{*1} & u_1^q A_{*2} & u_1 A_{2*} & u_1 A_{1*}\\
u_1^{q+1}(B_{1*} + B_{2*}t_2^q) & 1 + u_1^q B_{*1} & u_1^q B_{*2} & u_1 B_{2*} & u_1 B_{1*}\\
u_1^{q+1}(C_{1*} + C_{2*}t_2^q) & u_1^q C_{*1} & 1 + u_1^q C_{*2} & u_1 C_{2*} & u_1 C_{1*}\\
u_1^{q+1}(D_{1*} + D_{2*}t_2^q) & u_1^q D_{*1} & u_1^q D_{*2} & 1 + u_1 D_{2*} & u_1 D_{1*}
\end{pmatrix}
\begin{pmatrix} a_{00}\\ a_{01}\\ a_{02}\\ a_{20}\\ a_{10} \end{pmatrix} = 0.$$

Therefore we can eliminate a_{00}, a_{01}, a_{02} and a_{20} in $k[[u_1, t_2]]$, as

$$\begin{aligned}
a_{00} &= u_1(A_{1*} + u_1c_{00}) = u_1b_{00},\\
a_{01} &= u_1(B_{1*} + u_1c_{02}) = u_1b_{01},\\
a_{02} &= u_1(C_{1*} + u_1c_{10}) = u_1b_{02},\\
a_{20} &= u_1(D_{1*} + u_1c_{20}) = u_1b_{20},
\end{aligned}$$

with b_{ij} and c_{ij} in $k[[u_1, t_2]]$. The equation F_{12} becomes

$$u_1^q(1 - a_{00}u_1^q)(b_{02} - b_{00}u_1t_2)^q - u_1u_1^q(b_{20} - b_{00}u_1^q t_2^q)(b_{01} - b_{00}u_1)^q.$$

Recall that $C_{11}D_{12} - C_{12}D_{11} \neq 0$ and $C_{11}B_{12} - C_{12}B_{11} \neq 0$. Since $(C_{11}, C_{12}) \neq (0, 0)$, the equation $b_{02}(t_2) = 0$ has a single solution. It is not a zero of b_{20} nor b_{01}, since neither B_{1*} nor D_{1*} is collinear with C_{1*}. □

5.6. **Blowing up** $b \in X_1$**.** Recall we have the 6 points U^iV^{iq} in the intersection with S, and the 3 points U^1, U^3, U^4 are aligned, as well as V^2, V^5, V^6. Apply the action of a matrix in PGL_3 sending U^1 to x_1, and V^1 to x_0. With this transformation, b belongs to the affine patch $u_0 = 1$ of $\mathbf{P}(V) \times \mathbf{P}(\Lambda)$, so we can study it locally through the equations of X_0 derived in Section 5.4.

Lemma 5.11. *When D is not a trap, the matrix defining H can be written as*

$$\begin{pmatrix}
1 & 0 & 0 & 0 & * & * & 0 & * & *\\
0 & 0 & 1 & 0 & * & * & 0 & * & *\\
0 & 0 & 0 & 1 & C_{11} & * & 0 & C_{21} & *\\
0 & 0 & 0 & 0 & D_{11} & * & 1 & D_{21} & *
\end{pmatrix}$$

with $C_{11}D_{21} - C_{21}D_{11} \neq 0$.

Proof. The matrix can be written in the form

$$\begin{pmatrix}
1 & 0 & 0 & * & * & * & * & * & *\\
0 & 0 & 1 & * & * & * & * & * & *\\
0 & 0 & 0 & C_{10} & C_{11} & C_{12} & C_{20} & C_{21} & C_{22}\\
0 & 0 & 0 & 0 & D_{11} & D_{12} & D_{20} & D_{21} & D_{22}
\end{pmatrix}.$$

If $C_{10}D_{20} \neq 0$, the matrix can then be written as in the lemma. By contradiction, suppose that $C_{10}D_{20} = 0$; we deduce that there is a relation of the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 & E_{11} & E_{12} & 0 & E_{21} & E_{22} \end{pmatrix}$$

Applied to U^4 and V^4, we get that $(V^4)^{(q)}$ is on the line

$$L^4 = (1 : E_{11}U_1^4 + E_{12}U_2^4 : E_{21}U_1^4 + E_{22}U_2^4).$$

But $(V^1)^{(q)} = x_0$ also lies on this line, therefore so does $(V^6)^{(q)}$ (up to a reordering of V^2, V^5, V^6). Similarly, the relation applied to U^6, V^6 implies that $(V^6)^{(q)}$ lies on the line

$$L^6 = (1 : E_{11}U_1^6 + E_{12}U_2^6 : E_{21}U_1^6 + E_{22}U_2^6).$$

Since L^6 also contains $(V^1)^{(q)}$, we have $L^4 = L^6$. Note that (U_1^4, U_2^4) and (U_1^6, U_2^6) are linearly independent (otherwise U^4, U^6 and V^1 would be aligned). Therefore, the equality $L^4 = L^6$ implies that there are $(\alpha, \beta) \neq (0, 0)$ such that $\alpha(E_{12}, E_{22}) = \beta(E_{11}, E_{21})$. The relation becomes

$$(\alpha u_1 + \beta u_2)(E_{11}v_1^q + E_{21}v_2^q).$$

We conclude that $(0 : \alpha : \beta)$ is the line passing through U^2,U^3 and U^5, and it also contains V^1, a contradiction.

The matrix can be written as stated in the lemma, and it remains to prove that $C_{11}D_{21} - C_{21}D_{11} \neq 0$. A proof similar to the above shows that $C_{11}D_{21} - C_{21}D_{11} = 0$ implies that V^1, V^3, and V^4 are aligned, another contradiction. □

Lemma 5.12. *If $D_{11}D_{12}^q \neq D_{11}^q D_{21}$, the point $b \in X_1$ is analytically irreducible.*

Remark 3. We deal with the case $D_{11}D_{12}^q = D_{11}^q D_{21}$ in Section 5.9.

Proof. From Lemma 5.11, we can rewrite the matrix defining H as

$$\begin{pmatrix} 1 & 0 & 0 & 0 & A_{11} & A_{12} & 0 & A_{21} & A_{22} \\ 0 & 0 & 1 & 0 & B_{11} & B_{12} & 0 & B_{21} & B_{22} \\ 0 & 0 & 0 & 1 & C_{11} & C_{12} & 0 & C_{21} & C_{22} \\ 0 & 0 & 0 & 0 & D_{11} & D_{12} & 1 & D_{21} & D_{22} \end{pmatrix}$$

After blowing up via $u_2 = u_1t_2$, we get the equations

$$\begin{aligned} E_{11} &= a_{11} + u_1(a_{00}u_1^q - a_{10} - a_{01}u_1^{q-1}), \\ E_{12} &= a_{12} + u_1(a_{00}u_1^q t_2 - a_{10}t_2 - a_{02}u_1^{q-1}), \\ E_{21} &= a_{21} + u_1(a_{00}u_1^q t_2^q - a_{20} - a_{01}u_1^{q-1}t_2^q), \\ E_{22} &= a_{22} + u_1(a_{00}u_1^q t_2^q t_2 - a_{20}t_2 - a_{02}u_1^{q-1}t_2^q), \\ F_{12} &= (a_{10} - a_{00}u_1^q)(a_{02} - a_{00}u_1t_2)^q - (a_{20} - a_{00}u_1^q t_2^q)(a_{01} - a_{00}u_1)^q. \end{aligned}$$

