Lifting L-polynomials of Smooth Plane Quartics

UROP+ Final Paper, Summer 2021

Andrew Weinfeld
Mentor: David Jongwon Lee
Project suggested by: Andrew Sutherland

Abstract

We describe a method to lift L-polynomials of smooth plane quartics from their mod-p reduction using Jacobian arithmetic. We discuss a number of intricacies of implementation, particularly Jacobian arithmetic in the case of atypical divisors. We discuss curves which do not intersect a line at four rational points.

1 Introduction

Let $C/\mathbb{Q}$ be a smooth projective curve of genus g over $\mathbb{Q}$. For each prime of good reduction p, the reduction of C mod p is a smooth projective curve $C/\mathbb{F}_p$ which has an associated zeta function

$$Z(C/\mathbb{F}_p; T) = \exp\left(\sum_{k=1}^{\infty} \#(C/\mathbb{F}_{p^k})T^k/k\right) = \frac{L_p(T)}{(1-T)(1-pT)}$$

where $L_p(T)$ is a polynomial of degree $2g$ called the L-polynomial of $C/\mathbb{F}_p$. The zeta function of the curve records important geometric information, such as the group order of the associated Jacobian varieties, which is useful for cryptographic applications. The curve $C/\mathbb{Q}$ also has an associated L-function

$$L(C/\mathbb{Q}; s) = \prod_p L_p(p^{-s})^{-1}$$

where L_p is the L-polynomial of $C/\mathbb{F}_p$ when p is a prime of good reduction. Thus the L-polynomial $L_p(T)$ describes important number-theoretic information relevant to the Sato-Tate conjecture, which discusses the distribution of coefficients of $L_p(T)$ in the L-function. We are interested in the case when C is a nonhyperelliptic curve of genus 3; equivalently, C is a smooth plane quartic.

For smooth plane quartics, it has been suggested that it is possible to determine $L_p(T)$ from its reduction mod p in $O(p^{1/4})$ time using a baby-steps giant-steps algorithm.[1] There is an unpublished algorithm to compute the coefficients of $L_p(T)$ mod p,[2] with both an $O(p^{1/2})$ version for a single prime and an average polynomial time algorithm all $p \leq B$.

In order to compute the L-polynomial $L_p(T)$ of a nonhyperelliptic curve, we will use Jacobian arithmetic. The Jacobian $J(C)$ is a group of order $\#J(C) = L_p(1)$, and the Jacobian $J_2(C)$ over a degree two extension satisfies $\#J_2(C) = L_p(1)L_p(-1)$. Furthermore, there are bounds on the coefficients of $L_p(T)$ (see Section 3 for more details) which together with $L_p(T)$ mod p reduce to $O(p^{1/2})$ possibilities for the L-polynomial $L_p(T)$. A baby-steps giant-steps search may thus compute $L_p(T)$ using only $O(p^{1/4})$ operations in $J(C)$ and $J_2(C)$.

[FOR08] describe algorithms for arithmetic in the Jacobian of a smooth plane quartic C with a k-rational point. Of most interest to us is that if there is a tangent line ℓ^∞ which intersects C at four rational points, counting multiplicity (and which exists for $p \geq 66^2 + 1$), and if two divisors are "typical" (satisfy specific asymptotically favorable criteria), then [FOR08] provide an algorithm to compute the sum of these divisors in a fixed number of field operations–roughly 200 multiplications and a couple of inversions.

Thus Jacobian arithmetic in the typical case has the same asymptotic complexity as an inversion mod p, which is $(\log p)(\log\log p)^2$ time. However, atypical divisors might appear when running the baby-step giant-step algorithm.

Since only (heuristically) $O(1/p)$ divisors are atypical and we need just $O(p^{1/4})$ operations, it might seem that we could try applying baby-steps giant-steps to different starting divisors until we find one for

[1] See `https://web.maths.unsw.edu.au/~davidharvey/talks/ntdu.pdf`
[2] See Sutherland et. al. in `https://math.mit.edu/~drew/Oldenburg2017.pdf`

which no atypical divisors appear. However, we will see that atypical divisors occur not just randomly but also systemically; for instance, the identity divisor is always atypical. Should the baby-steps giant-steps algorithm require computation of a divisor which is atypical regardless of the starting divisor, we will need to work with atypical divisors.

We will describe how to handle efficient hashing of atypical divisors (necessary to create a table of baby-steps with fast lookups, since representations of atypical divisors as a linear combination of points may be nonunique). We will also show that most of [FOR08]'s algorithm may be applied in the tangent case to atypical divisors using a fixed number of field operations. Though the casework is not yet complete, there do not seem to be any significant difficulties beyond one feature of the resultant that does not seem to appear in the literature–see Conjecture 2.1–and the remaining pieces of casework may be performed through the use of polynomial factorization over the base field, which requires more than a fixed number of field operations. We use an implicit representation of divisors that extends the Mumford representation, and we examine how to apply [FOR08]'s algorithms with this new form.

In Section 3, we discuss the baby-steps giant-steps algorithm and the lifting of $L_p(T)$. In Section 4 we discuss Jacobian arithmetic. In Section 5 we discuss some of the practicalities of implementation. In Sections 6 and 7 we discuss the generic algorithms for divisor arithmetic. In Sections 8-14 we describe the handling of atypical divisors. In Section 15 we describe group inversions in the Jacobian. In Section 16 we discuss the existence of lines which intersect C at k-rational points only.

1.1 Acknowledgements

The author would like to thank David Jongwon Lee for mentorship and guidance and Professor Andrew Sutherland for suggesting this project. The author would like to thank the UROP+ program for making this research possible.

2 Preliminaries

Let k be a field. The projective plane $\mathbb{P}^2 = \mathbb{P}^2(k)$ is the set of triples $(x : y : z)$, $x, y, z \in k$ under the equivalence relation $(x : y : z) \sim (\lambda x : \lambda y : \lambda z)$ for $\lambda \in k^\times$. A plane curve $C = C(x, y, z)$ is a homogeneous polynomial in x, y, and z. A point $p \in \mathbb{P}^2(\overline{k})$ is on a plane curve C if $C(p) = 0$. A singularity on a plane curve C is a point on C where all the partial derivatives of C vanish. A plane curve is smooth if it has no singularities.

A divisor $D = \sum n_i P_i$ with $n_i \in \mathbb{Z}$, $P_i \in \mathbb{P}^2(\overline{k})$ on a smooth plane curve $C = C(x, y, z)$ is a formal linear combination of points on C over $\overline{k}$ such that D is fixed by $\mathrm{Gal}(\overline{k}, k)$. The degree of a divisor $D = \sum n_i P_i$ is $\sum n_i$. The divisors of degree zero form an abelian group $\mathrm{Div}^0(C)$.

Let f be a homogeneous polynomial in x, y, and z with coefficients from k. Then $f = 0$ defines a plane curve (not necessarily smooth). Suppose C and f do not share a common component. Then C and f intersect in finitely many points, and for each point P in the intersection we may assign an intersection multiplicity $\mathrm{ord}_P(C, f)$. For affine points P, we define $\mathrm{ord}_P(C, f)$ to be the dimension of the k-module $k[x, y]_P/(C|_{z=1}, f|_{z=1})$. We may then form the intersection divisor

$$(f \cdot C) = \sum_P \mathrm{ord}_P(C, f)P,$$

and by Beźout's theorem we have $\deg(f \cdot C) = \deg(f)\deg(C)$. Since C and f were defined over k, the intersection divisor will be closed under Galois conjugation.

We also have (see Lemma 6.1) that

$$\mathrm{ord}_{(0:0:1)}(C, f) \geq n \iff f(x, y, 1) \in \langle x, y\rangle^n + \langle C(x, y, 1)\rangle.$$

Let $\deg(C) = d$ and $\deg(f) = e$, so that $C = \sum_{i=0}^{d} a_i z^i$ and $f = \sum_{i=0}^{e} b_i z^i$ for some $a_i, b_i \in k[x, y]$. Then there is a homogeneous polynomial $\mathrm{res}_z(C, f) = \det(M|N)$ with $M = (a_{i-j})_{i,j=1,1}^{d+e,e}$ and $N = (b_{i-j})_{i,j=1,1}^{d+e,d}$. Furthermore, $\mathrm{res}_z(C, f) \in \langle C, f\rangle$.

Suppose that $(0 : 0 : 1)$ is not on the intersection of f and C. Then $\mathrm{res}_z(C, f) \in k[x, y]$ is homogeneous of degree $(f \cdot C) = \deg(C)\deg(f)$ and

$$\mathrm{res}_z(C, f) = \prod_{(x_i:y_i)\in\mathbb{P}^1} \prod_{(x_i:y_i:z_i)\in\mathbb{P}^2} (y_i x - x_i y)^{\mathrm{ord}_{(x_i:y_i:z_i)}(C,f)}.$$

Note that although the resultant may be computed for any curves f and C, the link between multiplicities and factors of the resultant depends on $(0:0:1)$ not being on the intersection of the curves. We will need to consider the resultant $\mathrm{res}_z(C,f)$ in the case where $(0:0:1)$ is on the intersection of f and C. This case does not seem to appear in the literature; however, we have Conjecture 2.1.

