LIFTING PROBLEMS, CROSS-FIBEREDNESS, AND DIFFUSIVE PROPERTIES ON ELLIPTIC SURFACES

by

William H. George

A thesis submitted in conformity with the requirements for the degree of Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto

© Copyright 2015 by William H. George
Abstract

Lifting Problems, Cross-fiberedness, and Diffusive Properties on Elliptic Surfaces

William H. George
Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto
2015

Given an elliptic curve $\tilde{E}$ over $\mathbb{F}_p$ the field of $p$ elements, and given points $\tilde{P}$ and $\tilde{Q}$ in $\tilde{E}(\mathbb{F}_p)$ such that $\tilde{Q} = n\tilde{P}$, the Elliptic Curve Discrete Logarithm Problem (ECDLP) is to find $n$. The difficulty of the ECDLP is the foundation for much of modern cryptographic security. S. Miri and V.K. Murty considered a lifting problem in which one asks to find lifts of points $P \in \tilde{E}(\mathbb{F}_p)$ to an appropriately chosen elliptic curve over $\mathbb{Q}$. They saw that the ECDLP would be equivalent to this lifting problem if one could find lifts of $\tilde{E}$ with certain properties. We consider a variant of this lifting problem, which we see is unconjecturally equivalent to the ECDLP.

Furthermore, we relate these ideas to a conjecture of B. Mazur which asserts that for any non-constant elliptic fibration $\{E_t\}_{t \in \mathbb{Q}}$, the set $\{t \in \mathbb{Q} : rk(E_t(\mathbb{Q})) > 0\}$ is finite or dense in $\mathbb{R}$ with respect to the real topology. Particularly interesting to us are elliptic surfaces considered by R. Munshi on which there is a second fibration by genus one curves such that the two fibrations interact in nice ways. On these surfaces, using the second fibration, non-torsion points are “diffused” from one fiber $E_t$ to others, and hence positive rank fibers are “diffused” through $\mathbb{R}$, allowing one to conclude Mazur’s conjecture for these families. We show that this process also “diffuses” certain other properties of fibers. We see that, under certain conditions, the set of fibers having a list of properties motivated by our lifting problems is either finite or dense in $\mathbb{R}$. Moreover, we study the dynamics of this process of diffusion, allowing us to bound the proportion of times our process produces fibers with the desired properties. We show that the probability that the diffusion process produces a lift with all of the (seemingly unrelated) properties
is the product of each of the respective probabilities up to a controllable error bound. Hence we see that whether the output fiber of the diffusion process has these properties is “asymptotically independent.”
Dedication

To my mother.
In memory of my father.

Acknowledgements

First and foremost, I am indebted to my advisor V. Kumar Murty without whom this thesis would not have been possible. I am grateful for his guidance, his patience, and the confidence he has shown in me and in my work.

I thank my external examiner Joseph Silverman as well as the members of my supervisory committee, Henry Kim and Stephen Kudla, for their comments, helpful criticisms, and suggestions.

I would like to thank all of the members of the Ganita seminar group who have listened to me, provided me with useful discussions, and encouraged me over the years. Included in this group are Catalina Anghel, Robert Burko, Aaron Chow, Anup Dixit, Payman Eskandari, Jack Klys, Nataliya Laptyeva, Meng Fai Lim, Mariam Mourtada, Gaurav Patil, Pramathanath Sastry, Ramarathnam Venkatesan, Ren Zhu, and Ying Zong. I would particularly like to thank Ramarathnam Venkatesan for the direction that he provided me when I was first developing the problems that make up this thesis.

The staff members of the mathematics department are outstandingly organized and helpful, and I am grateful for the assistance that they have provided me in critical moments in my life, from gathering documents for immigration to preparing for my defense.

I would like to express my appreciation to the Knox College community for the home it has provided me with these past years. Among the people that I have met there, I would particularly like to thank Lelia Fry, Pierre Mailly, Jeanne Mathieu-Lessard, and Julie St-Laurent for their friendship and their moral support. I thank Stephen Brown and Grace Lin for providing me with a quiet place to work when I was stressed and working out the last elements of my proofs. I thank Tianna Uchacz for her invaluable help in editing, her help with the figures, and her friendship.

Finally, I cannot even begin to adequately thank my parents. I could never have come to this point without their support.
Contents

1 Introduction

1.1 The Rank One Lifting Problem ........................................ 1
  1.1.1 Preliminaries .................................................. 1
  1.1.2 The Rank One Lifting Problem and the ECDLP ............. 4
  1.1.3 Previous efforts toward the R1LH ......................... 10

1.2 Diffusion .......................................................... 12

1.3 Statement of results ................................................ 17
  1.3.1 The Rank One Surface Lifting Problem .................... 17
  1.3.2 Diffusion of candidate lifts ................................. 19

2 Computational precision in the R1LP ................................ 27

3 A variant on the R1LP ................................................. 31

3.1 Important background theorems ................................... 31

3.2 Packaging rational lifts together into a surface ............... 32

3.3 Equivalence of the R1SLP with the ECDLP ...................... 39

3.4 Some comments on the rank distribution of surface (1.2) .... 41
  3.4.1 A bound on the average rank of surface (1.2) ............ 42
  3.4.2 The average root number of surface (1.2) ................ 43

4 Diffusion of candidate lifts on cross-fibered surfaces .......... 47

4.1 Cross-fibered surfaces ............................................ 47
  4.1.1 Showing that a surface is cross-fibered .................. 52
  4.1.2 Examples of cross-fibered surfaces ....................... 59
  4.1.3 Comments on elliptic surfaces with multiple fibrations . 68

4.2 The probability that $t_{n,m} \in I$ ................................ 70

4.3 Other diffusive properties on cross-fibered surfaces ........ 92
  4.3.1 Candidate lifts ............................................... 93
Chapter 1

Introduction

1.1 The Rank One Lifting Problem

1.1.1 Preliminaries

Recall the Elliptic Curve Discrete Logarithm Problem (ECDLP).

Problem 1.1.1 (ECDLP).

Given: an elliptic curve $\tilde{E}$ over a finite field $\mathbb{F}_p$ of $p$ elements and two points $\tilde{P}, \tilde{Q}$ in $\tilde{E}(\mathbb{F}_p)$ such that $\tilde{Q}$ is in the (sub)group generated by $\tilde{P}$

Find: $n$ such that $\tilde{Q} = n\tilde{P}$ and $n \leq \#\tilde{E}(\mathbb{F}_p)$

We write $ECDLP(\tilde{E}, p, \tilde{P}, \tilde{Q}) = n$.

The computational difficulty of solving the ECDLP is the foundation for the security of elliptic curve cryptography, and particularly for the security of important and widely used digital signatures and key exchange schemes (see [10] and [11]).

There have been many attempts to attack the ECDLP via lifting methods. (For a summary of these attempts see [34]). In attempting to lift to non-torsion points on curves over global fields, the most studied approach is to try to find an index calculus attack. Namely, one lifts random points until one has more lifted points than the rank of the (global) curve, and hence the points have a dependency relation that can be reduced to

\footnote{The requirement that $n \leq \#\tilde{E}(\mathbb{F}_p)$ is somewhat non-standard. As one can efficiently compute $\#\tilde{E}(\mathbb{F}_p)$ by Schoof’s algorithm, given any $n$ such that $\tilde{Q} = n\tilde{P}$, one can reduce to find an $n$ satisfying our requirements. However, as we will be considering reductions from other problems to the ECDLP (see below), it will be important that we know, a priori, that the $n$ produced by an ECDLP oracle is of manageable size.}
the original curve. One wants to lift to a curve of relatively large rank so that the heights of the lifted points will be small enough that they can be efficiently worked with.

An alternative approach, which has been considered by Miri and Murty in [23] and later by Cheng and Huang in [5], is to search for rank one lifts. Here lifted points will generally have very large heights, but one can solve the ECDLP given only the heights of lifted points without having to work with the points themselves. We will develop these ideas.

As we care about the efficiency with which we can solve problems like the ECDLP, we begin by recalling notions involving the of running times of algorithms. We think of an algorithm as a Turing machine performing a set of instructions designed to solve a problem. Then, we will always use a logarithmic bit cost model in which each instruction executed by the machine (such as addition or entering an input number) is assigned a cost proportional to the number of bits that are involved in the computation. More precisely, the cost function measures the total number of distinct memory locations accessed during the procedure weighted by the number of bits of the values contained in these locations (see [2, Section 1.1]). Thus, doing arithmetic operations with numbers with many digits will be seen as having a higher cost than arithmetic operations with numbers with fewer digits. This is a standard perspective for cryptographic problems, but it is particularly important in our case as the lifting problems we consider will often involve lifted points whose coordinates can only be expressed with many bits and should be thought of as being difficult to work with.