As in the proof of Lemma 5.10, for any $Z \in \{A, B, C, D\}$, write $Z_{*i} = Z_{1i} + Z_{2i}t_2^q$, and $Z_{i*} = Z_{i1} + Z_{i2}t_2$. We get the relations

$$\begin{pmatrix} 1 + u_1^{q+1}(A_{1*} + A_{2*}t_2^q) & u_1^q A_{*2} & u_1 A_{1*} & u_1 A_{2*} & u_1^q A_{*1} \\ u_1^{q+1}(B_{1*} + B_{2*}t_2^q) & 1 + u_1^q B_{*2} & u_1 B_{1*} & u_1 B_{2*} & u_1^q B_{*1} \\ u_1^{q+1}(C_{1*} + C_{2*}t_2^q) & u_1^q C_{*2} & 1 + u_1 C_{1*} & u_1 C_{2*} & u_1^q C_{*1} \\ u_1^{q+1}(D_{1*} + D_{2*}t_2^q) & u_1^q D_{*2} & u_1 D_{1*} & 1 + u_1 D_{2*} & u_1^q D_{*1} \end{pmatrix} \begin{pmatrix} a_{00} \\ a_{02} \\ a_{10} \\ a_{20} \\ a_{01} \end{pmatrix} = 0.$$

Eliminating a_{00}, a_{02}, a_{10} and a_{20} in the ring of formal power series $k[[u_1, t_2]]$ yields

$$\begin{aligned} a_{00} &= u_1^q(A_{*1} + u_1c_{00}) = u_1^q b_{00}, \\ a_{02} &= u_1^q(B_{*1} + u_1c_{02}) = u_1^q b_{02}, \\ a_{10} &= u_1^q(C_{*1} + u_1c_{10}) = u_1^q b_{10}, \\ a_{20} &= u_1^q(D_{*1} + u_1c_{20}) = u_1^q b_{20}, \end{aligned}$$

for some b_{ij} and c_{ij} in $k[[u_1, t_2]]$. We get the equation

$$u_1^q u_1^{q^2}(b_{10} - b_{00}u_1^q)(b_{02} - b_{00}u_1t_2)^q - u_1^q(D_{*1} + u_1c_{20} - b_{00}u_1^q t_2^q)(1 - a_{00}u_1)^q,$$

and removing the factor u_1^q,

$$u_1^{q^2}(b_{10} - b_{00}u_1^q)(b_{02} - b_{00}u_1t_2)^q - (D_{*1} + u_1c_{20} - b_{00}u_1^q t_2^q)(1 - a_{00}u_1)^q.$$

Lemma 5.11 implies that $(D_{11}, D_{21}) \neq (0,0)$, therefore $D_{*1}(t_2) = 0$ has a unique solution (possibly at infinity), with multiplicity q. We have

$$c_{20} = -D_{*1}D_{2*} - D_{1*}C_{*1} + u_1(\dots).$$

Since D_{*1} and C_{*1} are not collinear (Lemma 5.11), when $D_{11}D_{12}^q \neq D_{11}^q D_{21}$, the power series c_{20} is a unit, and we are done. □

Remark 4. Note for later that the power series c_{20} has both a non-zero constant and linear term.

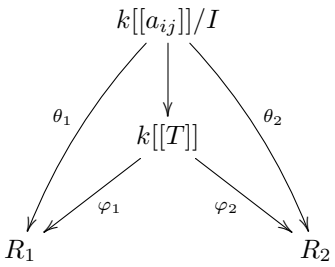
5.7. **Ramification indices.** The completion of the local ring at the desingularisation of a described above is of the form $R_1 = k[[u,t]]/(u - t^q A(u,t))$ for some unit $A(u,t)$. Similarly, at b, it is of the form $R_2 = k[[u,t]]/(u - t^q B(u,t))$ for some unit $B(u,t)$. The projection $X_1 \to X_0$, analytically at a, is of the form

$$\theta_1 : k[[a_{ij}]]/I \longrightarrow R_1 : a_{ij} \longmapsto u b_{ij}(u,t),$$

and analytically at b, it is of the form

$$\theta_2 : k[[a_{ij}]]/I \longrightarrow R_2 : a_{ij} \longmapsto u^q b'_{ij}(u,t).$$

The point s is not smooth in this model of X_0, but we can factor the morphism through the desingularization, leading to the commutative diagram



Let a be a linear combination of a_{ij}-values such that the corresponding combinations of b_{ij} and b'_{ij} are both units (that is possible since not all b_{ij}-values nor all b'_{ij}-values are zeroes locally; see the proofs of Lemmata 5.10 and 5.12). The order of the image of a in $k[[T]]$ is some integer x. For $i = 1, 2$, in R_i, we have

$$q^i = \operatorname{ord}(\theta_i(a)) = x \cdot \operatorname{ord}(\varphi_i(T)).$$

We deduce that $\operatorname{ord}(\varphi_2(T)) = q \cdot \operatorname{ord}(\varphi_1(T))$, and since $\operatorname{ord}(\varphi_1(T)) + \operatorname{ord}(\varphi_2(T)) = q + 1$, we deduce that the first has ramification index 1 and the second ramification index q.

5.8. **Blowing up** $(b,b) \in X_2$**.**

Lemma 5.13. *If $D_{11}D_{12}^q \neq D_{11}^q D_{21}$, the point (b,b) is analytically irreducible.*

Proof. Analytically at the point b, the desingularized equation is, up to multiplication by a unit (in $k[[u_1,t_1]]$, where t_1 is actually the translation to the origin of the previous t_1),

$$u_1 - t_1^q B(u_1, t_1),$$

where $B(u_1, s_1)$ is a unit (with a non-zero linear term, because c_{20} above had a non-zero linear term — see Remark 4). The fibre product at this point with respect to the projection to X_0 is given by the equations in $k[[u,t,v,s]]$

$$\begin{aligned} u - t^q B(u,t) &= 0, \\ v - s^q B(v,s) &= 0, \\ u^q b_{ij}(u,t) - v^q b_{ij}(v,s) &= 0, \end{aligned}$$

for all pairs i, j. There is an automorphism of $k[[u,t]]$ sending $u - t^q B(u,t)$ to u while fixing t. It sends u to some $F(u,t) = u + t^q G(u,t)$ where G is another unit. The same applied to $k[[v,s]]$

sends $v - s^q B(v,s)$ to v, and v to $F(v,s)$, and fixes s. Therefore the curve is isomorphic to the curve given by the equations in $k[[t,s]]$

$$F(0,t)^q b_{ij}(F(0,t),t) - F(0,s)^q b_{ij}(F(0,s),s) = 0.$$

For simplicity, we just write

$$F(t)^q b_{ij}(F(t),t) - F(s)^q b_{ij}(F(s),s) = 0.$$

At least one of them must be non-zero of course, which means $F(t)$ is not the zero polynomial (there are more explicit ways to see this I guess). Write $F(t) = t^q G(t)$ where $G(0) \neq 0$. The equations above are divisible by $t - s$ (which corresponds to the diagonal component of the fibre product). Blow up with $t = st'$. We get

$$\frac{t'^{q^2} G(st')^q b_{ij}(F(st'),st') - G(s)^q b_{ij}(F(s),s)}{(t'-1)} = 0.$$

Pick some indices i, j such that $b_{ij}(0,0) \neq 0$ (they exist since not all b_{ij}-values are zeroes locally; see the proof of Lemma 5.12). The only solution at $s = 0$ is $t' = 1$, which is non-singular. Indeed, the smallest degree (in terms of the variables s and $t'-1$) term of the numerator is $\alpha b_{ij}(0,0)(t'-1)s$ for some non-zero constant α (this comes from the facts that G has a non-zero linear term α and $b_{i,j}$ has no linear term: its first term after the constant is at degree q or larger), which is linear once the denominator removes the factor $t' - 1$. □

5.9. **The case $D_{11}D_{12}^q = D_{11}^q D_{21}$.** It only remains to show that the case $D_{11}D_{12}^q = D_{11}^q D_{21}$ can be avoided: it corresponds to D being some kind of trap.