The issue with $(0:0:1)$ is that while each other point $(x_0:y_0:z_0)$ appears as a factor of (y_0x-x_0y) in the resultant, it is not clear what factor $(0:0:1)$ should appear as. We expect that $(0:0:1)$ appears in the resultant as a combination of the resultant having lower degree than the expected $\deg((f\cdot C))$ and the resultant having factors corresponding to the projection of $(0:0:1)$ to the line $z=0$ along the tangent to C at $(0:0:1)$.

Let $\pi:\mathbb{P}^2\to\mathbb{P}^1$ be the map sending $(x:y:z)$ to $(x:y)$. If we consider $\mathbb{P}^1$ to be embedded in $\mathbb{P}^2$ as the line $z=0$, this corresponds to projection of $(x:y:z)$ down to $z=0$ along the line through $(0:0:1)$ and $(x:y:z)$. We may extend π to $P=(0:0:1)$ by projection along the tangent line to C at P, so that $\pi(P)=(T_P(C)\cdot C)$.[3] Given a point $(x_0:y_0)$ in $\mathbb{P}^1$, we let $(x_0:y_0)^*$ be the homogeneous polynomial (y_0x-x_0y), so that when $(0:0:1)$ is not in the intersection of f and C, we have

$$\mathrm{res}_z(C,f)=\prod_{P\in\mathbb{P}^2}(\pi(P)^*)^{\mathrm{ord}_P(C,f)}.$$

Conjecture 2.1. *Let $C=C(x,y,z)$ be a smooth plane curve and let $f=f(x,y,z)$ be a homogeneous polynomial. Suppose $P=(0:0:1)$ lies on both C and f. Let $(f\cdot C)=nP+\sum n_iP_i$. Then the resultant $\mathrm{res}_z(C,f,z)$ has degree $r<\deg(C)\deg(f)$ and we have*

$$\mathrm{res}_z(C,f,z)=(\pi(P)^*)^{n-\deg(C)\deg(f)+r}\prod(\pi(P_i)^*)^{n_i}.$$

Note that when $n=1$, the tangent lines to C and f at P need not match and exponent of $\pi(P)^*$ is zero.

Conjecture 2.1 may be proven in cases when there are no additional factors corresponding to $\pi(P)=\pi((0:0:1))$ by the usual proof that the resultant respects multiplicities: noting (through looking at localizations) that that the resultant cannot underestimate factors corresponding to points other than $P=(0:0:1)$.[4] However, while it is not clear how to prove it in general, it might be possible to use some kind of continuity argument.

We may extend intersection divisors to rational functions by $((f/g)\cdot C)=(f\cdot C)-(g\cdot C)$. A divisor is principal if it is the intersection divisor of some rational function of degree 0. Principal divisors form an abelian subgroup of $\mathrm{Div}^0(C)$. We say that two divisors D_1, D_2 are linearly equivalent, $D_1\sim D_2$, if there is a function f with $D_1=D_2+(f\cdot C)$. We set $J(C)$, the Jacobian of C, to be $J(C)=J(C/k)=\mathrm{Div}^0(C)/\sim$. When k is a finite field $\mathbb{F}_p$, we set $J_n(C)=J(C/\mathbb{F}_{p^n})$.

Let D be a divisor. The set of degree zero rational functions f with $D+(f\cdot C)\geq 0$, along with $f=0$, form a k-vector space $\mathcal{L}(D)$ of dimension $\ell(D)$.

Theorem 2.2 (Riemann-Roch)**.** *There is a canonical divisor κ and an integer g (the genus) such that for every divisor D, we have*

$$\ell(D)=\deg(D)-g+1+\ell(K-D).$$

A smooth plane quartic has genus 3. A curve is said to be hyperelliptic if it has a degree two morphism to $\mathbb{P}^1$. The genus three curves which are not hyperelliptic are precisely the smooth plane quartics.

Let P be a point on C. Then $\mathcal{L}(P)$ contains the constant functions, so $\ell(P)\geq 1$. If we have a nonconstant function in $\mathcal{L}(P)$ then we have a map from C to $\mathbb{P}^1$ and the genus of C is zero. Thus for points P on smooth plane quartics, $\mathcal{L}(P)$ consists of the constant functions.

3 The L-polynomial

In this section we will discuss the lifting of the L-polynomial of a smooth plane quartic over a finite field $\mathbb{F}_p$ from its reduction mod p. Select a base field $k=\mathbb{F}_p$ for some prime $p\in\mathbb{Z}$. Let $C:C(x,y,z)=0$ be

[3] This extension was suggested by Dr. Edgar Costa.

[4] See discussion in https://math.stackexchange.com/questions/3446833/does-each-factor-of-the-resultant-correspond-to-exactly-one-intersection-point

a nonhyperelliptic curve of genus $g = 3$ over $k = \mathbb{F}_p$. Equivalently, $C(x, y, z)$ is a smooth plane quartic. The zeta function of C is

$$Z(C/\mathbb{F}_p; T) = \exp\left(\sum_{k=1}^{\infty} \#(C/\mathbb{F}_{p^k})T^k/k\right) = \frac{L_p(T)}{(1-T)(1-pT)}$$

where

$$L_p(T) = 1 + a_1T + a_2T^2 + a_3T^3 + a_2pT^4 + a_1p^2T^5 + p^3T^6$$

for some $a_1, a_2, a_3 \in \mathbb{Z}$. Furthermore (see [KS08]), we have

$$|a_i|p^{-i/2} \leq \binom{2g}{i}$$

and

$$-g + 2 + \frac{\frac{a_1^2}{p} - \delta^2}{2} \leq \frac{a_2}{p} \leq g + \left(\frac{g-1}{2g}\right)\frac{a_1^2}{p}$$

where δ is the distance from $\frac{a_1}{\sqrt{p}}$ to the nearest multiple of 4 (so $\delta < 2$).

Substituting $g = 3$ and rearranging gives

$$\begin{aligned} -6\sqrt{p} &\leq a_1 \leq 6\sqrt{p} \\ -p + \frac{1}{2}\left(a_1^2 - p\delta^2\right) &\leq a_2 \leq 3p + \frac{1}{3}a_1^2 \\ -20p^{3/2} &\leq a_3 \leq 20p^{3/2} \end{aligned}$$

Let $\overline{L_p(T)}$ be the reduction of $L_p(T)$ mod p. Then $\overline{L_p(T)} = 1 + \overline{a_1}T + \overline{a_2}T^2 + \overline{a_3}T^3$ where $\overline{a_i}$ is the reduction of a_i mod p. Therefore, if we know $\overline{L_p(T)}$, then there are p times fewer possibilities for each a_i.

When $p > 144$, we have $\sqrt{p} > 12$ and then $p > 2 \cdot 6\sqrt{p}$, so that a_1 is determined uniquely. We have $\delta^2 < 4$, so that the range of possible values for a_2 has size as most

$$3p + \frac{1}{3}a_1^2 + p - \frac{1}{2}(a_1^2 - p\delta^2) = 4p - \frac{a_1^2}{6} + \frac{p\delta^2}{2} < 6p$$

and given a_1, there are at most 6 values for a_2 (compare [KS08], which notes that a_2/p is constrained to an interval of radius 3). Finally, there are $40\sqrt{p}$ possible values of a_3.

Lemma 3.1. *Let $p > 12$. Let $\overline{L_p(T)}$ be the reduction of $L_p(T)$ mod p. Then $\overline{L_p(T)}$, $L_p(1)$, and $L_p(-1)$ uniquely determine $L_p(T)$.*

Proof. Suppose we know $L_p(1)$ and $L_p(-1)$. Then

$$\begin{aligned} L_p(1) &= (p^3 + 1) + a_1(p^2 + 1) + a_2(p + 1) + a_3 \\ L_p(-1) &= (p^3 + 1) - a_1(p^2 + 1) + a_2(p + 1) - a_3 \end{aligned}$$

Suppose there are two different possibilities for (a_1, a_2, a_3), say (a_1, a_2, a_3) and (a_1', a_2', a_3'). Substituting these values into $L_p(1) + L_p(-1)$ gives $a_2 = a_2'$. Substituting into $L_p(1) - L_p(-1)$ gives

$$a_1(p^2 + 1) + a_3 = a_1'(p^2 + 1) + a_3' \tag{1}$$

so $a_1 = a_1' \implies a_3 = a_3'$. Thus $a_1 \neq a_1'$, so $|a_1 - a_1'| \geq p$. Let $p \geq 12$, so that $p(p^2 + 1) > 40p^{3/2}$. Then

$$|a_1 - a_1'|(p^2 + 1) \geq p(p^2 + 1) > 40p^{3/2} \geq |a_3 - a_3'|$$

which contradicts (1). □

Remark 3.2. Lemma 3.1 is nonconstructive. To determine a_1, a_2, a_3 from $\overline{L_p(T)}$, $L_p(1)$, and $L_p(-1)$ we first note that

$$a_2 = \frac{L_p(1) + L_p(-1) - 2(p^3+1)}{2(p+1)}$$

and

$$\frac{a_1}{p} + \frac{a_3}{p(p^2+1)} = \frac{L_p(1) - L_p(-1)}{2p(p^2+1)}. \tag{2}$$