We define:

**Definition 1.1.2.** A function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ is said to be “good” if $f(x) \geq 2x + \ln 2$ for all (positive) $x$.

Our choice of $f$ will be a reflection of the computing power that is available to us. We will measure the number of steps of our algorithms, the sizes of lifts that we allow, and the precision with which we can access the heights of these lifts all in terms of $f$. The choice of the exact condition defining “good” will become clear below.

Generally, our scale for what is a large number is provided by a prime $p$ such as that which is inputed in Problem 1.1.1. Then, as $p$ has bit size proportional to $\ln p$, it makes sense to measure the running times of an algorithm in terms of $f(\ln p)$. We will often say that a problem can be solved via a procedure that “runs in $O(f(\ln p))$ many steps” or “runs in $O(f(\ln p))$ time.” When we say that a procedure “runs in $O(n)$ many steps,” we mean that there exists some machine which, given any instance (from some previously specified set of allowable inputs) of the problem, returns an output solving the problem.
such that the step cost of the procedure is bounded by $O(n)$. Similarly, when we say that a procedure “runs in $O(f(n))$ time,” we mean that there exists a machine which, given any instance whose input size is less than (some fixed multiple times) $n$, returns an output solving the problem such that the step cost of the procedure is bounded by $O(f(n))$. The constants in the $O$’s here should not depend on $n$, but we may specify other quantities on which they depend.

We say that problem $A$ can be reduced to problem $B$ if there is an algorithm which, given an access to an oracle that can produce, as the result of an instruction, solutions to problem $B$ (whose inputs have been entered into memory), produces a solution to problem $A$. (For a precise definition of oracle-Turing machines, see [2, Section 1.3].) We talk about the running times of such reductions as above; namely, that a reduction “runs in $O(n)$ many steps” if the step cost of the oracle Turing machine performing this reduction is bounded by $O(n)$. We similarly say that a reduction “runs in $O(f(n))$ time” if the oracle Turing machine returns an output solving the problem such that the step cost of the procedure is bounded by $O(f(n))$ given any instance whose input size is less than (some fixed multiple times) $n$. Then, we say that problems $A$ and $B$ are equivalent if there are reductions from $A$ to $B$ and from $B$ to $A$. The running time of the equivalence is the maximum of the running times of the two reductions.

Recall that on the rational numbers, we have a notion of height given by:

$$H\left(\frac{a}{b}\right) = \max \{|a|, |b|\},$$

where $\gcd(a, b) = 1$ (see [39, Section 8.4]). So, when we use a non-zero rational number $\frac{a}{b}$ in an algorithm, its size is (proportional to) $\ln H\left(\frac{a}{b}\right)$.

We will also make use the canonical height on elliptic curves over $\mathbb{Q}$. The key properties of the canonical height that we will use are that it can be quickly computed (see, for example, [37]) and that

$$\hat{h}(nP) = n^2\hat{h}(P) \text{ (see [39] Ch. 8, Theorem 9.3.b)},$$

(1.1)

which relates the multiplicative structure of the group of points closely to the height. However, this property also forces the size of multiples of a point to grow very quickly as $n$ grows.
1.1.2 The Rank One Lifting Problem and the ECDLP

Miri and Murty in [23] considered the problem of lifting points on an elliptic curve $\tilde{E}$ over $\mathbb{F}_p$ for some prime $p$ to a fixed lift $E$ of $\tilde{E}$ over $\mathbb{Q}$. We state a version of their problem in height-theoretic terms.

**Problem 1.1.3** (Rank One Lifting Problem, R1LP).

**Given:**

- $f$ a good function
- $\tilde{E}$ an elliptic curve over $\mathbb{F}_p$
- $E$ an elliptic curve over $\mathbb{Q}$ of rank one such that the reduction of $E$ mod $p$ is $\tilde{E}$
- $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$
- $\epsilon > 0$
- $W \in E(\mathbb{Q})$ such that $W$ does not reduce to zero mod $p$
- $h_W \in \mathbb{Q}$ such that $|\hat{h}(W) - h_W| < \frac{\epsilon}{4p^2}$ and the numerator of $h_W$ is at most $e^{f(\ln p)}$

such that the sizes of these entries (particularly the coefficients of $E$, the coordinates of $W$, and $h_W$) are all bounded by $f(\ln p)$

**Find:** $h \in \mathbb{Q}$ such that such that exists some $P \in E(\mathbb{Q})$ such that $P$ reduces to $\tilde{P}$ mod $p$, $|\hat{h}(P) - h| < \epsilon$, $h \leq 4p^2h_W$, and $H(h) \leq e^{f(\ln p)}$.

We write $R1LP(\tilde{E}, p, E, W, h_W, \tilde{P}, f, \epsilon) = h$.

Of course, it may not always be possible to solve the R1LP if there are no points on $E$ that lift a given $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$. However, it turns out that under reasonable, cryptographically common assumptions on $p$ and $\tilde{E}$ (see below), any $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$ can be lifted to some point on $E$. So, basically, given a point $\tilde{P}$ and a rank one curve on which one knows there is a lift of this point, the R1LP is to find (the height up to some error of) such a lift of reasonable size.

The idea of Miri and Murty ([23]) is that (under these cryptographically common assumptions $p$ and $\tilde{E}$) the ECDLP should be equivalent to the R1LP. We must stress that we do not know of any efficient algorithms to solve the R1LP. Particularly, due to the rate of growth of the canonical heights of multiples of points that we saw in equation (1.1), the heights of lifts of points to a rank one curve will generally be very large, and...
as a result even writing down such lifts will require exponential time in $\ln p$. Thus, we would expect that an efficient attack on the R1LP would require a way to get the heights of lifts without having to do computations with the lifts themselves. It is currently very unclear how one could find such an attack that does not pass through the ECDLP; however, an unconjectural equivalence between the ECDLP and the R1LP would add to our understanding of what makes the ECDLP difficult.

We give an example to illustrate the argument of Miri and Murty.

**Example 1.1.4.** Consider the elliptic curve over $\mathbb{F}_{31}$:

$$\tilde{E}: y^2 = x^3 + 8x + 19.$$  

Then we can compute $\#\tilde{E}(\mathbb{F}_{31}) = 23$ by Schoof’s algorithm.

Suppose we are given an instance of the ECDLP: $\tilde{P} = (3, 15)$ and $\tilde{Q} = (6, 2)$, and we want to find $n \pmod{\#\tilde{E}(\mathbb{F}_{31}) = 23}$ such that $\tilde{Q} = n\tilde{P}$.

Consider the lift of $\tilde{E}$ to $Q$:

$$E : y^2 = x^3 + 39x + 19.$$  

Using Sage version 6.1, we see that this curve has rank one.

Note that we have the point $W = (5351801892376857, 54767061301731095396245, 520896907214568426664296)$ on $E$. We see that $W$ reduces to $\tilde{W} = (30, 17) \not\equiv \tilde{O} \pmod{31}$ and $\hat{h}(W) \approx 36.719$.

Then suppose we can find lifts:

$$P = (243560690146329349038265586257531578305984360039466727417581258244691699336925965062072, 245743988794, 70060660610895836891375710389047682478550338767495278306200523232725367087477, 2667256185588554917569, 1058816359848131012890022254095401432485464663254224460652653097, 9655353796390259921711090631914826265306434855805556602281472951096627154077067191, 18544338, 32581853640255370461466863076696201803042008348798352868978676425427287395600084675515779548, 66208460910792526362870980503340516325703329694753)$$  

of $\tilde{P}$ which has height $\hat{h}(P) \approx 229.495$ and

$$Q = (1810126573433124726032976947973800972976465759333919988050780415843570371313880642761, 019561053820408917126522311232846626662802465407395728080034900920470063792872636343470320, 100526788665541267411904040824188644254308087702215880361094940326668348773885853048873942, 56114276115287238106360408704555096315769237682082514180407426422679013521481394042026203625, 067557087594734640667006294301729, 83447047098736207465415862221562824667121310861186147806, 9231007602690860923497553987665409414803666703390873781477692874595049656877097421792538, 7022072115244326934180086317279033563735353081810536698391406312616708667147646699702288397, 955710271705640286335889549612748248479783821089852771, 129879800070007451941721733440378528)$$  

of $\tilde{Q}$.
Chapter 1. Introduction

2054071543489615339249633169719667417358924202758398953707340117821924772976270603996438804
7682511874487326576521619151448689712736807210145099836062472120223072979365588849079741
68303685538334491567795692623785107342377164539462326112079944066056383567)
o of \( \tilde{Q} \), which has height \( \hat{h}(Q) \approx 449.810 \). Our computations of \( \hat{h}(W) \), \( \hat{h}(P) \), and \( \hat{h}(Q) \) were again performed using Sage version 6.1.