Lemma 5.14. *One can choose $s \in X_0 \cap S$ such that $D_{11}D_{12}^q \neq D_{11}^q D_{21}$, unless D belongs to a strict subvariety $\mathscr{T}_4^5$ of $\mathscr{D}_4$. For any $P_0, P_1 \in E$, we have $\mathscr{P}_2(P_0) + \mathscr{P}_2(P_1) \not\subset \mathscr{T}_4^5$.*

Proof. Let $\mathscr{T}_4^5$ be the subvariety of $\mathscr{D}_4$ such that $D_{11}D_{12}^q = D_{11}^q D_{21}$ for all the corresponding exceptional points. We need to show that for any $P_0, P_1 \in E$, we have $\mathscr{P}_2(P_0) + \mathscr{P}_2(P_1) \not\subset \mathscr{T}_4^5$. Consider points $R, T \in E$, and the divisor

$$D = [R] + [P_0 - R] + [T] + [P_1 - T] \in \mathscr{P}_2(P_0) + \mathscr{P}_2(P_1).$$

Let $u^1 = \ell(D_1, D_3)$, and $(v^1)^{(q)} = \ell(D_2 + Q, D_4 + Q)$. The following computation shows that $D_{11}D_{12}^q - D_{11}^q D_{21}$ is a non-zero rational function of R and T, at the exceptional point $(v^1)^q u^1$. For simplicity of exposition, we allow exponents $1/q$ in rational functions for the rest of this proof, so we can consider $v^1 = \ell\left(D_2^{(1/q)} + Q, D_4^{(1/q)} + Q\right)$. Consider the matrix

$$m = \begin{pmatrix} v_0^1 & v_1^1 & v_2^1 \\ u_0^1 & u_1^1 & u_2^1 \\ 0 & 0 & 1 \end{pmatrix},$$

which sends the line u^1 to the line $(0:1:0)$ and v^1 to the line $(1:0:0)$. Observe that this matrix is non-singular away from a strict subvariety of pairs $(R,T) \in E^2$. Indeed, it is easy to check that $v_0^1 u_1^1 - v_1^1 u_0^1$ is a non-zero rational function of R and T. Let $m(D_i) = (a_0^i : a_1^i : a_2^i)$, and $m^{(q)}(D_i + Q) = (b_0^i : b_1^i : b_2^i)$. We have $a_1^1 = a_1^3 = 0$ and $b_0^2 = b_0^4 = 0$. The matrix defining H (after applying the action of m) is

$$\begin{pmatrix} b_0^1 a_0^1 & 0 & b_0^1 a_2^1 & b_1^1 a_0^1 & 0 & b_1^1 a_2^1 & b_2^1 a_0^1 & 0 & b_2^1 a_2^1 \\ 0 & 0 & 0 & b_1^2 a_0^2 & b_1^2 a_1^2 & b_1^2 a_2^2 & b_2^2 a_0^2 & b_2^2 a_1^2 & b_2^2 a_2^2 \\ b_0^3 a_0^3 & 0 & b_0^3 a_2^3 & b_1^3 a_0^3 & 0 & b_1^3 a_2^3 & b_2^3 a_0^3 & 0 & b_2^3 a_2^3 \\ 0 & 0 & 0 & b_1^4 a_0^4 & b_1^4 a_1^4 & b_1^4 a_2^4 & b_2^4 a_0^4 & b_2^4 a_1^4 & b_2^4 a_2^4 \end{pmatrix},$$

From Lemma 5.11, apart from a strict subvariety of $(P_0, P_1) \in E_2$, one must have

$$\det \begin{pmatrix} b_0^1 a_0^1 & b_0^1 a_2^1 \\ b_0^3 a_0^3 & b_0^3 a_2^3 \end{pmatrix} \neq 0,$$

We deduce

$$D_{11} = b_1^2a_0^2 \times b_1^4a_1^4 - b_1^4a_0^4 \times b_1^2a_1^2 = b_1^2b_1^4(a_0^2a_1^4 - a_0^4a_1^2),$$
$$D_{12} = b_1^2a_0^2 \times b_1^4a_2^4 - b_1^4a_0^4 \times b_1^2a_2^2 = b_1^2b_1^4(a_0^2a_2^4 - a_0^4a_2^2),$$
$$D_{21} = b_1^2a_0^2 \times b_2^4a_1^4 - b_1^4a_0^4 \times b_2^2a_1^2.$$

Let us prove that D_{11} and D_{12} both have a pole of order $6q + O(1)$ at R (for almost all T), while D_{21} only has a pole of order $3q + O(1)$ (this implies that $D_{11}D_{12}^q - D_{11}^qD_{21}$ is a non-zero rational function of R and T). Only the b_i^j-values can contribute poles of order larger that $O(1)$, and more specifically, only the terms that have a $(u_i^j)^q$-factor (they have degree multiple of q, while other terms have degree $O(1)$). We have

$$b_1^j = (u_0^1)^{(q)} + (u_1^1)^{(q)}x(D_j + Q) + (u_2^1)^{(q)}y(D_j + Q),$$

and

$$u_0^1 = \det\begin{pmatrix} x(D_1) & y(D_1) \\ x(D_3) & y(D_3) \end{pmatrix} = \det\begin{pmatrix} x(R) & y(R) \\ x(T) & y(T) \end{pmatrix},$$

so it only remains to show that $a_0^2a_1^4 - a_0^4a_1^2$ and $a_0^2a_2^4 - a_0^4a_2^2$ are non-zero. We have

$$a_0^j = v_0^1 + v_1^1x(D_j) + v_2^1y(D_j),$$
$$a_1^j = u_0^1 + u_1^1x(D_j) + u_2^1y(D_j),$$
$$a_2^j = y(D_j).$$

Therefore,

$$\begin{aligned} a_0^2a_2^4 - a_0^4a_2^2 &= (v_0^1 + v_1^1x(D_2) + v_2^1y(D_2))y(D_4) - (v_0^1 + v_1^1x(D_4) + v_2^1y(D_4))y(D_2) \\ &= v_0^1(y(D_4) - y(D_2)) + v_1^1(x(D_2)y(D_4) - x(D_4)y(D_2)) \end{aligned}$$

Its terms with highest pole at D_4 are $y(D_4)(v_0^1 + v_1^1x(D_2))$, since $y(D_4)$ has a pole of degree 3 and $v_0^1 + v_1^1x(D_2)$ is a zero of degree at most $O(1/q)$ (unless $v_0^1 + v_1^1x(D_2)$ is itself the zero function, but it is the case only for finitely many D_2 since it has a pole of degree $2 + O(1/q)$ at D_2). So $a_0^2a_2^4 - a_0^4a_2^2$ is non-zero. Also,

$$\begin{aligned} a_0^2a_1^4 - a_0^4a_1^2 &= (v_0^1 + v_1^1x(D_2) + v_2^1y(D_2))(u_0^1 + u_1^1x(D_4) + u_2^1y(D_4)) \\ &\quad - (v_0^1 + v_1^1x(D_4) + v_2^1y(D_4))(u_0^1 + u_1^1x(D_2) + u_2^1y(D_2)) \\ &= v_0^1(u_1^1x(D_4) + u_2^1y(D_4)) + v_1^1x(D_2)(u_0^1 + u_2^1y(D_4)) + v_2^1y(D_2)(u_0^1 + u_1^1x(D_4)) \\ &\quad - v_0^1(u_1^1x(D_2) + u_2^1y(D_2)) - v_1^1x(D_4)(u_0^1 + u_2^1y(D_2)) - v_2^1y(D_4)(u_0^1 + u_1^1x(D_2)) \end{aligned}$$

The latter expression has the following terms with highest pole at D_4:

$$y(D_4)(v_0^1u_2^1 - v_2^1u_0^1 + x(D_2)(v_1^1u_2^1 - v_2^1u_1^1)).$$

Again this proves that $a_0^2a_1^4 - a_0^4a_1^2$ is a non-zero function of R and T, unless $v_0^1u_2^1 - v_2^1u_0^1 = v_1^1u_2^1 - v_2^1u_1^1 = 0$, which would imply that u^1 and v^1 are the same line, which happens for a strict subvariety of $(R, T) \in E^2$ (these correspond to traps $\mathscr{T}_4^2$ or $\mathscr{T}_4^3$). □

5.10. **Irreducibility of X_3.** We can now prove the main result of this section.