Let $\overline{L_p(t)} = 1 + \overline{a_1}t + \overline{a_2}t^2 + \overline{a_3}t^3$. Then $a_1 = p\left\lfloor \frac{a_1}{p} \right\rfloor + \overline{a_1}$ and $a_3 = p\left\lfloor \frac{a_3}{p} \right\rfloor + \overline{a_3}$, so rearranging (1) gives

$$\left\lfloor \frac{a_1}{p} \right\rfloor + \frac{\left\lfloor \frac{a_3}{p} \right\rfloor}{p^2+1} = \frac{L_p(1) - L_p(-1)}{2p(p^2+1)} - \frac{\overline{a_1}}{p} - \frac{\overline{a_3}}{p(p^2+1)}. \tag{3}$$

Since $p > 12$ and $|a_3| < 20p^{3/2}$, we see that $\left| \frac{\left\lfloor \frac{a_3}{p} \right\rfloor}{p^2+1} \right| < \frac{1}{2}$ and thus $\left\lfloor \frac{a_1}{p} \right\rfloor$ is the nearest integer to the right hand side of (3). Then $a_1 = p\left\lfloor \frac{a_1}{p} \right\rfloor + \overline{a_1}$ and $a_3 = \frac{L_p(1)-L_p(-1)}{2} - a_1(p^2+1)$ are determined. These values for a_1, a_2, a_3 are consistent with the known values of $\overline{L_p(T)}$, $L_p(1)$, and $L_p(-1)$, so by Lemma 3.1 we must have the correct values.

3.1 Baby-Steps Giant-Steps

Here we discuss the details of the baby-steps giant-steps search necessary to determine $L_p(T)$ from $\overline{L_p(T)}$, $L_p(1)$, and $L_p(-1)$.

For $p > 12$, we may apply the following baby-steps giant-steps algorithm. Recall that $L_p(1) = \#J(C)$. Fix some $r \approx \sqrt{20p^{1/2}}$ and let $s \approx \sqrt{20p^{1/2}}$ be the least integer with $sr > 20p^{1/2}$.

Algorithm 3.3. Baby-steps giant-steps search.

1. Select a divisor $D \in J(C)$.
2. Compute the baby steps pD, $2pD$, $\ldots$, rpD and store them in a hash table using a hashing function.
3. For each of the finitely many possible values of a_1 and a_2, let

   $$\ell = (p^3+1) + a_1(p^2+1) + a_2(p+1) - p\left\lfloor \frac{-20p^{3/2}}{p} \right\rfloor + \overline{a_3}$$

   and compute the giant steps ℓD, $(\ell + rp)D$, $(\ell + 2rp)D$ $\ldots$, $(\ell + srp)D$.
4. Look up each giant step in the hash table of baby steps. If the giant step $(\ell + jrp)D$ agrees with the baby step ipD, then $\ell + (jr - i)p$ is a possible value for $L_p(1)$ and the corresponding possibilities for the a_i are $a_1 = a_1$, $a_2 = a_2$, and $a_3 = \ell + (jr - i)p$. Otherwise, $|D| \not| \ell + (jr - i)p$ is not a possible value for $L_p(1)$.

If this algorithm outputs only a single possibility for $L_p(1)$, then we may take the corresponding possibilities for the a_i's. If this algorithm outputs multiple possible values of a_1, a_2, a_3 such that the corresponding values of $\#J(C)$ have different radicals, or such that the corresponding values of $\#J_2(C)$ have different radicals, then we may use the following algorithm to narrow down the possibilities.

Algorithm 3.4. Let $A_1(T) \ldots, A_n(T)$ be distinct possibilities for $L_p(T)$. So long as not all of the radicals $A_i(1)$ are distinct:

1. Select a divisor $D \in J(C)$.
2. For each A_i, compute $A_i(1) \cdot D$.
3. If $A_i(1) \cdot D \neq 0$, discard $A_i(T)$.

If there is only one A_i remaining, then $L_p(T) = A_i$. If all of the remaining A_i's have the same radicals, we perform the same procedure with $J_2(C)$:

1. Select a divisor $D \in J_2(C)$.
2. For each A_i, compute $A_i(-1) \cdot A_i(1) \cdot D$.
3. If $A_i(-1) \cdot A_i(1) \neq 0$, discard $A_i(T)$.

If there is only one A_i remaining, then $L_p(T) = A_i$. Otherwise, this method is not able to determine $L_p(T)$.

The only case where the above methods do not suffice are when there are at least two distinct triples (a_1, a_2, a_3) for which the corresponding $L_p(1)$ values have the same radical and the corresponding $L_p(1)L_p(-1)$ values also have the same radical. This situation is both rare and hard to analyze, so we will not study it further. However, generic group algorithms exist which can probabilistically determine the structure of a group given possibilities for the order, so this case may still be handled through other methods.

4 Jacobian Arithmetic

Fix a smooth plane quartic $C = C(x, y, z)$ over a finite field $\mathbb{F}_p$, p prime.

We say that a curve E passes through an effective divisor D if $D \leq (E \cdot C)$. Similarly, we say that E passes through $P_1, \ldots, P_n$ if E passes through $D = \sum P_i$, where the sum counts points with multiplicity. We say that points $P_1, \ldots, P_n$ are colinear if there is a line ℓ that passes through them. For instance, $3P$ is colinear if and only if P is a flex point (or hyperflex).

In order to perform Algorithm 3.3, we need:

1. Arithmetic in the Jacobian $J(C/\mathbb{F}_p)$.
2. Arithmetic in the Jacobian $J(C/\mathbb{F}_{p^2})$.
3. Unique representation of degree zero divisors on C, to be used for the hash table.

For 1 and 2, we may use the algorithms of Flon et. al. in [FOR08]. Flon et. al. describe both a generic geometric algorithm[5] and a number of broadly applicable special cases requiring a fixed number of field operations, which we will review at the end of the section. For 3, we have the following lemma:

Lemma 4.1. *Let C be a smooth plane quartic over a field k. Fix an effective divisor $D^\infty = P_1^\infty + P_2^\infty + P_3^\infty$ of degree $g = 3$. Let D be a divisor of degree zero. Then there exists an effective divisor $D^+ = P_1 + P_2 + P_3$ of degree 3 with*

$$D \sim D^+ - D^\infty.$$

Furthermore, exactly one of the following holds:

- *There is a unique effective divisor $D^+ = P_1 + P_2 + P_3$ of degree 3 with P_1,P_2,P_3 not colinear and*

$$D \sim D^+ - D^\infty.$$

- *There is a unique k-rational point P with*

$$D \sim (-P) - D^\infty.$$

Proof. We see that $D+D^\infty$ is a divisor of degree 3. By Riemann-Roch we have $\ell(D+D^\infty) = 1+\ell(\kappa-D) \geq 1$, so there is a nonzero function $f \in \mathcal{L}(D)$. Then $D^+ = D + D^\infty + \mathrm{div}(f)$ is an effective divisor of degree 3, so $D \sim D^+ - D^\infty$.

[5] The most general algorithm in[FOR08] requires a rational point on C, which is the case if $p > 29$ (see [HLT04]). If $p \leq 29$ and there is no rational point on C, then this approach is not applicable. Fortunately, such situations are rare and do not happen if $C/\mathbb{Q}$ has a rational point.

Let $D \sim (-P) - D^\infty$. Let ℓ be any line through P. Then $D^+ = (\ell \cdot C) - P$ is an effective divisor of degree 3, so $D \sim (-P) - D^\infty \sim (\ell \cdot C) + (-P) - D^\infty \sim D^+ - D^\infty$. Alternatively, let $D \sim D^+ - D^\infty$ where D^+ is colinear, say $D^+ \leq (\ell \cdot C)$ for some line ℓ. Then $D^+ = (\ell \cdot C) - P \sim -P$, so $D \sim (-P) - D^\infty$. Therefore, $D \sim (-P) - D^\infty$ if and only if there is some colinear D^+ with $D \sim D^+ - D^\infty$.

Suppose $D \sim D^+ - D^\infty$ for some $D^+ = P_1 + P_2 + P_3$ with P_1,P_2,P_3 not colinear. Then [FOR08], Section 3.1 notes that D^+ is unique. Then there is no D^+ colinear with $D \sim D^+ - D^\infty$, so there is no P with $D \sim (-P) - D^\infty$.

If there is no such D^+, then $D \sim D^+ - D^\infty$ for some D^+ colinear. Then $D \sim (-P) - D^\infty$ where $D + P = (\ell \cdot C)$. Suppose $(-P) - D^\infty \sim (-Q) - D^\infty$. Then $P \sim Q \implies P + (f \cdot C) = Q \geq 0$ for some function $f \in \mathcal{L}(P)$. As noted in Section 2 the only elements of $\mathcal{L}(P)$ are constants, so $(f \cdot C) = 0$ and $P = Q$. Thus P is unique. □

Thus after fixing D^∞, we may represent divisors by the corresponding $D^+ = P_1 + P_2 + P_3$, and in order to obtain a unique representation of a divisor,

- If P_1,P_2,P_3 are not colinear, then D^+ is unique and we may hash the multiset $\{P_1,P_2,P_3\}$.
- If P_1,P_2,P_3 are colinear, then we may compute the line ℓ through D and hash the unique additional k-rational point P on the intersection divisor $(\ell \cdot C)$, that is, the unique P with $D + P = (\ell \cdot C)$.