As we can see, the number of digits of these points does indeed become quite large even for very small \( p \). However, suppose we had a R1LP oracle that just gave us these heights:

\[
R_1LP(\tilde{E}, 31, E, W, 36.719, \tilde{P}, f) = 229.495
\]

and

\[
R_1LP(\tilde{E}, 31, E, W, 36.719, \tilde{Q}, f) = 449.810.
\]

Then, as \( P \) and \( Q \) are some (unknown) multiples of a generator \( R \) of the Mordell-Weil group \( E(\mathbb{Q}) \): \( P = n_1R \) and \( Q = n_2R \), we can compute

\[
\sqrt{\frac{\hat{h}(Q)}{\hat{h}(P)}} = \sqrt{\frac{n_2^2}{n_1^2}} = \frac{n_2}{n_1} \equiv n \mod \#\tilde{E}(\mathbb{F}_{31})
\]

\[
n \equiv \sqrt{\frac{449.810}{229.495}} \approx \sqrt{1.960} = 1.40 = \frac{7}{5} \equiv 7 \cdot 14 \equiv 6 \mod 23
\]

and we can check that indeed \( \tilde{Q} = 6\tilde{P} \). Note the \( \approx \) symbols here. We know that \( \sqrt{\frac{\hat{h}(Q)}{\hat{h}(P)}} \) is a priori a rational number, but the heights \( \hat{h}(P) \) and \( \hat{h}(Q) \) are generally irrational. Thus, we can only access approximations of them to a given precision, which is why we include \( \epsilon \) as an input in the R1LP. We will see how much precision is necessary to identify (the class mod \( p \) of) \( n \) below.

On the other hand, suppose we had an ECDLP oracle, and we wanted to find the height of a lift of \( \tilde{Q} = (6, 2) \). Then, we want to find a rational point whose reduction generates a subgroup that includes \( \tilde{Q} \); as \( \#\tilde{E}(\mathbb{F}_{31}) = 23 \) is prime we just need to find any rational point on \( E \) that does not reduce to zero, so \( W \) in particular works.

We saw that \( \hat{h}(W) \approx 36.719 \), and we find \( \text{ECDLP}(\tilde{E}, p, \tilde{W}, \tilde{Q}) = 15 \), so we can compute

\[
h_Q \equiv 15^2 \cdot \hat{h}(W) \approx 6011.775 \mod 23,
\]

which is (approximately) the height of the point \( 15 \cdot W \), which is a lift of \( \tilde{Q} \).

However, the choice of the rank one lift \( E \) over \( \mathbb{Q} \) can be problematic. Specifically,
taking $\phi$ to be the reduction map mod $p$, when $\phi(E(\mathbb{Q})) = \{\tilde{O}\}$, there is no clear relation between $\tilde{E}(\mathbb{F}_p)$ and $E(\mathbb{Q})$. A typical failure case would be if the rank one lift that is produced $E$ has trivial torsion group and $p$ divides the denominator of a generator for the non-torsion points. Indeed, if $E(\mathbb{Q}) = \langle R \rangle$ and $p$ divides the denominator of $R$, then $p$ divides the denominator of every point in $E(\mathbb{Q})$.

**Example 1.1.5.** In Example 1.1.4 we considered the curve $E : y^2 = x^3 + 39x + 19$ over $\mathbb{Q}$ that has rank one. Moreover, we can see that the rational points of this curve are generated by

$$(8754/289, -836549/4913) = (8754/17^2, -836549/17^3).$$

If we had tried to use this as a rank one lift of a curve over $\mathbb{F}_{17}$, we would have had that the generator of the rational points reduces to $\tilde{O}$, and thus all rational points reduce to $\tilde{O}$. Thus, our choice of $E$ would not have satisfied the R1LH and our argument above to prove the equivalence of ECDLP with R1LP would not have worked.

This motivates the definition:

**Definition 1.1.6.** We say that the reduction mod $p$, $\phi : E(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_p)$, is non-trivial if $E$ has good reduction at $p$ and $\phi(E(\mathbb{Q})) \neq \{\tilde{O}\}$. A given point $P \in E(\mathbb{Q})$ such that $\phi(P) \neq \tilde{O}$ is said to reduce non-trivially.

When the ECDLP is used for cryptographic applications, one generally assumes $\# \tilde{E}(\mathbb{F}_p)$ is prime. We will call such instances of ECDLP “cryptographic.” This assumption prevents one from solving the ECDLP in smaller groups and then using the Chinese Remainder Theorem to piece together a solution for the whole group. However, in the setting of cryptographic instances, there is a sharp dichotomy in what the reduction of the set of rational points on a lift can be. If there is a single point in $E(\mathbb{Q})$ that reduces to a non-zero point, then its multiples form a subgroup of $\tilde{E}(\mathbb{F}_p)$, which then must be the entire group. Thus, we have that $\phi(E(\mathbb{Q}))$ is either $\{\tilde{O}\}$ or all of $\tilde{E}(\mathbb{F}_p)$. Namely, all points in $\tilde{E}(\mathbb{F}_p)$ can be lifted to $E$ or only the zero point can be lifted.

However, when $\# \tilde{E}(\mathbb{F}_p)$ we also have:

**Proposition 1.1.7** (Lemma 1 of [23]). If $p > 23$ and $\tilde{E}$ is an elliptic curve over $\mathbb{F}_p$ with $\tilde{E}(\mathbb{F}_p)$ of prime order, then for any lift $E$ of $\tilde{E}$ to $\mathbb{Q}$, we have that $E_{\text{torsion}}(\mathbb{Q})$ is trivial.

Thus, for cryptographic instances of the ECDLP, if we have non-trivial reduction, it must be because there is some non-torsion point that does not reduce to zero.
In the event that we try a rank one lift that fails as a result of trivial reduction, we can hope that some other lift will work. Generally, we expect the probability that $p$ divides the denominator of the generator of the rational points of a given rank one lift to be about $\frac{1}{p}$ and thus unlikely for the large primes generally used in cryptographic applications. However, it is possible that there exists some collection of resistant instances of the ECDLP where this lift cannot quickly be found. Note that (as we will see) there are many lifts of a given curve mod $p$ that have rank one and many lifts that have non-trivial reduction, so for such resistant instances to exist would require the lifts that are rank one to be disproportionately likely to have rational points with $p$ in their denominator. This would imply a correlation between two rather distinct arithmetic properties, one of which is a mod $p$ property and the other of which is global. One of the themes of this work will be the circumstances under which we can prove that such properties “mix well.”

Remark 1.1.8. A naive thing we could try at this point would be to perform a substitution

$$x' = p^{2r}x, \quad y' = p^{3r}y$$

to produce another Weierstrass model $E'$ of our curve such that the generator of $E'(\mathbb{Q})$ is no longer divisible by $p$. However, by the substitution formulas of [39, Ch. 3, Table 1.2], the coordinates of $E'$ have $p$ in their denominator and $\Delta' = p^{-12r}\Delta$, thus this model has bad reduction mod $p$ and cannot be used for the R1LH. Thus, such a curve $E$ seems to have an intrinsic disconnect between its rational and mod $p$ points that persists even after doing available substitutions. (Even doing non-homogeneous substitutions $x = u^2x' + r$ with $r, s, t \neq 0$ does not help because the property that the new model be a lift forces $r, s \equiv 0 \mod p$. If we try to choose $r, u$ such that $v_p(u^2 \frac{2\gamma}{p^2} + r) \geq 0$ we need $v_p(u) = 0$ so that the model still has good reduction, but then $v_p(r) < 0$.)

If this phenomenon occurs, we could reasonably hope to find some other lift of $\tilde{E}$. Miri and Murty conjecture that “good” lifts always exist; namely, that there should be a solution to the following problem.

Problem 1.1.9 (Rank One Lifting Hypothesis, see [23], R1LH).

Given: $f$ a good function, $\tilde{E}$ an elliptic curve over $\mathbb{F}_p$, and $\delta \in \left(\frac{1}{2^f(\ln p)}, 1\right)$ (such that the sizes of these entries are bounded by $f(\ln p)$)

Find:

- $E$ a rank one curve over $\mathbb{Q}$ whose reduction mod $p$ is $\mathbb{F}_p$
Chapter 1. Introduction

9

• \( L \in \mathbb{Q} \) such that \( \hat{h}(P) \geq L \) for all non-torsion \( P \in E(\mathbb{Q}) \) and such that
\[
L \geq \frac{2p^2}{e^f(\ln p)}
\]

• \( W \in E(\mathbb{Q}) \) that reduces to a non-zero point mod \( p \) such that
\[
\hat{h}(W) \leq \frac{L2^{\sqrt{f(\ln p) + \ln(L) - \ln(8p^2)^\frac{-2}{4p^2}}}}{4p^2} - 1
\]

• \( h_W \in \mathbb{Q} \) such that \(|h_W - \hat{h}(W)| < \delta\).