Proposition 5.15. *For any divisor $D \in (\mathscr{D}_4 \setminus \mathscr{T}_4)(k)$, the curve X_3 contains an absolutely irreducible component defined over k.*

Proof. We have shown that $\theta : X_1 \to X_0$ satisfies all the conditions of Proposition 4.2, so the result follows. □

6. Avoiding traps

Paradoxically, to avoid traps, we need to add more traps. Originally, a divisor is a trap if it cannot be eliminated into smaller degree divisors. These are traps of level 0. Now, we want to call a divisor a trap also if it can be eliminated, but only into divisors that are themselves traps. We call these traps of level 1, and so on. For a rigorous definition, let $x_0 = 1$, $x_1 = x$ and $x_2 = y$ in $k[E]$, and for $n = 2$ or 3 let $V_n = \mathrm{span}(x_i x_j^q \mid i, j < n)$ and $\Lambda_n = \mathrm{span}(x_i \mid i < n)$. Recall that the 4–to–3 elimination arises from the relation $\varphi(f) \equiv \psi(f) \mod \mathscr{I}$ for any $f \in V_4$. Indeed, when f splits as a product of linear factors $f = \prod_{i=1}^{q+1} L_i$, and applying the norm and the logarithm maps, we deduce

$$\sum_{i=1}^{q+1} \log(N_{k/\mathbf{F}_q}(L_i)) = \mathrm{Log}(N_{k/\mathbf{F}_q}(D)) + \mathrm{Log}(N_{k/\mathbf{F}_q}(D')) - 3 \cdot [k : \mathbf{F}_q] \cdot \mathrm{Log}([Q]),$$

for some divisor D' of degree 2. The sum on the left is referred to as the *left-hand side* of the elimination, and the terms on the right are the *right-hand side* of the elimination. Similarly, for the 3–to–2 elimination, we get relations of the form

$$\sum_{i=1}^{q+1} \log(N_{k/\mathbf{F}_q}(L_i \circ \tau_P)) = \mathrm{Log}(N_{k/\mathbf{F}_q}(D)) + \mathrm{Log}(N_{k/\mathbf{F}_q}([P'])) \\ - 2 \cdot \mathrm{Log}(N_{k/\mathbf{F}_q}([-P])) - 2 \cdot \mathrm{Log}(N_{k/\mathbf{F}_q}([-Q - P^{(q)}])),$$

and the sum on the left is the *left-hand side* of the elimination, and the terms on the right are the *right-hand side* of the elimination.

Consider the morphisms

$$\delta' : \mathbf{P}(V_3) \times \mathbf{P}(\Lambda_3) \longrightarrow \mathscr{D}_3 : (f, u) \longmapsto \mathrm{div}(u) + 3[0_E],$$

$$\delta_i : \mathbf{P}(V_2) \times \mathbf{P}(\Lambda_2) \times E \longrightarrow \mathscr{D}_4 : (f, u, P) \longmapsto \mathrm{div}(u \circ \tau_P) + \mathrm{div}\left((u \circ \tau_P)^{\left(q^{2^{i-1}}\right)}\right) + 4[0_E].$$

The intuition behind these morphisms is the following. Given any degree 4 divisor D, the corresponding X_1 is a curve in $\mathbf{P}(V_3) \times \mathbf{P}(\Lambda_3)$. Suppose $f \in X_0$ splits as a product of linear polynomials $f = \prod_{i=1}^{q+1} L_i$. For any such f, the preimages of f in X_1 are the points (f, L_i), and we have $\delta'(f, L_i) = \mathrm{div}(L_i) + 3[0_E]$. Therefore, $\delta'(X_1)$ contains all the degree 3 divisors susceptible to appear on the left-hand side of the elimination, i.e., the $\sum_{i=1}^{q+1} \log(N_{k/\mathbf{F}_q}(L_i))$ part of the elimination. In particular, we wish to show that $\delta'(X_1)$ does not consist only of traps. Similarly, δ_i allows to capture the divisors susceptible to appear on the left-hand side of the 3–to–2 elimination.

Consider the natural morphisms $\pi_3 : E^3 \to \mathscr{D}_3$ and $\pi_4 : E^4 \to \mathscr{D}_4$. For any $i \geq 0$, let $T_3(i, 0) = \pi^{-1}(\mathscr{T}_3)$ and $T_4(i, 0) = \pi^{-1}(\mathscr{T}_4)$. For any $i > 0$, let $T_3(i, 1)$ be the set of pairs $(P_1, P_2) \in E^2$ such that

$$\left(P_1, P_2, P_1^{\left(q^{2^{i-1}}\right)}, P_2^{\left(q^{2^{i-1}}\right)}\right) \in T_4(i-1, 0) \subset E^4,$$

and for any $i > 0$, let $T_4(i, 1)$ be the set of pairs $(P_1, P_2) \in E^2$ such that

$$(P_1, P_2, -P_1 - P_2) \in T_3(i, 0) \subset E^3,$$

For any $1 < j \leq 2i - 1$ define $T_3(i, j) = T_4(i - 1, j - 1) \subset E^2$, and for any $1 < j \leq 2i$ define $T_4(i, j) = T_3(i, j - 1) \subset E^2$. Now, for every i, let

$$T_3(i) = \bigcup_{j=1}^{2i-1} T_3(i, j), \text{ and } T_4(i) = \bigcup_{j=1}^{2i} T_4(i, j).$$

Finally, we can define traps at level i as

$$\mathscr{T}_3(i) = \mathscr{T}_3 \cup \left\{ \sum_{k=1}^{3} [P_k] \;\middle|\; \forall k \neq \ell, (P_k, P_\ell) \in T_3(i) \right\},$$
$$\mathscr{T}_4(i) = \mathscr{T}_4 \cup \left\{ \sum_{k=1}^{4} [P_k] \;\middle|\; \forall k \neq \ell, (P_k, P_\ell) \in T_4(i) \right\}.$$

The following proposition suggests this is the correct notion of traps: if a divisor is not a trap at a certain level, then its eliminations do not all lead to traps at the level below (at least on the left-hand side). Given a divisor D of degree 3 (respectively, of degree 4), we write $X_1(D)$ for the corresponding curve X_1 as defined in Section 4.1 (respectively, in Section 5).

Proposition 6.1. *For any $i > 0$,*

(1) *if $D \in \mathscr{D}_4$ and $D \notin \mathscr{T}_4(i)$, then $\delta'(X_1(D)) \not\subset \mathscr{T}_3(i)$, and*
(2) *if $D \in \mathscr{D}_3$ and $D \notin \mathscr{T}_3(i)$, then $\delta_i(X_1(D)) \not\subset \mathscr{T}_4(i-1)$.*

Proof. Suppose $D \notin \mathscr{T}_4(i)$. So there is a pair (P_1, P_2) dividing D such that $(P_1, P_2) \notin T_4(i)$. In particular, $(P_1, P_2) \notin T_4(i, 1)$ so $[P_1] + [P_2] + [-P_1 - P_2] \notin \mathscr{T}_3$. Also, for any $1 < j \leq 2i$, we have $(P_1, P_2) \notin T_4(i, j) = T_3(i, j-1)$ so $(P_1, P_2) \notin T_3(i)$. Therefore,

$$[P_1] + [P_2] + [-P_1 - P_2] \in \delta'(X_1(D)) \setminus \mathscr{T}_3(i),$$

proving that $\delta'(X_1(D)) \not\subset \mathscr{T}_3(i)$. The second point is proved in the same way. □

6.1. **Degree of trap subvarieties.** Let $n \in \{3, 4\}$. Embedding E in $\mathbf{P}^2$, we can naturally see E^n as a projective variety in $\left(\mathbf{P}^2\right)^n$. When referring to the degree of a subvariety of E^n, we refer to its degree through the Segre embedding. Alternatively, we could consider its degree in the projectivization of the affine patch $\mathbf{A}^{2n}$, and as long as the variety properly intersects the hyperplane at infinity, these two notions of degree differ by a factor $O(1)$.