In the second case (with P_i's colinear), we must take care to count points with the appropriate multiplicity. Details of efficient computation of unique representation are discussed in Section 10.

4.1 Typical Divisors

In addition to generic geometric algorithms, [FOR08] give algebraic algorithms for several broad special cases. The more special the choice of D^∞, the faster the algorithm will be. The most broad case is the tangent case, which is what we will focus on.

Given a line ℓ^∞ that intersects C at four rational points, we may change coordinates so that ℓ^∞ is the line $z = 0$ at infinity and set $(\ell \cdot C) = P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty$. If ℓ is a tangent line, then we may take $P_1^\infty = P_2^\infty = (0 : 1 : 0)$ and $P_4^\infty = (1 : 0 : 0)$, then set $D^\infty = P_1^\infty + P_2^\infty + P_3^\infty$ in Lemma 4.1 and [FOR08].

We say that a divisor $D = P_1 + P_2 + P_3$ is typical if it is the sum of distinct noncolinear affine points with distinct x coordinates. In this case, we may represent D as a pair of univariate polynomials (u, v) of degrees 3 and 2, where u is monic and simple with roots the x coordinates of the P_i's and v is such that if $P_i = (x_i : y_i : 1)$ then $v(x_i) = y_i$. This is the Mumford representation of a divisor.[6] [FOR08] give algorithms to compute the sum of two typical divisors D_1 and D_2, provided that all intermediate divisors are typical and all intersection divisors have distinct affine points; specifically, there are

1. a cubic E and a typical divisor D_3 with $(E \cdot C) = D_1 + D_2 + P_1^\infty + P_2^\infty + P_4^\infty + D_3$
2. a conic Q and a typical divisor D_4 with $(Q \cdot C) = D_3 + P_1^\infty + P_2^\infty + D_4$

and then $D_1 + D_2 \sim D_4$.

We will need to handle atypical divisors. Note that while every divisor may be unique represented as $D^+ - D^\infty$ or as $(-P) - D^\infty$ and every typical divisor will have the form $D^+ - D^\infty$, not every divisor of the form $D^+ - D^\infty$ is typical–for instance, three distinct affine points, exactly two of which share an x coordinate, will always be represented as $D^+ - D^\infty$ yet will never be typical. The precise criteria for an atpyical divisor $D = P_1 + P_2 + P_3$ are the following.

- Not all of the P_i's are the same; D has a double point or a triple point.
- Two of the P_i's share an x coordinate; such an x coordinate must be k-rational, but the other coordinates need not be.
- The P_i's are colinear.

[6] In the hyperelliptic case, all divisors have a Mumford representation. This is not the case with nonhyperelliptic curves.

5 Implementation Discussion

What we have described in Sections 3 and 4 is an algorithm which can lift the L-polynomial of a smooth plane quartic using $O(p^{1/4})$ additions in $J(C)$ and $J_2(C)$, usually with proof. In order to implement this algorithm, we need to be able to perform Jacobian arithmetic. While [FOR08] describes heavily optimized algorithms which require a fixed number of field operations, these algorithms (specifically Algorithm 1) are not applicable in all cases, even assuming prerequisites like a rational flex point.

For instance, it is possible for the sum of two typical divisors to be atypical, in which case the algorithm will fail. This is quite rare when p is large, so it might seem reasonable to select a new divisor and restart the algorithm. However, it is possible for one of the giant steps to be an exact multiple of the order of $J(C)$. Since the zero divisor $0 \sim -(\ell^\infty \cdot C) = (-P_4^\infty) - D^\infty$ is atypical, the algorithm will always fail that this step.

This suggests a possible fallback: if we repeatedly encounter an atypical divisor at a particular giant step nD, this might be indicative that $nD \sim 0$ and n is a multiple of $\#J(C)$. However, there are other reasons why a particular multiple nD might be atypical for all D. If $J(C) \simeq C_{n_1} \times C_{n_2}$ is a product of cyclic groups where n_1, n_2 are relatively prime, then there are n_1 elements of order dividing n_1, and if all are atypical then $n_2 D$ will be atypical for all D. Thus we will eventually need to perform computations with atypical divisors. Furthermore, if we can do computations with atypical divisors efficiently this will be much faster than restarting the entire algorithm with a new choice of D.

Fortunately, we can find a variant of Mumford representation to include all divisors, and we will provide algorithms for arithmetic of atypical divisors. Although these algorithms do not completely reduce the problem to a fixed number of field operations (a polynomial factorization may be required in some branches), most cases are quite efficient.

Efficient algorithms for the typical case are described in [FOR08]. We will discuss generic algorithms which apply in all cases and then describe how to refine these into fast algorithms for atypical divisors in the tangent case. By [OR10], Theorem 2, all curves with p sufficiently large have a tangent line which intersects the curve at four (counting multiplicity) rational points. Furthermore, [OR10] Proposition 2 provides a lower bound of $p + 1 - 66\sqrt{p}$ such tangent lines,[7] and since there are at most 28 bitangents and 24 flex points, it is reasonable to randomly search for tangent lines when p is sufficiently large. Thus for atypical divisors, we will focus on the tangent case.

6 Interpolation

First, we recall the following result about intersection multiplicity.

Lemma 6.1. *Let $P = (x_0, y_0)$ be an affine point on a curve C. Then the ideal of plane curves which intersect C with multiplicity at least n at P is*

$$\langle x - x_0, y - y_0 \rangle^n + \langle C(x, y) \rangle.$$

Proof. Let E be a plane curve which intersects C at P. Change coordinates so that P becomes $P' = (0, 0)$, E becomes $E'(x, y)$, and C becomes $C'(x, y)$. The intersection multiplicity E' and C' at P' is the least n with

$$E' \in \langle x, y \rangle^n k[x, y]_{P'} / \langle C' \rangle.$$

Then the result follows from changing coordinates back. □

Now interpolation may be done easily–we change to affine coordinates, compute the ideal in the lemma for each point in the divisor, compute the intersection of these ideals using Gröbner basis techniques, select an element of the intersection of the desired degree, and then change coordinates back and homogenize.

However, computing Gröbner bases and ideal intersections is rather slow. The ideal $\langle x - x_0, y - y_0 \rangle^n$ has a reasonably special form, and it turns out that we can reduce the problem to linear algebra over a fixed dimension.

Select a positive integer d. For the rest of this section, given a smooth plane curve $C(x, y, z)$, let $\mathcal{E}$ be the vector space of homogeneous degree d curves over $k[x, y, z]$, and given a divisor $\mathcal{D}$ on C, let $\mathcal{E}_{C,\mathcal{D}}$ be the subspace of $\mathcal{E}$ of curves which pass through $\mathcal{D}$.

[7] counting bitangents twice

Lemma 6.2. *Fix a positive integer n. Let $P = (0 : 0 : 1)$ be a point on a curve $C(x, y, z)$. Let $\mathcal{T} = k[x, y]/\langle x, y\rangle^n$ be the k-vector space spanned by monomials in x and y of degree less than n, where x and y act on $\mathcal{T}$ by $x({}^iy^j) = x^{i+1}y^j$ and $y(x^iy^j) = x^iy^{i+1}$ for $\deg(x^iy^j) < n-1$ and $x(x^iy^j) = y(x^iy^j) = 0$ for $\deg(x^iy^j) = n-1$. Let $\overline{C} = C(x, y, 1)$ mod $\langle x, y\rangle^n$ be the dehomogenization of C reduced into $\mathcal{T}$. Then $\mathcal{E}_{C,nP}$ spanned by the degree d homogenizations (with respect to z) of*

$$x^iy^j \cdot \overline{C}$$

for all $i, j < n$.

Now interpolation through a divisor D on C is straightfoward: for each term nP in D, we change coordinates and use Lemma 6.2 to compute a basis for $\mathcal{E}_{C,nP}$. Then, we use standard linear algebra to determine the intersection of all of these spaces and choose any element of this intersection. In more detail:

Algorithm 6.3. Let C be a plane curve. Fix a positive integer d and let $\mathcal{E}$ be as earlier. Let $D = \sum n_iP_i$ be a divisor on C. We will find a degree d curve E with $(E \cdot C) \geq D$ or reject if there is no such curve.

1. For each n_iP_i in D:
   (a) Change coordinates so that $P_i = (0 : 0 : 1)$. Let C' be C after changing coordinates.
   (b) Compute the spanning set $\mathcal{S}$ of $\mathcal{E}_{C',n_iP_i}$ as in Lemma 6.2.
   (c) From S, compute a basis $\mathcal{B}_i'$ for $\mathcal{E}_{C',n_iP_i}$.
   (d) Change coordinates back so that $\mathcal{B}_i'$ becomes a basis $\mathcal{B}_i$ for $\mathcal{E}_{C,n_iP_i}$.
   (e) Construct a basis $\mathcal{B}_i^\top$ for the orthogonal complement $\mathcal{E}_{C,n_iP_i}^\top$ of $\mathcal{E}_{C,n_iP_i}$.
2. Let N be the matrix whose rows are the elements of $\mathcal{B}_i^\top$ for all i, so that
$$\ker N = \bigcap_i \mathcal{E}_{C,n_iP_i} = \mathcal{E}_{C,D}$$
3. Select an element E of the kernel of N. If the kernel of N is empty, reject.