The sizes of the coefficients of \( E, L \), the coordinates of \( W \), and \( h_W \) should be less than \( f(\ln p) \).

We write \( LH(\hat{E}, p, f, \delta) = (E, W, L, h_W) \).

**Conjecture 1.1.10** (Algorithmic Lifting Hypothesis). For \( p \) larger than some computable constant and for some good, sub-exponential function \( f \), there exists an algorithm that solves Problem 1.1.9 and that runs in \( f(\ln p) \) many steps.

We state this conjecture for a \( f \) sub-exponential because our aim is to show an equivalence between the ECDLP and the R1LP with running time in terms of \( f \), and there already exist exponential algorithms that attack the ECDLP. Various definitions of sub-exponential exist, and essentially we just want something that grows substantially slower than exponential functions, but for the sake of being explicit we say a function \( f(x) \) is sub-exponential if \( f(x) = 2^{o(x)} \) (see [18]).

The content of Conjecture 1.1.10 is mostly that one can algorithmically find \( E \) and \( W \) (of reasonable size). The point \( W \) is thought of as a “witness” that \( E \) does not have trivial reduction mod \( p \). Once these have been found one can compute a lower bound for the height on \( E \) using the methods of [9] and one can compute the canonical height of \( W \) to desired precision using the methods of [37]. In fact, according to Lang’s Conjecture, one should have a lower bound on the heights of non-torsion points in terms of the discriminant of the curve.

**Conjecture 1.1.11** (Lang, see [16]). There is a constant \( c > 0 \) such that for all elliptic curves \( E/\mathbb{Q} \) and all non-torsion points \( P \in E(\mathbb{Q}) \),
\[
\hat{h}(P) \geq c \ln |\Delta|
\]
where \( \Delta \) is the minimal discriminant of \( E \).

If Lang’s Conjecture is true, computing \( L \) would be particularly straightforward. We need \( L \geq \frac{2p^2}{e^f(\ln p)} \) so that \( L \) can be written down with our level of computational precision. Below we will sometimes assume that \( L \leq 1 \) without loss of generality, which is not
contradictory as \( f \) is good. We demand the above bound on \( \hat{h}(W) \) because, as we saw in Example 1.1.4, we will be working with the heights of large multiples of \( W \), and we want these heights to still be small enough so that the computations we want to do with them are manageable. We are only allowed to choose \( \delta > \frac{1}{2e f(ln p)} \) because, if \( \delta \) is very small, we are demanding that \( h_W \) approximate a potentially irrational number \( \hat{h}(W) \) to very high precision, which may not be possible respecting the bounds on the sizes of the outputs and could cause \( LH(\tilde{E}, p, f, \delta) \) to be unsolvable. Note that \( \frac{1}{2e f(ln p)} < 1 \) because \( f \) is good and that \( \delta < 1 \) implies \( h_W \leq 4L^22\sqrt{f(ln p)+ln(ln p)-ln(8p^2)}-2-\frac{1}{2p^2} \).

In practice, for most \( \tilde{E} \) and \( p \), finding a lift satisfying Problem 1.1.9 seems to be easy. In fact, if one takes random lifts of \( \tilde{E} \), one will usually find a satisfactory lift relatively quickly. However, finding an algorithm that is guaranteed to produce such a lift for any choice of \( \tilde{E} \) and \( p \) has been surprisingly difficult. In fact, it is not yet known that a lift satisfying Problem 1.1.9 even exists for all instances of ECDLP. In this work, we will establish partial results toward such an algorithm. We will review in Section 1.1.3 previous efforts to find such curves. Ultimately, these efforts have either applied to very special cases, or they have required some kind of conjecture about the distribution of ranks in some family of curves. In Chapter 3 we will considerably weaken the kinds of rank distributional conjectures necessary, and in Chapter 4 we will relate this problem to a natural generalization of a conjecture of Mazur for elliptic surfaces.

Then, assuming a lift satisfying the R1LH can be found, Miri and Murty indeed showed the equivalence of ECDLP and R1LP (see [23, Propositions 4 and 5]). We state a version of this result in which we have made explicit the running time of the equivalence. We perform the necessary analysis of the running time in Chapter 2.

Theorem 1.1.12. Assume Conjecture 1.1.10 holds for some good sub-exponential function \( f \). Let \( p > 23 \) and \( \tilde{E} \) an elliptic curve over \( \mathbb{F}_p \) such that \#\( \tilde{E}(\mathbb{F}_p) = l \) is prime. Compute \( LH(\tilde{E}, p, f, \frac{1}{2e f(ln p)}) = (E, W, L, h_W) \). Then, there is an equivalence between \( R1LP(\tilde{E}, p, E, W, h_W, -, f, \frac{p^2}{e f(ln p)}) \) and \( ECDLP(\tilde{E}, p, -, -) \) that runs in \( \max \{O(f(ln p)), \text{poly}(ln p)\} \) many steps for some fixed polynomial \( \text{poly} \) and where the constant in the \( O \) is absolute.

1.1.3 Previous efforts toward the R1LH

Average values of \( L \)-functions

Miri and Murty tried to find lifts satisfying Problem 1.1.9 by considering an average of values of derivatives of \( L \)-functions. More precisely, if \( \tilde{E} \) is the curve over \( \mathbb{F}_p \) that one
wants to lift, they take any lift

\[ E : y^2 = x^3 + ax + b \]

of \( \tilde{E} \) (not necessarily satisfying the other conditions of Problem [1.1.9]), and then, for any \( t \in \mathbb{Q} \), they consider the quadratic twist of \( E \) by \( t \),

\[ E_t : ty^2 = x^3 + ax + b. \]

Then, they average over values of the derivatives of the \( L \)-functions of the twists as \( t \) varies. By this argument, and using an asymptotic from a paper of Murty and Murty, they produce a lift of analytic rank one. Then, by Kolyvagin’s Theorem, this curve has actual rank one. However, it is difficult to get control over the denominators of the rational points on the lift constructed; hence, the lift could not be shown to satisfy the property that there is a point which does not reduce to zero mod \( p \).

In Section 6 of their paper, it was shown that, assuming the Riemann hypothesis, if the twist \( E_t \) produced by the averaging argument is such that \( t \ll (\ln p)^{2-\epsilon} \), then there must be a point on \( E_t \) whose denominator must be smaller than \( p \) and hence not divisible by \( p \). However, using these methods to achieve a lift with \( t \) on this order would require a much faster rate of convergence for the average of derivatives of \( L \)-functions than what is currently available.

**Producing lifts for which the Selmer rank is bounded**

Cheon, Lee, and Hahn (in [6]) have a method to look for rank one lifts (towards the same ECDLP ends) with non-trivial 2-torsion. Recalling that there is an upper bound on rank of curves of the form

\[ y^2 = x(x^2 + ax + b) \]

(note that any such curve has the 2-torsion point \((0,0)\)) in terms of the number of prime factors of \( b \) and \( a^2 - 4b \), one searches for lifts where these quantities have as few prime factors as possible. In particular, in cases where one can choose lifts where both of these quantities are prime, this curve has rank one.

Their work is pursued by Yasuda in [47] in analyzing the Selmer ranks of their proposed lifts. Assuming the Shafarevich-Tate Conjecture, he managed to construct lifts of bounded rank, but he could not get this bound all the way down to one.

**Remark 1.1.13.** Note, the motivation given by Miri and Murty is incompatible with having non-trivial torsion by Proposition [1.1.7]
Randomly choosing lifts among a family

In the work of Cheng and Huang [5], one looks for lifts satisfying Problem 1.1.9 among the fibers of a certain surface. Suppose that we have an elliptic curve

\[ \tilde{E} : y^2 = x^3 + \tilde{a}x + \tilde{b} \]

over \( \mathbb{F}_p \) that we want to lift. Then fix some non-zero point \((\tilde{x}_0, \tilde{y}_0) \in \tilde{E}(\mathbb{F}_p)\) and choose rational numbers \(a, x_0, \) and \(y_0\) that reduce to \(\tilde{a}, \tilde{x}_0,\) and \(\tilde{y}_0\) respectively. Then Cheng and Huang consider the surface

\[ E_t : y^2 = x^3 + (a + tp)x + (y_0^2 - x_0^3 - (a + tp)x_0) \quad (1.2) \]

over \( \mathbb{Q} \) where \(y_0^2 \equiv x_0^3 + ax_0 + b \mod p\). All fibers of this surface, except those such that \(p\) divides the denominator of \(t\), are rational lifts of \(y^2 = x^3 + ax + b\) over \( \mathbb{F}_p \) containing the non-trivially reducing rational point \((x_0, y_0)\).