The variety $\mathscr{D}_n$ can be seen as a subvariety of $\mathbf{P}\left(S^n(\mathbf{A}^3)\right) \cong \mathbf{P}^{\binom{n+2}{2}-1}$, where $S^n(\mathbf{A}^3)$ is the affine n-th symmetric power of $\mathbf{A}^3$. Each morphism $\pi_n : E^n \to \mathscr{D}_n$ is the restriction of the natural morphism $\left(\mathbf{P}^2\right)^n \to \mathbf{P}\left(S^n(\mathbf{A}^3)\right)$. We refer to the embedding $\mathscr{D}_n \subset \mathbf{P}^{\binom{n+2}{2}-1}$ when discussing the degree of a subvariety of $\mathscr{D}_n$. An important observation is that for any variety $\mathscr{A} \subset E^n$, the degree of $\mathscr{A}$ differs from the degree of $\pi_n(\mathscr{A}) \subset \mathscr{D}_n$ by a factor $O(1)$. It is easy to see that with this notion of degree, we have $\deg(\mathscr{T}_3) = q^{O(1)}$ and $\deg(\mathscr{T}_4) = q^{O(1)}$.

Lemma 6.2. *For $i > 0$ and any $j > 0$,*

$$\begin{aligned} T_3(i, 2j) &= T_4(i - j, 1), \\ T_3(i, 2j+1) &= T_3(i - j, 1), \\ T_4(i, 2j) &= T_3(i - j + 1, 1), \\ T_4(i, 2j+1) &= T_4(i - j, 1). \end{aligned}$$

Proof. These identities easily follow from the recursive definitions of $T_3(i, j)$ and $T_4(i, j)$. □

Lemma 6.3. *For $i > O(1)$, we have*[2] $\deg(T_4(i, 1)) = q^{O(1)}$ *and* $\deg(T_3(i, 1)) = q^{2^{i-1}+O(1)}$.

Proof. The fact that $\deg(T_4(i, 1)) = q^{O(1)}$ follows from $\deg(\mathscr{T}_3) = q^{O(1)}$, which easily follows from the definition of $\mathscr{T}_3$. For $T_3(i, 1)$, let $f_j(P_1, P_2, P_3, P_4)$ be the equations defining $\pi^{-1}(\mathscr{T}_4) \subset E^4$. By construction of $\mathscr{T}_4$, each of them has degree $q^{O(1)}$. Choosing any of these equations (at least a non-trivial one), say f_1, we have,

$$T_3(i, 1) \subset \left\{ (P_1, P_2) \;\middle|\; f_1\left(P_1, P_2, P_1^{\left(q^{2^{i-1}}\right)}, P_2^{\left(q^{2^{i-1}}\right)}\right) = 0 \right\} \subset E^2.$$

[2]Here and in the rest of the article, when we write that some statement holds "for $i > O(1)$", we mean that there exists a constant c such that it holds for any $i > c$.

There is a constant c such that for all $i > c$, the equation

$$f_1\left(P_1, P_2, P_1^{\left(q^{2^{i-1}}\right)}, P_2^{\left(q^{2^{i-1}}\right)}\right) = 0$$

is non-trivial. This equation has degree $q^{2^{i-1}+O(1)}$, and so does $T_3(i,1)$. □

Corollary 6.4. *For any $i > O(1)$, we have $\deg(\mathscr{T}_3(i)) = q^{2^{i-1}+O(1)}$ and $\deg(\mathscr{T}_4(i)) = q^{2^{i-1}+O(1)}$.*

Proof. From Lemmata 6.2 and 6.3, we deduce that for any $i > 0$ and $j > 0$,

$$\begin{aligned}
\deg(T_3(i,2j)) &= q^{O(1)},\\
\deg(T_4(i,2j)) &= q^{2^{i-j}+O(1)},\\
\deg(T_3(i,2j-1)) &= q^{2^{i-j}+O(1)},\\
\deg(T_4(i,2j-1)) &= q^{O(1)}.
\end{aligned}$$

The result follows from the definitions of $\mathscr{T}_3(i)$ and $\mathscr{T}_4(i)$. □

6.2. **Degree 3–to–2 elimination.** The following proposition allows to avoid traps appearing on the left-hand side during the 3–to–2 elimination.

Proposition 6.5. *For any $i > 0$, if $D \in \mathscr{D}_3$ and $D \notin \mathscr{T}_3(i)$, then*

$$|(\delta_i(X_1(D)) \cap \mathscr{T}_4(i-1))(\mathbf{F}_{q^{2^{i-1}}})| \leq q^{\frac{3}{2}\cdot 2^{i-1}+O(1)}.$$

Proof. Since $D \notin \mathscr{T}_3(i)$, $\delta_i(X_1(D)) \not\subset \mathscr{T}_4(i-1)$. Also, $\deg(\delta_i(X_1(D))) = q^{2^{i-1}+O(1)}$ and $\deg(\mathscr{T}_4(i-1)) = q^{2^{i-2}+O(1)}$. Applying Bézout's theorem,

$$|\delta_i(X_1(D)) \cap \mathscr{T}_4(i-1)| \leq \deg(\delta_i(X_1(D))) \cdot \deg(\mathscr{T}_4(i-1)) = q^{2^{i-1}+2^{i-2}+O(1)},$$

which proves the proposition. □

Proposition 6.6 (Degree 3–to–2 elimination)**.** *Consider the field $k = \mathbf{F}_{q^{2^i}}$ and a divisor $D \in (\mathscr{D}_3 \setminus \mathscr{T}_3(i))(k)$. For $i \geq O(1)$, there is a probabilistic algorithm that finds a list $(D_j)_{j=1}^{q+1}$ of effective divisors of degree 2 over k, three divisors D'_1, D'_2, D'_3 of degree 1 over k and, integers $\alpha_1, \alpha_2, \alpha_3$ such that*

$$\mathrm{Log}(N_{k/\mathbf{F}_q}(D)) = \sum_{j=1}^{q+1} \log(N_{k/\mathbf{F}_q}(D_j)) + \sum_{i=1}^{3} \alpha_i \cdot \log(N_{\mathbf{F}_{q^{2^{i-1}}}/\mathbf{F}_q}(D'_j)),$$

in expected time polynomial in q and 2^i. Furthermore, it ensures that

1. *for any D_j, we have $N_{k/\mathbf{F}_{q^{2^{i-1}}}}(D_j) \notin \mathscr{T}_4(i-1)$, and*
2. *for any D'_j, we have $N_{k/\mathbf{F}_{q^{2^{i-2}}}}(D'_j) \notin \mathscr{T}_4(i-2)$.*

Proof. Consider an affine patch A of the ambient space (which intersects all the components of X_3), and the corresponding restriction $\widetilde{X}_3 \subset A$. We have $\deg(\widetilde{X}_3) = q^{O(1)}$. From Proposition 4.8 and [Bac96, Theorem 3.1], we have

$$\left|\widetilde{X}_3(k)\right| \geq q^{2^i} - q^{2^{i-1}+O(1)}.$$

The algorithm simply consists in generating random points of $\widetilde{X}_3(k)$, which can be done in polynomial time since the degree of the curve is polynomial in q. Each $(f, P, u_1, u_2, u_3) \in \widetilde{X}_3(k)$ gives a possible elimination, as described in Section 3.3. It only remains to prove that with high probability, no trap appears in the elimination.