Output E, a degree d curve with $(E \cdot C) \geq D$.

Remark 6.4. If d is at least the degree of C, then the methods in this section may return a multiple of C. This is not a concern for our purposes (since we will always have C a quartic and $d = 2, 3$) but in general it may be useful to exclude such curves.

Our methods for handling atypical divisors will frequently use specialized versions of this algorithm for specific situations.

7 Intersection

We summarize the classical algorithm for computing the intersection divisor of two curves.[8]

Let C_1 and C_2 be two curves of degrees m and n, not necessarily smooth, with no common components.

1. Factor the resultant $\mathrm{res}_y(C_1, C_2)$ factors as a product of linear factors of the form $(bx - az)$.
2. For each distinct linear factor $(bx - az)$ of the resultant and each root y_i of
$$\gcd(C_1(a, y, b), C_2(a, y, b)),$$
the point $P = (a : y_i : b)$ is on the intersection of C_1 and C_2. If the gcd is zero, then C_1 and C_2 share the common component $(bx - az)$.
3. The distinct points in the intersection divisor are precisely the points $(a : y_i : b)$ determined in the previous step and possibly the point $(0 : 1 : 0)$ (which may be checked by substitution into C_1 and C_2).

[8] See for instance `http://www.math.chalmers.se/~stevens/bezout.pdf`.

4. To determine the multiplicities, we first change coordinates so that $(0:1:0)$ is not on the intersection and not on any line containing any two distinct intersection points. There are finitely many such lines, so such a change of coordinates exists (possibly requiring a field extension).

5. The resultant $\mathrm{res}_y(C_1, C_2)$ (note that we have changed coordinates) factors as a product

$$\mathrm{res}_y(C_1, C_2) = \prod (b_i x - a_i z)^{n_i}.$$

By our change of coordinates, $\gcd(C_1(a_i, y, b_i), C_2(a_i, y, b_i))$ has a unique root y_i (since otherwise we would have two intersection points on the veritcal line $b_i x - a_i z$, which passes through $(0:1:0)$).

6. Finally,

$$(C_1 \cdot C_2) = \sum n_i (a_i : y_i : b_i).$$

When working with atypical divisors, we prefer to avoid polynomial factorizations, so we will have to use other means to determine the distinct points in the intersection. However, once we have a description of the distinct points in the intersection, we will use the resultant to determine the corresponding intersection multiplicities (and we will need Conjecture 2.1 to avoid changes of coordinates).

8 Atypical Divisor Arithmetic

In order to compute with atypical divisors efficiently, we would like a way to describe these divisors over the base field. For Sections 8-14, we take $\ell^\infty = z$ to be the line at infinity and which is tangent to C at $P_1^\infty = P_2^\infty = (0:1:0)$, intersects C at $P_4^\infty = (0:0:1)$, and intersects C at one addition point P_3^∞ which is distinct from the other P_i^∞'s.

Definition 8.1. Let $u, v, w \in k[x]$ and $a \in k$. Set

$$(u, v) = \sum_{u(x_0)=0} (x_0 : v(x_0) : 1)$$

and

$$[a, w] = \sum_{w(y_0)=0} (a : y_0 : 1).$$

We require that u and w are monic of degree at least two, with simple roots and $\deg(v) < \deg(u)$. Note that u and w may be reducible.

An effective divisor of degree at most 3 on a curve may be (nonuniquely) represented by a sum of divisors of the following form.

1. $D = (x_0 : y_0 : 1)$, a k-rational affine point.
2. $D = P_i^\infty$, a point at infinity. For us, all points at infinity will be k-rational.
3. $D = (u, v)$, precisely $\deg(u)$ distinct points with distinct x coordinates, possibly k-rational but possibly defined over an extension field.
4. $D = [a, w]$, precisely $\deg(w)$ distinct points sharing an x coordinate $a \in k$, possibly k-rational but possibly defined over an extension field.

To see this, write the divisor as a sum of Galois orbits and note that the only possible issue is that the first coordinates of a Galois orbit might not be distinct (preventing a representation as (u, v)) while the first coordinates might not all be defined over k (preventing a representation as $[a, w]$). Then there is a strict inclusion of fields $k_2 \supset k_1 \supset k$ where k_1 contains the first coordinates and k_2 contains the second coordinates. Then $[k_2 : k] \geq 4$, so our divisor has degree at least 4, so for divisors of degree at most 3 this cannot happen.

Similar to the Mumford representation, this representation of effective divisors provides enough information to reconstruct the original divisor while allowing convenient implicit descriptions. For instance,

we do not require the divisor to be decomposed down to Galois orbits, thus avoiding the need to check for irreducibility later on.

Every effective divisor of degree 3 is uniquely represented by one of the following ten possible configurations.

1. $D = (u, v)$ with $\deg(u) = 3$. Three distinct points with distinct x coordinates. When $\deg(v) = 2$, we have the typical case.
2. $D = (u, v) + P_i^\infty$ with $\deg(u) = 2$. Two distinct points with different x coordinates and a point at infinity.
3. $D = [a, w]$ with $\deg(w) = 3$. Three distinct points sharing an x coordinate.
4. $D = [a, w] + (x_0 : y_0 : 1)$ where $\deg(w) = 2$ and $x_0 \neq a$. Three distinct affine points, two of which share an x coordinate.
5. $D = [a, w] + P_i^\infty$ where $\deg(w) = 2$. Two distinct affine points sharing an x coordinate and a point at infinity.
6. $D = 2(x_0 : y_0 : 1) + (x_1 : y_1 : 1)$ where $(x_0 : y_0 : 1)$ and $(x_1 : y_1 : 1)$ are distinct affine points. Double point with another affine point.
7. $D = 2(x_0 : y_0 : 1) + P_i^\infty$. Double point with a point at infinity.
8. $D = 3(x_0 : y_0 : 1)$. Triple point.
9. D is the sum of two points at infinity and one k-rational affine point.
10. D is the sum of three points at infinity.

Note that although this represents effective divisors of degree three uniquely, this does not uniquely represent the corresponding elements of $J(C)$. This is discussed in Section 10.

9 Linear Interpolation

We will need to determine when the points of a divisor lie on a line. We will first need to determine how to interpolate through a degree two effective divisor.

Let $\mathcal{D}$ be a degree two effective divisor. Then it is always possible to find a line ℓ through $\mathcal{D}$. We do so as follows.

1. $\mathcal{D} = (u, v)$ with $\deg(u) = 2$. Then $\ell = y - v$.
2. $\mathcal{D} = [a, w]$ with $\deg(w) = 2$. Then $\ell = x - az$.
3. $\mathcal{D} = (x_0 : y_0 : z_0) + (x_1 : y_1 : z_1)$ is the sum of two distinct affine points with different x coordinates. Then $\ell = (y_0 z_1 - y_1 z_0)x + (x_1 z_0 - x_0 z_1)y + (x_0 y_1 - x_1 y_0)z$.
4. $\mathcal{D} = 2P = 2(x_0 : y_0 : z_0)$. Then $\ell = \frac{\partial C}{\partial x}\big|_P x + \left.\frac{\partial C}{\partial y}\right|_P y + \frac{\partial C}{\partial z}\big|_P z$.

Now let D be a degree three effective divisor. We will determine if the points of D are colinear, and if they are, find the line ℓ with $D \leq (\ell \cdot C)$ and the point P with $D + P = (\ell \cdot C)$.

1. $D = (u, v)$ with $\deg(u) = 3$. Then the curve $y - v$ passes through D, so the points are colinear if and only if $\deg(v) \leq 1$ and in this case $\ell = y - v$. Then ℓ does not contain P_1^∞, and ℓ contains P_4^∞ if and only if $\deg(v) = 0$, in which case $P = P_4^\infty$. Otherwise, $P = (x_0, y_0, 1)$ where x_0 is the unique root of $\mathrm{res}_x(C, \ell)/u = C(x, v, 1)/u$ and $y_0 = v(x_0)$.
2. $D = [a, w]$ with $\deg(w) = 3$. Then the points of D are always colinear and $\ell = x - az$. The fourth point is $P = P_1^\infty$.

3. In the remaining cases, $D = \mathcal{D} + P'$ is the sum of a degree two effective divisor $\mathcal{D}$ and some k-rational point P'. We may interpolate a line ℓ through $\mathcal{D}$ as in earlier in the section, and it suffices to determine if ℓ passes through P' (with the appropriate multiplicity, if P' occurs in $\mathcal{D}$).
   (a) If P' does not occur in $\mathcal{D}$, then we may substitute P' into ℓ, and D is colinear if and only if ℓ contains P'.
   (b) If $\mathcal{D} = P' + P''$, then D is colinear if and only if ℓ is the tangent line to C through P' (and thus intersects P' with multiplicity at least 2).
   (c) If $\mathcal{D} = 2P'$, then $D = 3P'$ and the points of D are colinear if and only if P' is a flex point of C, which is the case if and only if the determinant of the hessian of C (which is a degree 6 curve) vanishes at P.[9]

10 Linear Intersection

In the later sections, when handling degenerate curves, we will frequently encounter a line ℓ and an effective divisor $D \leq (\ell \cdot C)$ and need to compute the effective divisor $(\ell \cdot C) - D$. We are concerned with the cases where D has degree 1, 2, or 3. In particular, when D has degree 3, the methods in this section allow us to determine the unique point P with $D + P = (\ell \cdot C)$, which resolves the issue of efficiently and uniquely identifying elements of the Jacobian.