Again if one assumes \#\(\tilde{E}(\mathbb{F}_p)\) is prime and \(p > 23\), by Proposition 1.1.7 all non-zero points on a lift must be non-torsion; hence, all of these fibers (such that \(p \nmid \text{den}(t)\)) have rank at least 1, as \((x_0, y_0)\) considered in \(\mathbb{Q}[t]^2\) is a non-torsion section on this surface.

Cheng and Huang note that, appealing to a folkloric conjecture on rank distribution, for a random choice of integer \(t\) one expects to yield a rank one curve with probability \(1/2\) and a rank two curve with probability \(1/2\). Thus, with probability half one chooses an acceptable lift.

1.2 Diffusion

Mazur in [21] explores the structure of the closure of the rational points of varieties. In particular, he considers situations in which the presence of a single rational point in a connected component of an algebraic variety forces rational points to be dense in this component under the real topology. Thus, he looks at relations between the real and the Zariski topology. He conjectures:

Conjecture 1.2.1 (Conjecture 1 of [21]). Let \(V\) be a smooth variety over \(\mathbb{Q}\) such that \(V(\mathbb{Q})\) is Zariski dense in \(V\). Then, the topological closure of \(V(\mathbb{Q})\) in \(V(\mathbb{R})\) consists of a finite union of connected components of \(V(\mathbb{R})\).

It is proved in [8] that Conjecture 1.2.1 is actually false in this generality. However, they propose the following weakened version which remains open:
Conjecture 1.2.2 (Conjecture 5 of [8]). Let $V$ be a smooth, integral variety over $\mathbb{Q}$, and let $U$ be a connected component of $V(\mathbb{R})$. If $V(\mathbb{Q}) \cap U$ is Zariski dense in $V$, then it is dense in the real topology in $U$.

Furthermore, many special cases of these conjectures are known, and the following partial result is known in the setting of abelian varieties:

Theorem 1.2.3 (Theorem 3.2 of [45]). If $A$ is a simple abelian variety over $\mathbb{Q}$ of dimension $d$ and the rank of $A(\mathbb{Q})$ is at least $d^2 - d + 1$, then the closure of $A(\mathbb{Q})$ in the Euclidean topology contains the connected component of the identity: $A(\mathbb{R})^0$.

Particularly, as elliptic curves are simple one dimensional varieties, Theorem 1.2.3 applies to any elliptic curve of rank at least one. One can see:

Proposition 1.2.4 (Proposition 1.1 from Chapter 2 of [44]). Let $E$ be an elliptic curve over $\mathbb{R}$, $\gamma$ a point of infinite order in $E(\mathbb{R})$, and $\Gamma = \mathbb{Z} \gamma$ the subgroup generated by $\gamma$. Then the closure of $\Gamma$ in $E(\mathbb{R})$ in the real topology is either $E^0(\mathbb{R})$ or $E(\mathbb{R})$; namely, the identity component of $E(\mathbb{R})$ or all of $E(\mathbb{R})$.

In fact, as noted in [44], Proposition 1.2.4 can be seen to follow in a relatively straightforward way from:

Theorem 1.2.5 (Chebyshev, see for example Theorem 1.1 from Chapter 1 of [44]). Let $\theta$ be an irrational number. Then the subgroup $\mathbb{Z} + \mathbb{Z} \theta$ of $\mathbb{R}$ is dense in $\mathbb{R}$.

We recall the definition:

Definition 1.2.6 (See Section 3 of [32]). Take $C$ to be a smooth projective curve. An elliptic surface $\mathcal{E}$ over $C$ is a smooth projective surface with an elliptic fibration over $C$, i.e. a surjective morphism

$$\pi : \mathcal{E} \to C$$

such that

- almost all fibers are smooth curves of genus 1
- no fiber contains a curve of self-intersection number $-1$
- there exists a section on $\mathcal{E}$, namely a morphism

$$\iota : C \to \mathcal{E}$$

such that $\pi \circ \iota = \text{id}_C$. 

Our elliptic surfaces will always be over $C = \mathbb{P}^1$, the projective line. For simplicity, we will always work over fields of characteristic not equal to 2 or 3. Then a Weierstrass equation over $\mathbb{Q}(t)$: $y^2 = x^3 + a_4(t)x + a_6(t)$ yields an elliptic surface by taking the Zariski closure of the set

$$\left\{ ([X,Y,Z], t) \in \mathbb{P}^2 \times \mathbb{P}^1 : t \neq \infty, ZY^2 = X^3 + a_4(t)XZ^2 + a_6(t)Z^3 \right\}$$

and resolving the singular points via Tate’s Algorithm and repeatedly blowing them up (see [32, Section 4]). When we talk about the elliptic surface given by a Weierstrass equation, we mean the surface resulting from this procedure.

Mazur considers the consequences of Conjecture 1.2.1 for elliptic surfaces. Particularly, he shows it would imply:

**Conjecture 1.2.7** (Conjecture 4 of [21]). Suppose $\{E_t\}$ is an elliptic fibration over $\mathbb{Q}$ with projection to $\mathbb{P}^1(\mathbb{Q})$. Then either:

- $\{t \in \mathbb{Q} : rk(E_t(\mathbb{Q})) \geq 1\}$ is dense in $\mathbb{P}^1(\mathbb{R})$, or
- $\{t \in \mathbb{Q} : rk(E_t(\mathbb{Q})) \geq 1\}$ is finite.

Note that even though Conjecture 1.2.1 was seen to be false, later work on special cases of Conjecture 1.2.7 have still expressed the belief that Conjecture 1.2.7 should be true (see [24] and [25]). Moreover, the weakened version of Mazur’s Conjecture proposed by [8] would still imply Conjecture 1.2.7. We briefly note this argument:

**Conjecture 1.2.2 implies Conjecture 1.2.7**. We proceed as in [21]. Take $S$ to be the minimal regular model of the elliptic surface corresponding to this family. Assume that there are infinitely many values of $t$ such that $rk(E_t(\mathbb{Q})) \geq 1$. Let $\Sigma$ denote the connected component of the real locus of $S$ that contains the zero section. Note that by Proposition 1.2.4, the real points of each positive rank fiber are dense on its identity component. Thus, the real points on the identity component for each of our infinitely many fibers of positive rank are in $\Sigma$. As each of these fibers is an irreducible curve, the Zariski closure of $\Sigma(\mathbb{Q})$ must contain all of these fibers; hence, $S(\mathbb{Q}) \cap \Sigma$ is Zariski dense in $S$. Then, by Conjecture 1.2.2, the rational points of $\Sigma$ are dense in $\Sigma$ in the real topology. One then continues exactly as in [21].

As Mazur remarks in [21], this conjecture would say that the property of having positive rank exhibits a sort of “contagion” in that the presence of a single fiber of
positive rank forces them to be dense. While Conjecture 1.2.7 is known in some special cases (some of which we will look at in detail), in general it remains open.

There is a folkloric belief (see the remarks in Section 3.4 and recent work of Bhargava and Shankar in [3] where this belief is partially fulfilled) that, on average, elliptic curves in a given family will tend to have the lowest rank “possible.” Specifically, one expects that there are very few fibers on an elliptic surface with rank significantly larger than the generic rank of the surface; however, this kind of behavior would only be true asymptotically (under some kind of ordering). In contrast, very sparse sets can be dense in the sense of Conjecture 1.2.7. This prompts us to ask:

**Question 1.2.8 (Rank N Mazur’s Conjecture - RNMC).** For what elliptic fibrations over \( \mathbb{Q} \) does one have either:

- \( \{ t \in \mathbb{Q} : \text{rk}(E_t(\mathbb{Q})) \geq N \} \) is dense in \( \mathbb{R} \), or
- \( \{ t \in \mathbb{Q} : \text{rk}(E_t(\mathbb{Q})) \geq N \} \) is finite?

In this direction one has:

**Proposition 1.2.9 (Proposition 9(ii) of [30]).** Let

\[
E : y^2 = x^3 + ax + b
\]

be an elliptic curve over \( \mathbb{Q} \) such that either

- \( E \) acquires good reduction mod 2 over some abelian extension of \( \mathbb{Q}_2 \)

or

- \( E \) has potentially multiplicative reduction at \( p = 2 \)

There exists an irreducible quadratic polynomial \( f(t) \) such that the surface

\[
E_t : f(t)y^2 = x^3 + ax + b
\]

- has generic rank 0
- \( E_t \) has positive rank for a dense set of \( t \in \mathbb{Q} \) (i.e. \( E_t \) satisfies Conjecture 1.2.7)
- \( W(E_t) = 1 \) for all \( t \in \mathbb{Q} \).

Thus, if one assumes the parity conjecture, one has R2MC for this surface.
Here \( W(E_t) \) is the root number of the fiber \( E_t \). (For a more detailed discussion of root numbers and the parity conjecture see Section 3.4).