Fix a linear factor u, and consider the subvariety H_u of A parameterising polynomials of which u is a factor. One cannot have $\widetilde{X}_3 \subset H_u$ (or D would be in $\mathscr{T}_3^0$), so $\widetilde{X}_3 \cap H_u$ contains at most $(q-1)\deg(\widetilde{X}_3)$ points (let H'_u be the (degree 1) subspace of A where $u = u_1$; each point (f, P, u, u_2, u_3) in $\widetilde{X}_3 \cap H'_u$ gives $q-1$ points in $\widetilde{X}_3 \cap H'_u$ simply by choosing u_1 to be any of the linear factors of f other than u_2 and u_3). Similarly, any divisor coprime to D appears in

at most $q^{O(1)}$ of the functions $\varphi_P(f)$, for $(f, P, u, v, w) \in X_3$, by looking at the hyperplanes $H_P = \mathbf{P}(V) \times \{P\} \times (\mathbf{P}^1)^3$ for $P \in E$.

Each element on $X_3(k)$ gives a relation where the right-hand side is a divisor of the form $D + [P_0] - 2[P_1] - 2[P_2]$ for some points $P_\ell \in E(\mathbf{F}_{q^{2^i}})$. Let $\ell \in \{0, 1, 2\}$. Ranging over all rational points $X_3(k)$, the point P_ℓ takes $q^{2^i+O(1)}$ distinct values. Any such point can be descended to $N_{k/\mathbf{F}_{q^{2^{i-2}}}}([P_\ell]) \in \mathscr{D}_4(\mathbf{F}_{q^{2^{i-2}}})$. Applying [Bac96, Theorem 3.1], there are only $q^{3\cdot 2^{i-2}+2^{i-3}+O(1)}$ such divisors that are traps.

Now, let us look at traps that could appear on the left-hand side. The degree 4 divisors that can appear on the left-hand side are $\delta_i(X_1(D))$. Since $D \notin \mathscr{T}_3(i)$, Proposition 6.5 implies that $|(\delta_i(X_1(D)) \cap \mathscr{T}_4(i-1))(\mathbf{F}_{q^{2^{i-1}}})| \leq q^{3\cdot 2^{i-2}+O(1)}$. Therefore, at most $q^{3\cdot 2^{i-2}+O(1)}$ points of $X_3(k)$ give rise to a trap on the left-hand side.

Finally, if $G \subset \widetilde{X}_3(k)$ is the subset of points giving an elimination that does not involve traps on either side, we get

$$\left|\widetilde{X}_3(k) \setminus G\right| \leq q^{3\cdot 2^{i-2}+2^{i-3}+O(1)} + q^{3\cdot 2^{i-2}+O(1)} = q^{\frac{7}{8}\cdot 2^i+O(1)}.$$

Therefore, for $i \geq O(1)$, more than half the points of $X_3(k)$ are in G, so choosing uniformly random points in $X_3(k)$, the elimination succeeds in expected polynomial time in q and 2^i. □

6.3. **Degree 4–to–3 elimination.** The following proposition allows to avoid traps appearing on the left-hand side during the 4–to–3 elimination.

Proposition 6.7. *For any $i > O(1)$, if $D \notin \mathscr{T}_4(i)$, then $|(\delta'(X_1(D)) \cap \mathscr{T}_3(i))(\mathbf{F}_{q^{2^i}})| \leq q^{2^{i-1}+O(1)}$.*

Proof. Since $D \notin \mathscr{T}_4(i)$, $\delta'(X_1(D)) \not\subset \mathscr{T}_3(i)$, so $\dim(\delta'(X_1(D)) \cap \mathscr{T}_3(i)) = 0$. Now, $\deg(\delta'(X_1(D))) = q^{O(1)}$ and $\deg(\mathscr{T}_3(i)) = q^{2^{i-1}+O(1)}$. Applying Bézout's theorem,

$$|(\delta'(X_1(D)) \cap \mathscr{T}_3(i))(\mathbf{F}_{q^{2^i}})| \leq \deg(\delta'(X_1(D))) \deg(\mathscr{T}_3(i)) = q^{2^{i-1}+O(1)}.$$

□

The following results allow to avoid traps on the right-hand side during the 4–to–3 elimination.

Lemma 6.8. *For any $S, R \in E$ such that $S^{(q)} \notin \{S - Q, S + 2Q\}$, we have $\mathscr{P}_2(S) + \mathscr{P}_2(R) \not\subset \mathscr{T}_4$ and $\mathscr{P}_2(S) + [-S] \not\subset \mathscr{T}_3$.*

Proof. This is simply a summary of Lemmata 4.3, 5.1 and 5.14. □

Lemma 6.9. *As long as the order of Q is not a power of two (which can be enforced), there is no $S \in E(\mathbf{F}_{q^{2^i}})$ such that $S^{(q)} \in \{S - Q, S + 2Q\}$.*

Proof. Suppose $S^{(q)} = S + jQ$ for $j \in \{-1, 2\}$. Then, for any integer r, $S^{(q^r)} = S + rjQ$. The smallest r such that $S^{(q^r)} = S$ is the order of jQ, which not a power of two. So S cannot be defined over a power-of-two degree extension of $\mathbf{F}_q$, i.e., it cannot be defined over a field $\mathbf{F}_{q^{2^i}}$. □

For any positive integer i and any $P \in E$, let $\mathscr{B}_i(S) = \left\{ F + F^{\left(q^{2^i}\right)} \;\middle|\; F \in \mathscr{P}_2(S) \right\}$.

Lemma 6.10. *Let $S \in E(\mathbf{F}_{q^{2^{i+1}}})$. For any $i \geq O(1)$, we have that $\mathscr{B}_i(S) \not\subset \mathscr{T}_4$.*

Proof. We show that for any $i \geq O(1)$, there exists $D \in \mathscr{P}_2(S)$ such that $D + D^{\left(q^{2^i}\right)} \notin \mathscr{T}_4$. Let $\mathscr{A} = \left(\mathscr{P}_2(S) + \mathscr{P}_2\left(S^{\left(q^{2^i}\right)}\right)\right) \cap \mathscr{T}_4$. Since $\mathscr{P}_2(S) + \mathscr{P}_2\left(S^{\left(q^{2^i}\right)}\right)$ is an absolutely irreducible surface and is not contained in $\mathscr{T}_4$, the intersection $\mathscr{A}$ is a curve. We have

$$|\mathscr{A}(\mathbf{F}_{q^{2^i}})| \leq c(\mathscr{A})(q^{2^i} + 1 + \deg(\mathscr{A})^2 q^{2^{i-1}}) \leq q^{2^i+O(1)},$$

where $c(\mathscr{A})$ is the number of absolutely irreducible components of $\mathscr{A}$. On the other hand, observe that through the morphism $\mathscr{P}_2(S) \to \mathscr{B}_i(S)$, each point has at most 4 preimages, so

$$|\mathscr{B}_i(S)(\mathbf{F}_{q^{2^i}})| \geq |\mathscr{P}_2(S)(\mathbf{F}_{q^{2^{i+1}}})|/4 = q^{2^{i+1}+O(1)}.$$

Therefore $\mathscr{B}_i(S) \not\subset \mathscr{A}$. Since $\mathscr{B}_i(S) \cap \mathscr{T}_4 \subset \mathscr{A}$, we deduce $\mathscr{B}_i(S) \not\subset \mathscr{T}_4$. □

Lemma 6.11. *Let $S \in E(\mathbf{F}_{q^{2^i}})$. For any $i > O(1)$, and $j > 0$, we have $\mathscr{P}_2(S) \not\subset T_3(i,j)$.*

Proof. From Lemma 6.2, it suffices to prove that $\mathscr{P}_2(S) \not\subset T_4(i,1)$ and $\mathscr{P}_2(S) \not\subset T_3(i,1)$ for any $i > 0$. Since $\mathscr{P}_2(S) + [-S] \not\subset \mathscr{T}_3$, there is a divisor $D \in \mathscr{P}_2(S)$ such that $D + [-S] \notin \mathscr{T}_3$ which by definition implies that $D \notin T_4(i,1)$. Also, from Lemma 6.10, we have $\mathscr{B}_{i-1}(S) \not\subset \mathscr{T}_4$ so there exists $D \in \mathscr{P}_2(S)$ such that $D + D^{\left(q^{2^{i-1}}\right)} \notin \mathscr{T}_4$, which implies that $D \notin T_3(i,1)$. □