Let ℓ be a line. We may determine $(\ell \cdot C)$ as follows.

- If $\ell = z$, then $(\ell \cdot C) = P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty$ and $(\ell \cdot C) - D$ may be computed directly.
- If $\ell = x - az$, then since ℓ does not contain $(1 : 0 : 0)$, we may take the resultant with respect to x to obtain the multiplicities of the $(y : z)$ ratios in $(\ell \cdot C)$. We have $\mathrm{res}_x(C, \ell) = C(az, y, z)$ is a homogeneous quartic in y and z. Furthermore, since $P_1^\infty(0 : 1 : 0)$ is the only point on ℓ and P_1^∞ is on C, we see that $z | C(az, y, z)$ and the multiplicity of P_1^∞ in $(\ell \cdot C)$ is equal to the number of factors of z which divide $C(x, az, z)$. Then setting $z = 1$ in the resultant yields a polynomial $w(y) = C(a, y, 1)$ whose roots are the y coordinates of $(\ell \cdot C)$, counting multiplicity. If $\deg w \leq 1$ or there are repeated roots, then we may find all roots y_i explicitly and the affine points on the divisor are $(a : y_i : 1)$. Otherwise, $w(y)$ is a monic simple polynomial of degree at least two and the affine points on the divisor are $[a, w]$. Then computation of $(\ell \cdot C) - D$ is straightforward, since the only case where we might not use direct compartison of points is when $(\ell \cdot C)$ has an $[a, w(y)]$ term and D has an $[a, \tilde{w}(y)]$ term with $\tilde{w} | w$, in which case we may use $[a, w] - [a, \tilde{w}] = [a, w / \gcd(w, \tilde{w})]$.
- If $\ell = y - ax - bz$, then since ℓ does not contain $(0 : 1 : 0)$ we may take the resultant with respect to y to determine the $(x : z)$ ratios in $(\ell \cdot C)$. For each of the possibilities for terms in a divisor (affine point, infinite point, (u, v), $[a, w]$) the multiplicity of each $(x : z)$ ratio is known, so we have a homogeneous polynomial $u(x, z)$ in x and z whose roots are the multiplicity of $(x : z)$ ratios in $(\ell \cdot C) - D$ and which thus has degree at most 3. There is at most one distinct point at infinity, which may be determined by substitution into ℓ, and its multiplicity in $(\ell \cdot C) - D$ is the number of factors of z in $u(x, z)$. Then $u = u(x, 1)$ has roots which are the multiplicities of the x coordinates of the affine points of $(\ell \cdot C) - D$ and we may either determine the x coordinates x_i explicitly (and the y coordinates are then $y_i = ax_i + b$) and proceed as in the previous case, or u is irreducible of degree at least 2 and the affine points of $(\ell \cdot C) - D$ are represented by $(u, ax + b)$.

In the case where D has degree 3, we may determine as in Section 9 whether or not there is a line ℓ through D, and if there is, we may use the above methods to compute the unique point P such that $D + P = (\ell \cdot C)$, which was what we needed for unique identification of elements of the Jacobian.

11 Conic Interpolation

Given a divisor D described in the above form, we need to find a conic Q with $(Q \cdot C) \geq D + P_1^\infty + P_2^\infty$. If the points of D are colinear, say $D \leq (\ell \cdot C)$ for some line ℓ, then ℓ may be computed as in Section 9 and we may take $Q = \ell^\infty \ell$. Otherwise, there are 8 cases.

[9] See [FOR08], Proposition 6.

1. $D = [a, w] + (x_0 : y_0 : 1)$. Then $Q = (x - az)(x - x_0 z)$.

2. $D = 2(x_0 : y_0 : 1) + (x_1 : y_1 : 1)$. If the tangent T_P to C at $(x_0 : y_0 : 1)$ is vertical (intersects P_1^∞), we may take $Q = (T_P)(x - x_1 z)$. Otherwise, the relations $\frac{\partial C}{\partial x}\frac{\partial Q}{\partial y} = \frac{\partial C}{\partial y}\frac{\partial Q}{\partial x}$ at $x = x_0, y = y_0, z = 1$ and requiring (x_0, y_0) and (x_1, y_1) to be affine points on $Q(x, y, 1)$ give a system of linear equations in the coefficients of the conic $Q = y + ax^2 + bx + c$ whose solution is the desired curve.

3. $D = 3(x_0 : y_0 : 1)$. If the tangent T_p to C at $(x_0 : y_0 : 1)$ is vertical (intersects P_1^∞), we may take $Q = T_p^2$. Otherwise, let $C' = C(x + x_0, y + y_0, 1)$. Then

$$C' \equiv f_1 x + f_2 y + f_3 x^2 + f_4 xy + f_5 y^2 \bmod \langle x, y\rangle^3$$

with f_2 nonzero. Set

$$\begin{aligned} Q' &= f_2 y + \left(f_3 - \frac{f_1 f_4}{f_2} + \frac{f_1^2 f_5}{f_2^2}\right) x^2 + f_1 x \\ &\equiv C' - \frac{f_5}{f_2} y C' - \left(\frac{f_4}{f_2} + \frac{f_1 f_5}{f_2^2}\right) x C' \bmod \langle x, y\rangle^3 \\ &\in \langle x, y\rangle^3 + \langle C'\rangle \end{aligned}$$

and we may take Q to be the homogenization with respect to z of $Q'(x - x_0, y - y_0, 1)$.

4. $D = (u, v)$ with $\deg(u) = 3$ and $\deg(v) = 2$. This is the typical case.

5. $D = P_3^\infty + \mathcal{D}$ or $D = P_4^\infty + \mathcal{D}$, where $\mathcal{D}$ is a degree two effective divisor. Then we may select a line ℓ through $\mathcal{D}$ as in Section 9 and take $Q = \ell^\infty \ell$.

Let $C = y^3 + y^2(gx^2 + hx + i) + y(jx^3 + kx^2) +$ lower terms. Let $Q = yz + gx^2 + bxz + cz^2$. Then $\operatorname{res}_y(C, Q)$ has degree 6, so Q passes through P_1^∞ with multiplicity at least 2.

Also, if $a \neq 0$ then Q cannot pass through P_3^∞ or P_4^∞, so each factor of z in $\operatorname{res}_y(C, Q)$ must correspond to an additional copy of P_1^∞ in $(Q \cdot C)$. Thus in order to interpolate through nP_1^∞ it suffices to ensure that $a \neq 0$ and that the first $n - 2$ coefficients of $\operatorname{res}_y(C, Q)$ are 0, so that $z^{n-2} | \operatorname{res}_x(C, Q)$.

6. $D = P_1^\infty + (u, v)$ with $\deg(u) = 2$. Let $Q = yz + ax^2 + bxz + cz^2$. Then the coefficient of x^6 in $\operatorname{res}_y(C, Q)$ is

$$a^3 - ga^2 = (-1)(-a + g)a^2.$$

Since $(0 : 1 : 0)$ is not a flex, $g \neq 0$. Then we may take $Q = y + gu - v$.

7. $D = 2P_1^\infty + (x_0 : y_0 : 1)$. Let $Q = yz + gx^2 + bxz + cz^2$, so that the coefficient of x^2 in Q is nonzero and the coefficient of x^6 in $\operatorname{res}_y(C, Q)$ is zero. The coefficient of $x^5 z$ in $\operatorname{res}_y(C, Q)$ is

$$bg^2 - g^2 h + gj = g^2(b - (h - j/g)).$$

Then we may take $Q = y + gx^2 + (h - j/g)x - (y_0 + hx_0^2 + (h - j/g)x_0)$.

8. $D = 3P_1^\infty$. Let $Q = yz + gx^2 + (h - j/g)xz + cz^2$, so that the coefficient of x^2 in Q is nonzero and the coefficients of x^6 and $x^5 z$ in $\operatorname{res}_y(C, Q)$ are zero. The coefficient of $x^4 z^2$ in $\operatorname{res}_y(C, Q)$ is

$$cg^2 - g^2 i - hj + gk + j^2/g = g^2(c - (g^3 i + ghj + g^2 k + j^2)/g^3).$$

Then we may take $Q = y + gx^2 + (h - j/g)x + (g^3 i + ghj - g^2 k - j^2)/g^3$.

12 Conic Intersection

Recall that Q is a conic with $(Q \cdot C) = P_1^\infty + P_2^\infty + D_3 + D$, with D_3 known and $P_1^\infty = P_2^\infty = (0 : 1 : 0)$. In particular, since the tangent line to C at P_1^∞ is $z = 0$, the tangent line to Q at P_1^∞ is also $z = 0$. In particular, the only nonzero terms in Q are yz, x^2, xz, and z^2.