For some of the known cases of Conjecture 1.2.7, as proved in [24], [25], and [30], the proofs take the form of an iterative process used to “spread” or “diffuse” rational points from one fiber to others. We notice that this process often preserves other properties of the initial fiber as well prompting us to define:

**Definition 1.2.10.** Let \( P \) be a property of elliptic curves. Then \( P \) is said to be “diffusive” if for all elliptic fibrations over \( \mathbb{Q} \) one has either:

- \( \{ t \in \mathbb{Q} : E_t \text{ has property } P \} \) is dense in \( \mathbb{R} \), or
- \( \{ t \in \mathbb{Q} : E_t \text{ has property } P \} \) is finite.

Furthermore, \( P \) is said to be diffusive on some class of elliptic fibrations if this dichotomy holds for all fibrations in the class.

Note that there exist arithmetically interesting properties that are not diffusive. Rohrlich ([30]) and Rizzo ([29]) consider the variation of the root number among the fibers of certain elliptic fibrations. Rohrlich shows:

**Theorem 1.2.11** (Theorem 2 of [30]). Let \( E \) be an elliptic curve. For a given polynomial we consider the elliptic surface:

\[
E_t : f(t)y^2 = x^3 + ax + b
\]

and consider

\[
T^\pm = \{ t \in \mathbb{Q} : W(E_t) = \pm 1 \}
\]

Then, there exists a polynomial \( f(t) \) such that the number of sign changes exceeds any preassigned value and such that one of the sets \( T^\pm \) is \( \{ t \in \mathbb{Q} : f(t) > 0 \} \) and the other is \( \{ t \in \mathbb{Q} : f(t) < 0 \} \).

So in our terminology we have:

**Corollary 1.2.12.** We say that an elliptic curve has property \( P \) if its root number is \( +1 \). Then for the property \( P \) and the surfaces of Theorem 1.2.11 where \( f \) has at least one sign change, the dichotomy of Definition 1.2.10 does not hold. Namely, the property of having root number \( +1 \) is not diffusive for these surfaces. Similarly the property of having root number \( -1 \) is also not diffusive for such surfaces.
However, (again, for certain of the elliptic surfaces for which Mazur’s Conjecture was proven in [24], [25], and [30]) we will be able to show that many of the properties we demand of our lifts in Conjecture [1.1.10] are “spread” by the same process used to “spread” the property of having positive rank, and hence these properties are diffusive on the class of such surfaces. See Section [1.3.2] for our results in this direction.

1.3 Statement of results

1.3.1 The Rank One Surface Lifting Problem

Above, in equation [1.2], we considered the elliptic surface studied by Cheng and Huang in [5]:

\[ E_t : y^2 = x^3 + (a + tp)x + (y_0^2 - x_0^3 - (a + tp)x_0) \]

over \( \mathbb{Q} \) where \( y_0^2 \equiv x_0^3 + ax_0 + b \mod p \). While we do not know that we can find an appropriate rank one fiber on this without the help of deep conjectures on the distributions of ranks over elliptic surfaces, we will see that the surface itself as an elliptic curve over \( \mathbb{Q}(t) \) has rank one. Thus changing our perspective and using the entire surface in place of the desired rank one lift, we can prove that the ECDLP is equivalent to:

**Problem 1.3.1 (Rank One Surface Lifting Problem, R1SLP).**

Given:

- \( f \) a good function
- \( \tilde{E} \) an elliptic curve over \( \mathbb{F}_p \)
- \( E \) an elliptic curve over \( \mathbb{Q}(t) \) of (generic) rank one such that the specialization at \( t = 0: E(0) \) reduces mod \( p \) to \( \tilde{E} \)
- \( \tilde{P} \in \tilde{E}(\mathbb{F}_p) \)
- \( \epsilon > 0 \)
- \( W \in E(\mathbb{Q}(t)) \) whose specialization at \( t = 0: W(0) \) does not reduce to zero mod \( p \)
- \( h_W \in \mathbb{Q} \) such that \( |\hat{h}(W) - h_W| < \frac{\epsilon}{4p^2} \) and the numerator of \( h_W \) is at most \( \epsilon^{f(\ln p)} \)

such that the sizes of these entries (particularly the total size of the coefficients of the polynomials that define \( E \), the coefficients of the polynomials of \( W \), and \( h_W \)) are all bounded by \( f(\ln p) \)
Find: $h \in \mathbb{Q}$ such that there exists some $P \in E(\mathbb{Q}(t))$ such that $P(0)$ reduces to $\tilde{P}$ mod $p$, $|\hat{h}(P) - h| < \epsilon$, $h \leq 4p^2h_W$, and $H(h) \leq e^{f(\ln p)}$.

We write $R1SLP(\tilde{E}, p, E, h_W, \tilde{P}, f, \epsilon) = h$.

Note that it is essential that there is a height function on elliptic curves over $\mathbb{Q}(t)$ (see [36, Section 3.4]). In fact, the canonical heights of points on elliptic curves over $\mathbb{Q}(t)$ are rational (see [36, Ch. 3, Remark 4.3.1]) so one might realistically hope to compute to exact values of $\hat{h}(P)$ and $\hat{h}(W)$ rather than having to approximate them.

In Chapter 3 we will define a technical condition similar to “good” on functions that we will call “very good.” Then we will see:

**Theorem 1.3.2.** Let $p > 23$ and $\tilde{E}$ an elliptic curve over $\mathbb{F}_p$ such that $\#\tilde{E}(\mathbb{F}_p) = l$ is prime. Then there is an equivalence between $R1SLP(\tilde{E}, p, -, -, -, -, f, e^{f(\ln p)})$ and $ECDLP(\tilde{E}, p, -, -)$. Furthermore, this equivalence runs in

$$\max\{O(f(\ln p)), \text{poly}(\ln p)\}$$

many steps in addition to performing one computation of the height of a point on an elliptic curve over $\mathbb{Q}(t)$ to within $\frac{1}{4e^{f(\ln p)}}$ precision. Here poly is a fixed polynomial and the constant in the $O$ is absolute.

There exist efficient methods to compute the canonical heights of points on elliptic curves over $\mathbb{Q}(t)$ (see, for example, the introductory remarks of [37]). However, the running time of these methods does not seem to have been analyzed in detail, so, when stating the running time in Theorem 1.3.2 we separate out this step.

The advantage here of lifting to sections (which one might expect to be more difficult) may seem limited as all of our specializations are to a single fiber $t = 0$. In fact, what this gives us is the dependence of our lifts of $\tilde{P}$ and $\tilde{Q}$. We know these points are dependent, as we know sections are dependent because the generic rank is one; however, two arbitrary points on our lift may not necessarily be dependent, as we do not know if $E(0)$ has rank one. Thus, the R1SLP may be looked at as the problem of lifting to certain types of points, namely those points that lie on some section.

We will see that whether R1LP is equivalent to R1SLP (and hence to the ECDLP) is related to the “excess rank phenomenon” — the phenomenon of the fibers of an elliptic surface having on average higher rank than one would expect them to have based on the rank of the surface. We will further explore this in Chapter 3.
1.3.2 Diffusion of candidate lifts

Here we state the results that make up the content of Chapter 4. We begin by defining a class of elliptic surfaces that we call “cross-fibered.” The critical property used in the proofs of Conjecture 1.2.7 for the surfaces considered by Munshi and Rohrlich in [24], [25], and [30] is that these elliptic surfaces all have a second fibration by genus one curves, and that these two fibrations interact well. For example, one of the surfaces for which Munshi proves Conjecture 1.2.7 (see [24, Theorem 1.7]) is

\[ E_t : y^2 = x^3 + bC(t)^2 \]

where \( C(t) = t^3 + \alpha t + \beta \) for \( \alpha, \beta, \) and \( b \in \mathbb{R} \) and \( b \neq 0. \) However, one also has the elliptic fibration

\[ E^*_s : v^2 = u^3 + A(s)u + B(s) \]

where \( A(s) = \alpha s^2 \) and \( B(s) = \beta s^3 + b, \) and there are transition maps between these surfaces that are given by the rational maps

\[(x, y) \in E_t \mapsto \left(\frac{x}{C(t)}, \frac{y}{C(t)}\right) \in E^*_s \]

and

\[(u, v) \in E^*_s \mapsto \left(sC\left(\frac{u}{s}\right), vC\left(\frac{u}{s}\right)\right) \in E_* \]

off the curves \( C(t) = 0 \) and \( s = 0. \)

We will consider other similar examples in Section 4.1. The definition of “cross-fiberedness” is modeled upon these examples. First we define:

**Definition 1.3.3 (Pre-Cross-Fibration).** Given an elliptic surface \( \mathcal{E} \) (over \( \mathbb{Q} \)) with projection map \( \pi : \mathcal{E} \rightarrow \mathbb{P}^1, \) a pre-cross-fibration is a triple \((\mathcal{E}^*, \Phi, \Phi^*)\) where \( \mathcal{E}^* \) is an elliptic surface (over \( \mathbb{Q} \)) with projection map \( \pi^* : \mathcal{E}^* \rightarrow \mathbb{P}^1 \) and \( \Phi \) is a birational map \( \Phi : \mathcal{E} \rightarrow \mathcal{E}^* \) over \( \mathbb{Q} \) which has inverse \( \Phi^*. \)

Thus, we have a diagram

\[ \xymatrix{ \mathcal{E} \ar[d]_{\pi} \ar[r]^{\Phi} & \mathcal{E}^* \ar[d]_{\pi^*} \\ \mathbb{P}^1 } \]

However, note that this diagram does not commute. Namely, \( \pi \neq \pi^* \circ \Phi \) in general.
We will see below that this is actually critical in our arguments below (see, for example, Diffusion Process \textsection 4.1.4 in Chapter 4).