Lemma 6.12. *Let $S \in E(\mathbf{F}_{q^{2^{i+1}}})$. For any $i \geq O(1)$, we have that $\mathscr{B}_i(S) \not\subset \mathscr{T}_4(i)$.*

Proof. Recall that $\mathscr{T}_4(i) = \bigcup_{j=0}^{2i} \mathscr{T}_4(i,j)$. From Lemma 6.10, $\mathscr{B}_i(S) \not\subset \mathscr{T}_4(i,0)$. From Lemma 6.11, $\mathscr{B}_i(S) \not\subset \mathscr{T}_4(i,j)$. We conclude from the absolutely irreducible of $\mathscr{B}_i(S)$ (it is an image of $\mathscr{P}_2(S)$). □

Proposition 6.13. *Let $S \in E(\mathbf{F}_{q^{2^{i+1}}})$. For any $i \geq O(1)$, $|\mathscr{B}_i(S) \cap \mathscr{T}_4(i)| \leq q^{\frac{3}{2}2^i + O(1)}$.*

Proof. From Lemma 6.12, we have $\mathscr{B}_i(S) \not\subset \mathscr{T}_4(i)$, therefore $\dim(\mathscr{B}_i(S) \cap \mathscr{T}_4(i)) < \dim(\mathscr{B}_i(S)) = 1$. Therefore, from Bézout's theorem,

$$|\mathscr{B}_i(S) \cap \mathscr{T}_4(i)| \leq \deg(\mathscr{B}_i(S)) \deg(\mathscr{T}_4(i)) = q^{2^i + 2^{i-1} + O(1)} = q^{\frac{3}{2}2^i + O(1)}.$$

□

Proposition 6.14 (Degree 4–to–3 elimination)**.** *Consider the field $k = \mathbf{F}_{q^{2^i}}$ and a divisor $D \in (\mathscr{D}_4 \setminus \mathscr{T}_4(i))(k)$. For $i \geq O(1)$, there is a probabilistic algorithm that finds a list $(D_j)_{j=1}^{q+1}$ of effective divisors of degree 3 over k, and one effective divisor D' of degree 2 over k such that*

$$\mathrm{Log}(N_{k/\mathbf{F}_q}(D)) = \sum_{j=1}^{q+1} \mathrm{Log}(N_{k/\mathbf{F}_q}(D_j)) - \mathrm{Log}(N_{k/\mathbf{F}_q}(D')) + 3 \cdot 2^i \cdot \mathrm{Log}([Q]),$$

and runs in expected time polynomial in q and 2^i. Furthermore, it ensures that $D_i \notin \mathscr{T}_3(i)$ for each index i, and $N_{k/\mathbf{F}_{q^{2^{i-1}}}}(D') \notin \mathscr{T}_4(i-1)$.

Proof. This proof is similar to the proof of Proposition 6.6. We consider an affine patch A of the ambient space, and the corresponding $\widetilde{X}_3$, and we have $\deg(\widetilde{X}_3) = q^{O(1)}$. From Proposition 5.15 and [Bac96, Theorem 3.1], we have

$$\left|\widetilde{X}_3(k)\right| \geq q^{2^i} - q^{2^{i-1}+O(1)}.$$

As in the 3–to–2 case, the algorithm consists in generating random points of $\widetilde{X}_3(k)$. Each $(f, u_1, u_2, u_3) \in \widetilde{X}_3(k)$ gives a possible elimination, as described in Section 3.3, and it remains to prove that with high probability, no trap appears in the elimination.

Fix a linear factor u, and consider the subvariety H_u of A parameterising polynomials of which it is a factor. Either $\widetilde{X}_3 \subset H_u$, a trap, or $\widetilde{X}_3 \cap H_u$ contains at most $(q-1)\deg(\widetilde{X}_3)$ points (let H'_u be the (degree 1) subspace of A where $u = u_1$; each point (f, u, u_2, u_3) in $\widetilde{X}_3 \cap H'_u$ gives $q-1$ points in $\widetilde{X}_3 \cap H'_u$ simply by choosing u_1 to be any of the linear factors of f other than u_2 and u_3). Similarly, any divisor coprime to D appears in at most $\deg(\widetilde{X}_3)$ of the functions $\varphi(f)$, for $(f, u, v, w) \in \widetilde{X}_3$.

Each element on X_3 gives a relation where the right-hand side is a divisor of the form

$$D + D' - 3[0_E] - 3[-Q]$$

for $D' \in \mathscr{P}_2(-\sigma D - 3Q)$, where σD is the sum of the points of D. Proposition 6.13 implies that at most $q^{\frac{3}{2}2^{i-1}+O(1)}$ such divisors D' give rise to a trap at level $i-1$. So at most $dq^{\frac{3}{2}2^{i-1}+O(1)} = q^{\frac{3}{2}2^{i-1}+O(1)}$ points of X_3 give rise to a trap on the right-hand side.

Now, let us look at traps that could appear on the left-hand side. The degree 3 divisors that can appear on the left-hand side are $\delta'(X_1(D))$ Since $D = F + F^{\left(q^{2^i}\right)}$ for some $F \in \mathscr{D}_2$ and

$D \notin \mathscr{T}_4(i)$, Proposition 6.7 implies that $|(\delta'(X_1(D)) \cap \mathscr{T}_3(i))(\mathbf{F}_{q^{2^i}})| \leq q^{2^{i-1}+O(1)}$. Therefore, at most $q^{2^{i-1}+O(1)}$ points of X_3 give rise to a trap on the left-hand side.

Finally, if $G \subset \widetilde{X}_3(k)$ is the subset of points giving an elimination that does not involve traps on either side, we get

$$\left|\widetilde{X}_3(k) \setminus G\right| \leq q^{3\cdot 2^{i-2}+O(1)} + q^{2^{i-1}+O(1)} = q^{\frac{3}{4}\cdot 2^i+O(1)}.$$

Therefore, for $i \geq O(1)$, more than half the points of $X_3(k)$ are in G, so choosing uniformly random points in $X_3(k)$, the elimination succeeds in expected polynomial time in q and 2^i.

□

7. Proof of the main theorem

Lemma 7.1. *Given a polynomial $F \in \mathbf{F}_q[E]$, there is a probabilistic polynomial-time algorithm that finds an irreducible polynomial $G \in \mathbf{F}_q[E]$ of degree 2^{e+2} such that $G \equiv F \mod \mathscr{I}$, for some integer $e = \log_2(n) + O(1)$. Furthermore, $G = N_{\mathbf{F}_{q^{2^e}}/\mathbf{F}_q}(D)$ for some irreducible divisor $D \in (\mathscr{D}_4 \setminus \mathscr{T}_4(e))(\mathbf{F}_{q^{2^e}})$.*

Proof. This is an application of the Chebotarev density theorem for function fields. Let $H(\mathscr{I})$ be the ray class field modulo $\mathscr{I}$ of $\mathbf{F}_q(E)$, and $\varphi : \mathrm{Cl}_{\mathscr{I}} \to \mathrm{Gal}(H(\mathscr{I})/\mathbf{F}_q(E))$ the Artin map from the ray class group. Recall that $\mathrm{Cl}_{\mathscr{I}} = D(\mathscr{I})/P(\mathscr{I})$ where $D(\mathscr{I})$ is the group of fractional ideals of $\mathbf{F}_q[E]$ coprime to $\mathscr{I}$ and $P(\mathscr{I})$ is the subgroup of principal ideals generated by elements $f \in \mathbf{F}_q[E]$ such that $\mathscr{I} \mid \mathrm{div}(f-1)$. From [Sal06, p. 520], φ is an isomorphism.