If Q has no x^2 term, then $Q = \ell^\infty \ell$ for some line ℓ and we may determine $(Q \cdot C) = (\ell \cdot C) + (\ell^\infty \cdot C)$ as in Section 10. (The difficulty that D_3 is not necessarily contained in $(\ell \cdot D)$ may be easily handled, since this is only possible if D_3 contains P_4^∞.)

The remaining cases are $Q = y - v$ where $v = ax^2 + bx + c$ and Q is a homogeneous quadratic in x and z.

Let $Q = y - v$. Note that P_3^∞ and P_4^∞ are not on Q. By Conjecture 2.1 we see that copies of $(0:1:0)$ correspond to factors of z in the resultant $\mathrm{res}_y(Q, C)$ (since the tangent line to C and Q at $(0:1:0)$ is $z = 0$, which intersects $y = 0$ at $(1:0:0)$, which corresponds to factors of z) or to missing factors in the resultant $\mathrm{res}_y(Q, C)$ (which has degree 8).

Let $r(x)$ be the resultant $r(x) = \mathrm{res}_y(Q, C)|_{z=1} = C(x, v, 1)$. Then the x coordinates of affine points of $(Q \cdot C)$ are given with multiplicity by the roots of $r(x)$, and the number n of copies of P_1^∞ in the intersection is $n = 8 - \deg(r)$ since both missing terms in the resultant and factors of z in the resultant will disappear from r. We may then determine the number of copies of P_1^∞ by removing the two copies known copies and any copies from D_3. Suppose there are m copies of P_1^∞ left. Then $D = mP_1^\infty + \mathcal{D}$, where the points of $\mathcal{D}$ are all affine.

The x coordinates of affine points of $(Q \cdot C)$ are given with multiplicity by the roots of $r(x) = \mathrm{res}_y(Q, C)|_{z=1} = C(x, v, 1)$. We may thus determine the x values of the divisor $\mathcal{D}$ by dividing r by terms corresponding to the affine x values of D_3. These terms are determined as follows.

1. $(x_0 : y_0 : 1)$ corresponds to $x - x_0$.
2. (u, v) corresponds to u. This (when $\deg(u) = 3$) is the typical case.
3. $[a, w]$ corresponds to $(x - a)^{\deg(w)}$.

After removing these terms from r, we see that the x coordinates the points of $\mathcal{D}$ are precisely the roots of r, counting multiplicity. Since Q is linear in y, we see that each x coordinate determines a unique y coordinate, that is, if $\mathcal{D}$ contains two points sharing an x coordinate then they are the same point. We may determine $\mathcal{D}$ as follows.

1. If $\gcd(r, r') = 1$, then $\mathcal{D} = (r, v)$. When $n = 0$ and $D = \mathcal{D}$, this is the typical case.
2. If $\gcd(r, r')) \neq 1$, then D has a double point or a triple point and the roots of r may be recovered directly. Then $\mathcal{D}$ is just the sum over $n_i(x_i : v(x_i) : 1)$, where n_i is the multiplicity of x_i as a root of $r(x)$.

Thus we have determined $D = mP_1^\infty + \mathcal{D}$.

Suppose Q has no y term. Then Q is a polynomial in x of degree at most 2. If Q is at most linear in x, then Q factors as $\ell^\infty \ell$ for some line ℓ and we may use the methods of Section 10. Otherwise, Q factors as a product $Q = (x - az)(x - bz)$ of lines; however, we might not know what these lines are (without a polynomial factorization, which we avoid). We will show how to determine a and b, and then the methods of Section 10 may be applied.

If $a = b$, then $Q = (x - az)^2$ and we may determine a. Let $a \neq b$. The only infinite points on $(Q \cdot C)$ are two copies of P_1^∞, so the points of D_3 are all affine and have x coordinates a or b. Since $\deg D_3 = 3$, we see that D_3 has a shared x coordinate or a double point, and looking at the cases for atypical divisors in Section 8, we see that the x coordinates of points of D_3 are always known. Thus we may determine a and b and apply the methods of Section 10 to the lines $x - az$ and $x - bz$.

13 Cubic Interpolation

In Section 11, we described a procedure for computing a conic passing through $P_1^\infty + P_2^\infty + D_3$. That procedure required a different case for each possible configuration of D_3. For the cubic, we need to interpolate through two divisors D_1 and D_2, which results in a dramatically greater number of configurations. Instead of treating each configuration separately, we will instead show how to convert each of the possible terms in a divisor (k-rational affine point, infinite point, (a, u), or $[a, w]$) into linear relations in the coefficients of the cubic. It is possible that some conditions will overlap, in which case there will be more than one cubic E and there will be multiple (linearly equivalent) possibilities for D_3.

One point that requires special care is that D_1 and D_2 might have a point in common without it being clear–for instance, if $u(x) = (x-2)(x-3)(x-9)$, $v(x) = 1+(x-2)(x-4)$, and $w(y) = (y-1)(y-5)(y-7)$, then $D_1 = (u, v)$ and $D_2 = [2, w]$ will both contain $(2 : 1 : 1)$ since $u(2) = 0$, $v(2) = 1$, and $w(2) = 0$. If we were to convert (u, v) and $[a, w]$ into linear relations directly, we would only interpolate once through $(2 : 1 : 1)$ instead of twice.

In order to avoid this, it is necessary to compare each term in D_1 with each term in D_2 to check for points in common. There are several cases to consider, all of which are straightforward (for instance, (u, v) and a, w share a point if and only if $u(a) = 0$ and $w(v(a)) = 0$, in which case the shared point is $(a : v(a) : 1)$). Thus we may efficiently write $D_1 + D_2$ as a sum of terms which are one of a k-rational affine point, an infinite point, (a, u), or $[a, w]$, such that the supports of each term are disjoint or equal.

Once we have written $D_1 + D_2$ in this form, we may to convert to linear criteria and solve for the cubic E.

A general cubic E has the form

$$f_1y^3 + f_2xy^2 + f_4x^3 + ry^2 + sy + t$$

where $f_1, f_2, f_3, r \in k$, $s, t \in k[x]$, and $\deg(s), \deg(t) \leq 2$. Let $s = s_2x^2 + s_1x + s_0$ and $t = t_2x^2 + t_1x + t_0$. As noted in [FOR08], Lemma 1, interpolation through $P_1^\infty + P_2^\infty + P_4^\infty$ is equivalent to $f_1 = f_2 = f_4 = 0$. Thus we must show how to convert each D_i into linear relations in r, s_2, s_1, s_0, t_2, t_1, and t_0.

Note that if an affine point occurs more than twice, then it must be a double point in either D_1 or D_2 and we will know its coordinates directly. Thus we only need to consider interpolation through divisors of the forms $[a, w]$, $2[a, w]$, (u, v), $2(u, v)$, nP, or mP_i^∞ where $a \in k$, $u, v, w \in k[x]$ u, w are monic and simple of degree 2 or 3, $\deg v < \deg u$, P is an affine point, $n \leq 6$, and $m \leq 8$.

1. $[a, w]$ becomes $w(y)|(ry^2 + s(a)y + t(a))$. When $\deg(w) = 3$, this gives three linear relations $r = s(a) = t(a) = 0$. When $\deg(w) = 2$, this gives $ry^2 + s(a)y + t(a) = rw$, which corresponds to two linear relations, one in the constant coefficients and one in the y coefficients.

2. (u, v) becomes $u|E(x, v, 1)$. Suppose $\deg u = 3$. Let $u = x^3+u_2x^2+u_1x+u_0$ and $v = v_2x^2+v_1x+v_0$. This gives
$$rv^2 + sv + t = (rv_2^2x - rv_2^2u_0 + 2rv_2v_1)u$$
which corresponds to three linear relations upon looking at the coefficients of 1, x, and x^2. Suppose $\deg u = 2$. Then $\deg v \leq 1$ and we have $rv^2 + sv + t = rv_1^2u$, which gives two linear relations, one in the constant coefficients and one in the x coefficients.

To handle $2[a, w]$ and $2(u, v)$, it suffices to describe the conditions for agreement of the tangent lines to E and C at the corresponding points in addition to the criteria for $[a, w]$ and (u, v).

3. $2[a, w]$ becomes $w|(\frac{\partial C}{\partial x}\frac{\partial E}{\partial y} - \frac{\partial C}{\partial y}\frac{\partial E}{\partial x})_{x=a,z=1}$.

4. $2(u, v)$ becomes the second collection of equations in the doubling step of [FOR08], specifically (in [FOR08]'s notation) $2v_1 + s \equiv r\delta_1$ $[u_1]$. When $\deg u = 3$, this is the typical case.

5. For points with known coordinates (affine or infinite), we may change coordinates to put the point at $(0 : 0 : 1)$, apply Lemma 6.2, take the orthogonal complement, and change coordinates back. All arithmetic will be done over the base field, and this procedure only requires linear algebra with fixed dimension. For affine points, the highest dimension necessary is 15 (in the case where $D_1 = D_2 = 3P$ for some affine point P). For points at infinity, the highest dimension would be 28 (in the case where $D_1 = D_2 = P_1^\infty$) but the relevant equations may be precomputed.