Every elliptic surface $E$ has a trivial pre-cross-fibration where $E^* = E$ and $\Phi$ is the identity. Below we will define elliptic surfaces with a pre-cross-fibration satisfying certain properties to be “cross-fibered,” and the additional properties we assume will eliminate this case.

For details on why we draw a distinction between $E$ and $E^*$ even though they are birationally equivalent, see Section \textsection 4.1.3.

We fix some additional notation that will be useful to us in discussing pre-cross-fibrations. We define

$$\sigma = \pi^* \circ \Phi \quad \text{and} \quad \tau = \pi \circ \Phi^*.$$

These maps tell us what fiber a point goes to when it is converted to the other fibration. Namely, $\sigma(P)$ is the fiber of $E^*$ to which $P$ is sent under $\Phi$. For $t$ and $s \in \mathbb{P}^1$ we often denote individual fibers in the respective fibrations by

$$E_t = \pi^{-1}(t) \quad \text{and} \quad E^*_s = \pi^*^{-1}(s).$$

Furthermore, for $P \in E$ (at which the map $\Phi$ is defined), when there is no risk of ambiguity, we condense our notation by writing $\Phi(P) = P^* \in E^*_\sigma(P)$; and for $P^* \in E^*$ (at which the map $\Phi^*$ is defined) we similarly write $\Phi^*(P^*) = P^{**} \in E^*_\tau(P)$. Generally, we use the $*$ symbol for objects that are associated with the $E^*$ fibration. Hence, given a point $P \in E$, $P^*$ represents the point in $E^*$ “associated with” $P$, namely its image under the conversion map.

Finally, to any (pre-)cross-fibered surface $E$ we will attach a value $L(E)$ which measures the size of the degrees of the rational maps that define the conversions (see Section \textsection 4.1).

So far, this definition would still make sense if we replaced $\mathbb{Q}$ with some other field. In particular, as all of the maps that define a pre-cross-fibration ($\Phi$, $\Phi^*$, $\pi$, $\pi^*$, and the coefficients of $E$ and $E^*$) are rational over $\mathbb{Q}$, we can reduce them mod $p$ for some prime $p$. Then, barring some degenerate situations (see Definition \textsection 4.1.12), we again have two elliptic fibrations, now over $\mathbb{F}_p$, where $\Phi$ and $\Phi^*$ still give a correspondence. In situations where we consider an elliptic surface $E$ with a cross-fibration simultaneously over $\mathbb{Q}$ and $\mathbb{F}_p$ we shall assume that we have a fixer Weierstrass model of $E$ so that our reductions are fixed.

However, the content of Mazur’s conjecture, as it involves the rank of the fibers, is intrinsically rational. So there are naturally some $\mathbb{Q}$ properties that Munshi uses in his
arguments that we would want a cross-fibered surface to have:

**Definition 1.3.4** (Cross-fibered surface). Let $\mathcal{E}$ be an elliptic surface that has a cross-fibration $(\mathcal{E}^*, \Phi, \Phi^*)$. We say that $\mathcal{E}$ is cross-fibered if the pre-cross-fibration satisfies the following properties:

1. For all but a finite number of $t \in \mathbb{Q}$ we have, for all but a finite number of points $P \in E_t(\mathbb{Q})$, $P^*$ is a non-torsion point on a non-singular fiber $E_{\sigma(P)}^*(\mathbb{Q})$.
2. For all but a finite number of $s \in \mathbb{Q}$ we have, for all but a finite number of points $P^* \in E_s^*(\mathbb{Q})$, $P^{**}$ is a non-torsion point on a non-singular fiber $E_{\tau(P^*)}(\mathbb{Q})$.
3. For all but the finitely many exceptional $t \in \mathbb{Q}$ of part 1, if $E_t$ is a curve of positive rank over $\mathbb{Q}$, then

$$\bigcup_{s:rk(E_s^*(\mathbb{Q}))>0, s \in \{\sigma(P): P \in E_t^* \cap E_t(\mathbb{Q})\}} \{\tau(P^*): P^* \in E_s^0(\mathbb{R}) \cap E_s^*(\mathbb{Q})\} = \mathbb{R}.$$

Note that this definition is asymmetric between the two fibrations; we call the $\{E_t\}$ fibration above the “main fibration.”

When working with cross-fibered surfaces we often take a point $P$ on some fiber $E_t$ (at which $\Phi$ is defined), and we look at what happens if we multiply that point by $n$, convert to the other fibration, multiply by $m$ in the second fibration, and convert back to produce the point $(m(nP)^*)^*$, which is typically on some other fiber than $E_t$. This process allows us to “move around” the surface from one fiber to another. We will study cross-fibered surfaces in more detail in Section 4.1.

Now we define a condition that regroups many of the properties required of our lifts in the R1LH.

**Definition 1.3.5** (Candidate Lift). Given an elliptic curve $\tilde{E}$ over a finite field $\mathbb{F}_p$, we define a candidate lift to be a lift $E$ of $\tilde{E}$ to $\mathbb{Q}$ such that:

- $rk(E) > 0$
- the reduction $E(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_p)$ does not send every point to $\tilde{O}$.

(So, the thing that could prevent a candidate lift from being the lift we want for the R1LH is that the rank of $E$ may be too big.)

We will see:
Proposition 1.3.6. Let \( \tilde{E} \) be an elliptic curve over a finite field \( \mathbb{F}_p \) (where \( p > 23 \)) such that \( \# \tilde{E}(\mathbb{F}_p) \) is prime. Let \( \mathcal{E} \) be a cross-fibered elliptic surface of which \( \{E_t\} \) is the main fibration. Then fibers \( E_t \) such that:

- \( E_t \) is a candidate lift of \( \tilde{E} \) and
- \( \exists \) a non-zero point \( \tilde{P} \in E_t(\mathbb{F}_p) \) such that \( \tilde{P}^* \) is a non-zero point of odd order on its cross-fiber \( E_{\sigma(\tilde{P})}^*(\mathbb{F}_p) \)

are diffusive. Namely,

\[
\left\{ \begin{array}{c}
t \in \mathbb{Q} : \\
E_t \text{ is a candidate lift of } \tilde{E} \text{ on which } \exists \text{ a non-zero point } \tilde{P} \in E_t(\mathbb{F}_p) \end{array} \right\}
\quad \text{such that } \tilde{P}^* \text{ is a non-zero point of odd order on } E_{\sigma(\tilde{P})}^*(\mathbb{F}_p)
\]

is dense in \( \mathbb{R} \) or finite. In fact, if this set is finite, its size is less than a computable bound.

As we mentioned above, as \( \mathcal{E} \) is being considered simultaneously over \( \mathbb{Q} \) and \( \mathbb{F}_p \), we assume that we are working with some fixed Weierstrass model of \( \mathcal{E} \) over \( \mathbb{Q} \). The condition that there be a point on \( E_t \) that converts to an odd order point may seem clunky; one might hope that the property of being a candidate lift itself be diffusive. We will look more at this in Chapter 4.

As a consequence:

Corollary 1.3.7. Let \( \tilde{E} \) be an elliptic curve over a finite field \( \mathbb{F}_p \) where \( p \) is larger than an absolute constant and such that \( \# \tilde{E}(\mathbb{F}_p) \) is prime. Suppose there exists a cross-fibered elliptic surface \( \mathcal{E} \) such that:

- \( \text{R2MC does not hold for } \mathcal{E} \) in the main fibration \( \{E_t\} \)
- the number of fibers of \( E_t \) which are candidate lifts and which have a point \( \tilde{P} \) which converts to a point of odd order on its cross-fibration under \( * \) exceeds a computable bound.

Then, there exists a lift satisfying Conjecture 1.1.10.