Let $e > \log_2(n) - 1$ be an integer, and pick a uniformly random function $f \in \mathbf{F}_q[E]$ of degree 2^{e+2} such that $\mathscr{I} \mid \mathrm{div}(f)$. Let $G = F + f$. Then, $G \equiv F \mod \mathscr{I}$, and G is uniformly distributed among the functions of degree 2^{e+2} in the $\mathscr{I}$-ray class of F. Recall that $n = \deg(\mathscr{I})$ and $N = \#E(\mathbf{F}_q)$. Let $S_{\mathbf{F}_q}(E, \mathscr{I})$ be the set of irreducible divisors of E other than $\mathscr{I}$, defined over $\mathbf{F}_q$. Applying the Chebotarev density theorem [Ros13, Theorem 9.13B] to $H(\mathscr{I})/\mathbf{F}_q(E)$, we get that for any $d > 0$,

$$\#\{P \in S_{\mathbf{F}_q}(E, \mathscr{I}) \mid \deg(P) = d, [P]_{\mathscr{I}} = [F]_{\mathscr{I}}\} = \frac{1}{\#\,\mathrm{Cl}_{\mathscr{I}}}\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right).$$

Let $d = 2^{e+2}$. Since $\#\,\mathrm{Cl}_{\mathscr{I}} = N(q^n-1)/(q-1)$, we get

$$\#\{P \in S_{\mathbf{F}_q}(E, \mathscr{I}) \mid \deg(P) = d, [P]_{\mathscr{I}} = [F]_{\mathscr{I}}\} = \frac{q^{2^{e+2}-n+O(1)}}{2^{e+2}}.$$

On the other hand, applying [Bac96, Theorem 3.1], we have $|\mathscr{T}_4(e)(\mathbf{F}_{q^{2^e}})| = q^{3\cdot 2^e+O(1)}$. So for $e = \log_2(n) + O(1)$, the random prime divisor G is not a trap with overwhelming probability. □

Let $c = O(1)$ be the smallest integer such that both degree 4–to–3 and 3–to–2 eliminations from Propositions 6.14 and Propositions 6.6 are guaranteed to work for $i > c$. Let

$$\widetilde{\mathfrak{F}} = \{N_{\mathbf{F}_{q^{2^c}}/\mathbf{F}_q}(D) \mid D \in \mathrm{Div}_k(E, \mathscr{I}), D > 0, \deg(D) \leq 2\}.$$

The factor base for the descent algorithm is defined as

$$\mathfrak{F} = \{f \in \mathbf{F}_q[E] \mid \exists D \in \widetilde{\mathfrak{F}} \text{ such that } \mathrm{div}(f) = ND\}.$$

Proposition 7.2 (Zigzag descent)**.** *Given a polynomial $F \in \mathbf{F}_q[E]$, there is a probabilistic algorithm that finds integers $(\alpha_f)_{f\in\mathfrak{F}}$ such that*

$$\log(F) = \sum_{f\in\mathfrak{F}} \alpha_f \cdot \log(f),$$

and that runs in expected time $q^{2\log_2(n)+O(1)}$.

Proof. First apply Lemma 7.1 to find an irreducible polynomial G in $\mathbf{F}_q[E]$ of degree 2^{e+2} such that $G \equiv F \mod \mathscr{I}$, and such that $\log(G) = \mathrm{Log}(N_{\mathbf{F}_{q^{2^e}}/\mathbf{F}_q}(D))$ for some irreducible divisor $D \in (\mathscr{D}_4 \setminus \mathscr{T}_4(e))(\mathbf{F}_{q^{2^e}})$. Applying the degree 4–to–3 elimination (Proposition 6.14), there is a list

$(D_i)_{i=1}^{q+1}$ of effective divisors of degree 3 over $\mathbf{F}_{q^{2^e}}$ and an effective divisor D' of degree 2 over $\mathbf{F}_{q^{2^e}}$ such that

$$\mathrm{Log}(N_{\mathbf{F}_{q^{2^e}}/\mathbf{F}_q}(D)) = \sum_{i=1}^{q+1} \mathrm{Log}(N_{\mathbf{F}_{q^{2^e}}/\mathbf{F}_q}(D_i)) - \mathrm{Log}(N_{\mathbf{F}_{q^{2^e}}/\mathbf{F}_q}(D')) + 3 \cdot 2^e \cdot \mathrm{Log}([Q]).$$

Since $D_i \in \mathscr{D}_3 \setminus \mathscr{T}_3(e)$, one can apply the degree 3–to–2 elimination (Proposition 6.6), rewriting each of them as combinations of smaller degree polynomials. At this stage, the quantity $\mathrm{Log}(N_{\mathbf{F}_{q^{2^e}}/\mathbf{F}_q}(D))$ is expressed as a product of $O(q^2)$ terms involving divisors of degree 1 or 2 over $\mathbf{F}_{q^{2^e}}$. They give irreducible divisors of degree 4 by considering the norm to $\mathbf{F}_{q^{2^{e-1}}}$ or $\mathbf{F}_{q^{2^{e-2}}}$ (and these divisors do not belong to $\mathscr{T}_4(e-1)$ or $\mathscr{T}_4(e-2)$ respectively), hence one can recursively apply the degree 4–to–3 and 3–to–2 eliminations, until all the resulting divisors are in the set $\widetilde{\mathfrak{F}}$. We obtain a linear combination of logarithms of factor base elements via the fact that for any $D \in \widetilde{\mathfrak{F}}$, we have $\mathrm{Log}(D) = \log(f)/N$, where f is any function such that $\mathrm{div}(f) = ND$. □

7.1. **Proof of the main theorem.** Theorem 1.1 follows immediately from Theorem 3.1, Theorem 2.4, and Proposition 7.2.

8. Acknowledgements

The authors wish to thank Zsolt Patakfalvi for discussions that led to the proof of Proposition 5.9, and Arjen K. Lenstra for valuable comments that helped improve the quality of this manuscript. Part of this work was supported by the Swiss National Science Foundation under grant number 200021-156420, and by the ERC Advanced Investigator Grant 740972 (ALGSTRONGCRYPTO).

References

[Bac96] Eric Bach. Weil bounds for singular curves. *Applicable Algebra in Engineering, Communication and Computing*, 7(4):289–298, 1996.

[BGJT14] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 2014.

[Die11] Claus Diem. On the discrete logarithm problem in elliptic curves. *Compositio Mathematica*, 147(1):75–104, 2011.

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

[Ful13] William Fulton. *Intersection theory*, volume 2. Springer Science & Business Media, 2013.

[GKZ18] Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. On the discrete logarithm problem in finite fields of fixed characteristic. *Transactions of the American Mathematical Society*, 270(5):3129–3145, 2018.

[KW18] Thorsten Kleinjung and Benjamin Wesolowski. A new perspective on the powers of two descent for discrete logarithms in finite fields. In *Thirteenth Algorithmic Number Theory Symposium – ANTS-XIII*, 2018. proceedings to appear in the Open Book Series, Mathematical Sciences Publishers.

[Mic19] Giacomo Micheli. On the selection of polynomials for the DLP quasi-polynomial time algorithm for finite fields of small characteristic. *SIAM Journal on Applied Algebra and Geometry*, 3(2):256–265, 2019.

[Pom87] Carl Pomerance. Fast, rigorous factorization and discrete logarithm algorithms. In David S. Johnson, Takao Nishizeki, Akihiro Nozaki, and Herbert S. Wilf, editors, *Discrete Algorithms and Complexity*, pages 119–143. Academic Press, 1987.

[Ros13] Michael Rosen. *Number theory in function fields*, volume 210. Springer Science & Business Media, 2013.

[Sal06] Gabriel Daniel Villa Salvador. *Topics in the theory of algebraic function fields*. Springer Science & Business Media, 2006.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Gradute Texts in Mathematics*. Springer-Verlag, 1986.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure*, 2(4):521–560, 1969.

[Wes18] Benjamin Pierre Charles Wesolowski. *Arithmetic and geometric structures in cryptography*. PhD thesis, EPFL, 2018.

EPFL IC LACAL, Station 14, CH-1015 Lausanne, Switzerland

Cryptology Group, CWI, Amsterdam, The Netherlands