14 Cubic Intersection

The casework for this section is not yet complete. However, here is a brief discussion of the relevant techniques which we expect will suffice.

We have a cubic E and two divisors D_1 and D_2, and we want to compute the divisor D_3 which satisfies $(E \cdot C) = P_1^\infty + P_2^\infty + P_4^\infty + D_1 + D_2 + D_3$.

Using Lemma 6.2, we may determine the multiplicities of infinite points on D_3. We may construct polynomials whose roots are the x coordinates or the y coordinates of (u, v) or $[a, w]$, counting multiplicity.

Then using resultants and Conjecture 2.1, and removing the factors corresponding to $P_1^\infty + P_2^\infty + P_4^\infty + D_1 + D_2$, we may construct polynomials whose roots are the x and y coordinates of the affine part of D_3, counting multiplicity. Note that since the tangent lines to C and E at P_4^∞ are not constrained in any way, we might need Conjecture 2.1 to remove the factors from $\mathrm{res}_x(C, E)$ which correspond to extra copies of P_4^∞.

The hope is that in typical or close to typical cases the methods used in [FOR08] will be applicable, while in the more atypical cases, the information described above will suffice. For instance, if there is only one affine point in D_3 then its coordinates may be determined from $\mathrm{res}_y(C, E)|_{z=1}$ and $\mathrm{res}_x(C, E)|_{z=1}$ by removing factors corresponding to points of $P_1^\infty + P_2^\infty + P_4^\infty + D_1 + D_2$ and taking the roots of the unique remaining factors to find the x and y coordinates.

15 Jacobian Inversions

We would like an efficient algorithm to compute a group inversion in the Jacobian. This is handled by [FOR08] in the case of a flex point (as part of their ordinary algorithm) but the tangent case is different.

Proposition 15.1. *Let D be a divisor. Let Q be the conic passing through $D + 2P_4^\infty$. Then Q passes through an additional three points which form the divisor which is the inverse of D.*

Proof. Let $(Q \cdot C) = 2P_4^\infty + D + D'$ for some effective divisor D' of degree 3. Then

$$(D - D^\infty) + (D' - D^\infty) \sim -2P_4^\infty - 2D^\infty = -2(\ell^\infty \cdot C) \sim 0$$

and D' is the additive inverse of D in the Jacobian. □

Lemma 15.2. *The conic Q from the proposition is generically of the form*

$$y^2 + ax\left(y + \frac{n}{j}\right) + by + c$$

where n is the coefficient of x^3z in C and j is the coefficient of x^3y in C.

Note that since we are in the tangent case, P_4^∞ is different from P_3^∞, the tangent line to C at P_4^∞ is not $\ell^\infty = z$, and j is nonzero.

It should be feasible to extend the work with atypical divisors to perform inversions in the Jacobian in a fixed number of field operations.

16 Rational Lines and Tangent Lines

From [OR10], we see that if $p \geq 127$ then there must always exist a line ℓ with $(\ell \cdot C) = P_1 + P_2 + P_3 + P_4$ and the P_i's all k-rational. Recall that when such a line exists, we may perform our algorithm with all computations over the base field. Oyono and Ritzenthaler note that their bound of $p \geq 127$ may not be optimal, and also that by [HLT04] there are curves with $p = 29$ with no rational points, hence no line ℓ. We suggest that it is practical to find all smooth plane quartics $C/\mathbb{F}_p$ with such a line ℓ for $p > 29$ prime up to linear change of coordinates via brute force search.

Let $C/\mathbb{F}_p$ be a smooth plane quartic, $p > 29$ prime, and suppose there is no line ℓ where $(\ell \cdot C) = P_1 + P_2 + P_3 + P_4$ with the P_i's all k-rational. By [HLT04], C has a rational point P. After a linear change of coordinates, we may assume $P = (0 : 1 : 0)$ and the tangent line to C at P is the line $\ell^\infty = z$. Then C has neither a y^4 nor an xy^3 term, so C has the form $ax^2y^2 + bx^3y + cx^4 + z(\text{degree} \leq 3 \text{ terms})$. The line $\ell^\infty = z$ cannot intersect C at four rational points, so we must have $ay^2 + bxy + cx^2$ an irreducible conic and a is nonzero. Fix some nonsquare element $\alpha \in \mathbb{F}_p$. Then after transforming $y \to y - \frac{b}{2a}x$ we may take $b = 0$, and after rescaling the x axis we may assume that $a = 1$ and $c = -\alpha$. Thus C has the form $x^2y^2 - \alpha x^4 + z(k_1xy^2 + k_2x^2y + \text{other degree } \leq 3 \text{ terms})$. We may transform $x \to x - \frac{k_1}{2}z$ and $y \to y - \frac{k_2}{2}z$ to eliminate the xy^2z and x^2yz terms. Finally, since C is smooth and the tangent line to C at $(0 : 1 : 0)$ is z, we see that C has a zy^3 term. Then rescaling the z axis, we may assume that the coefficient of zy^3 is 1. Thus C has the form

$$y^3 + x^2y^2 - \alpha x^4 + c_1x^3 + c_2y^2 + c_3yx + c_4x^2 + c_5y + c_6x + c_7 \tag{4}$$

Furthermore, such a representation is unique up to linear change of coordinates, the choice of the initial rational point P on C, and the choice of α.

Thus we need to check no more than p^7 possibilities for C. The largest value of p with which we are concerned is 113 (the largest prime less than 127). If a single processor core can check each curve in under 100 nanoseconds on average (which we will show is reasonable), then the search with $p = 113$ will conclude within a year (less if multiple cores are used, since parallelizing this brute force search is trivial).

Let C have the form (4), and suppose there is no line ℓ which intersects C at four rational points. Then the only infinite point on C is $(0 : 1 : 0)$. Let $(x_0 : y_1 : 1)$ and $(x_0 : y_2 : 1)$ be two affine points on C with the same x coordinate. Then the line $x - x_0 z$ passes through three rational points on C, hence passes through a fourth rational point, a contradiction. Thus C has at most p affine points, no two of which share an x coordinate. This leads to the following algorithm.

Algorithm 16.1. Precompute a table of all monic cubics and their distinct roots. Precompute a table of all quadratics and their distinct roots. Precompute a table of inverses mod p. Then for each curve C in the form of (4)

1. For each x_0 in $\mathbb{F}_p$, compute the coefficients of the monic cubic $f(y) = C(x_0, y, 1)$. Look up f in the table of monic cubics. If f has multiple roots, then there are multiple points with x coordinate x_0 and we reject C. If f has one root y_0, then $(x_0 : y_0 : 1)$ is the unique point on C with x coordinate x_0. If f has no roots, there is no point with x coordinate x_0 on C.

2. For each x_0 in $\mathbb{F}_p$ such that there is a y_0 with $P = (x_0 : y_0 : 1)$ on C, compute the tangent line ℓ to C at P. If $\ell = 0$, reject C. If ℓ is vertical, reject C. Let $r(x) = \mathrm{res}_y(C, \ell)/(x - x_0)^2$. If $\deg(r) < 2$, reject C. Look up r in the table of quadratics. If r has at least one root, reject C.

3. For each $x_1 \neq x_2$ in $\mathbb{F}_p$ such that there are y_1, y_2 with $P_1 = (x_1 : y_1 : 1)$, $P_2 = (x_2 : y_2 : 1)$ on C, compute the line ℓ through P_1 and P_2. Let $r(x) = \mathrm{res}_y(C, \ell)/(x - x_1)(x - x_2)$. If $\deg(r) < 2$, reject C. Look up r in the table of quadratics. If r has at least one root, reject C.

4. Use a computer algebra system to check if C is smooth and irreducible. If not, reject C.

5. Output C.

While step 4 may take much longer than 100 nanoseconds, step 1 only requires a handful of operations and array lookups, and in practice most curves are eliminated in step 1. When $p = 31$, we find that 183 536 curves reach step 4, and when $p = 37$ we find that only 49 282 curves reach step 4. The number of curves that reach step 4 seems to drop off quite rapidly–with $p = 41$ the number is 17 342, and with $p = 43$ the number is 8 830. The author's current implementation is able to achieve an average of 100 nanoseconds per curve, and has found curves with no line ℓ for p as high as 73.

A similar search approach could be used to look for curves with no rational tangent, but the bound for the existence of such a tangent is much larger ($p \geq 66^2 + 1$) and we would not expect to find all such curves in a reasonable amount of time.

References

[FOR08] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler. "Fast addition on non-hyperelliptic genus 3 curves". In: *Algebraic Geometry And Its Applications: Dedicated to Gilles Lachaud on His 60th Birthday*. World Scientific, 2008, pp. 1–28.

[HLT04] Everett W Howe, Kristin E Lauter, and Jaap Top. "Pointless curves of genus three and four". In: *arXiv preprint math/0403178* (2004).

[KS08] Kiran S Kedlaya and Andrew V Sutherland. "Computing L-series of hyperelliptic curves". In: *International Algorithmic Number Theory Symposium*. Springer. 2008, pp. 312–326.

[OR10] Roger Oyono and Christophe Ritzenthaler. "On rationality of the intersection points of a line with a plane quartic". In: *International Workshop on the Arithmetic of Finite Fields*. Springer. 2010, pp. 224–237.