We will state this more explicitly (specifically with regard to what the absolute constant and the computable bound are) as Corollary 4.3.2 when we give the proof in Section 4.3.
Suppose we had a cross-fibered surface (satisfying the conditions of Proposition 1.3.6) that had infinitely many fibers that were candidate lifts (and which had a point that converted to an odd order point under \(\ast\)) for a given instance of the R1LP, yet where the R2MC failed to be true; namely, if there was an interval \(I\) where all \(t \in I\) are such that \(E_t\) has at most rank one. Then, we could use that surface to find a rank one candidate lift for this instance of the R1LP. Hence, any such surface must either satisfy the R2MC or it can be used to solve instances of the R1LH. We must note that we know of no such surfaces that fail to satisfy the R2MC, but considering that there are surfaces on which arithmetic properties are not diffusive as in Theorem 1.2.11, it is perhaps not so implausible that such a surface could exist.

However, given an interval \(I \subset \mathbb{R}\), the height of the \(t \in I\) produced by the proof of Proposition 1.3.6 is exponential in \(p\). As we were motivated by the cryptographic considerations of Conjecture 1.1.10 in which \(p\) determines the scale of computational feasibility, we might ask if we can find such \(t\) of smaller height. Furthermore, we expect that the height of our output \(t\) will also depend on \(I\) as smaller intervals provide a smaller “target.” In Section 4.2 we will define a measure on the real line \(m_{E_t}(I)\) that detects what percentage of \((m(nP)\ast)\) are on fibers in \(I\) as \(n\) and \(m\) become large. Then we will study how the “rate of diffusion” depends on \(p\), \(L(\mathcal{E})\), and \(m_{E_t}(I)\).

In Section 4.4 we will see that, if we assume substantially more structure on \(\mathcal{E}\) in addition to being cross-fibered, we can achieve a version of Proposition 1.3.6 where the fibers produced have much more reasonable height with respect to \(p\).

To develop this, note that if \(C\) is a rational curve over \(\mathbb{Q}\) in \(\mathcal{E}\), then \((m(nP)\ast)\) is also a rational curve (perhaps with more singular points if \(C\) passes through points where the cross-fibration is undefined). Then, we have:

**Theorem 1.3.8.** Let \(\tilde{E}\) be an elliptic curve over a finite field \(\mathbb{F}_p\) \((p > 23)\). Let \(\{E_t\}\) be the main fibration of a cross-fibered elliptic surface \(\mathcal{E}\) which has non-trivial reduction (as a cross-fibered surface) mod \(p\). Further, assume that \(\{E_t\}\) has constant \(j\)-invariant mod \(p\) (and that \(j \not\equiv 1728\) mod \(p\) if \(p \equiv 1\) mod 4).

Assume that there exists a rational curve \(C\) on \(\mathcal{E}\) over \(\mathbb{Q}\); \(\Psi : \mathbb{P}^1(\mathbb{Q}) \rightarrow C\). For \(k \in \mathbb{P}^1(\mathbb{Q})\) at which \(\Psi\) is defined, we denote by \(P(k)\) the point on \(C\) that is the image of \(k\) under \(\Psi\). Suppose that

- the degree of \(C\) is such that \(p > 112 \deg(C) L(\mathcal{E})^3 6^{142L(\mathcal{E})}\)
- \(C\) contains at least one non-torsion point (on some non-singular fiber)
- \(C\) contains at least one point of order greater than \(r\) mod \(p\) on its fiber


for each \( n \) and \( m \), the rational curve \((m(nC)^{\ast})^{\ast}\) contains points on exactly \( \rho \) many non-isomorphic fibers over \( \mathbb{F}_p \), and one of these fibers is isomorphic to \( \tilde{E} \) over \( \mathbb{F}_p \).

Let \( I \subset \mathbb{R} \) be an interval and let \( \epsilon > 0 \). Let \( k_0 \in \mathbb{Q} \) avoiding at most

\[
\deg(C) \left( 17832L(\mathcal{E})^3 + 14830L(\mathcal{E})^2 + 5922L(\mathcal{E}) + 1481 \right)
\]

exceptions. Then there exists \( N_0 \in \mathbb{N} \) depending only on \( \mathcal{E}, C, I, k_0, \) and \( \epsilon \) such that for \( N, M \geq N_0 \), there exists an open set \( U(k_0, N, M) \) (which depends on \( N \) and \( M \)) around \( k_0 \) such that

\[
\left| \Pr_{n,m,k} \left( \begin{array}{l}
(m(nP(k))^{\ast})^{\ast} \text{ is on a fiber } \ E_{t_{n,m}(k), \text{ which is a candidate lift and } t_{n,m}(k) \in I} \\
n \leq N \text{ and } m \leq M
\end{array} \right) - \frac{m_{E_t(k_0)}(I)}{\rho} \right| < \frac{2\epsilon}{\rho} + C(\rho) \left( \frac{m_{E_t(k_0)}(I) + 2\epsilon}{p} \right)
\]

\[
+ 10^8L(\mathcal{E})^3 \max \left\{ \frac{1}{N^{1/4}} \frac{1}{M^{1/4}} \frac{1}{r^{1/4}} \left( \frac{\deg(C)}{p} \right)^{1/16}, \left( \frac{1}{\ln \left( \frac{p}{112 \deg(C)L(\mathcal{E}) t_{n,m}(k)^{\ast}} \right)} \right)^{1/4} \right\},
\]

where \( C(\rho) = \begin{cases} 10^5 \deg(C)L(\mathcal{E})^5(2\sqrt{2} + 3)^{N+M} \sqrt{p} & \text{if } \rho = 1, 2, \text{ or } 3 \\ \frac{p}{12} + 10^5 \deg(C)L(\mathcal{E})^5(2\sqrt{2} + 3)^{N+M} \sqrt{p} & \text{if } \rho = 6 \end{cases} \).

(Note, under these assumptions, these are the only possible values of \( \rho \) for which the error bound is non-trivial.)

For the definition “non-trivial reduction mod \( p \) as a cross-fibered surface,” see Section 4.1. The probability measure can be interpreted here as uniform on

\[
\{1, ..., N\} \times \{1, ..., M\} \times \left\{ \begin{array}{l}
\text{Any finite subset of } \\
U(k_0, N, M) \text{ in which } \\
\text{the classes } \mathbb{F}_p \text{ are } \\
\text{uniformly distributed}
\end{array} \right\}.
\]

Notice that if \( N \) and \( M \) are large relative to \( L(\mathcal{E}) \) and \( \deg(C) \), and if \( p \) and \( r \) are large relative to \( N \) and \( M \), then this error bound approaches the \( \epsilon \) error bound, and hence can be made arbitrarily small.

We will see that the choice of \( N_0 \) is related to the rate at which the proportion of
(m(nP)*) that are on fibers in I converges to \( m_{E_t(k_0)}(I) \). Furthermore, we will see that the smaller we take our “target” I to be, the large we must take \( N_0 \). This ultimately has the effect that we need \( p \) to be larger for the error bound to be non-trivial.

Further, notice that if we assume that the order of \( \tilde{E}(\mathbb{F}_p) \) is prime (as is the case for cryptographic instances of the ECDLP), then the condition that we have a point of order at least \( r \) on its fiber could be replaced with the assumption that we have a point of non-trivial reduction on a fiber isomorphic to \( \tilde{E} \), which would give us a point of order at least \( p + 1 - 2\sqrt{p} \). Then the \( r \) in the error bound could be replaced accordingly.

Then, if we want to produce such a candidate lift:

**Theorem 1.3.9.** Let \( \tilde{E} \) be an elliptic curve over a finite field \( \mathbb{F}_p \) \( (p > 23) \) and let \( \mathcal{E}, C, I, k_0, \epsilon, \) and \( N_0 \) be as in Theorem 1.3.8. Then if there exists \( N, M \geq N_0 \) such that

\[
\delta = \frac{m_{E_t(k_0)}(I)}{p} - \text{the error bound of Theorem 1.3.8} > 0,
\]

there is a candidate lift \( E_{t_{out}} \) of \( \tilde{E} \) such that \( t_{out} \in I \), \( ht(t_{out}) \leq \text{poly(ln}(p)) \). Furthermore, if one can efficiently compute values \( m_{E_t}(I) \) and \( N_0 \), then this \( t_{out} \) can be found in randomized \( \text{poly}(\ln(p), \frac{1}{\delta}) \) time where the coefficients of these polynomials depend on quantities associated with \( \mathcal{E}, C, I, \) and \( \epsilon \).

When we write \( \text{poly}(x_1, ..., x_n) \) we mean that a given quantity (in this case the height of \( t_{out} \) and the step cost of the procedure to find a candidate lift) is bounded by a polynomial in \( x_1, ..., x_n \). Note that \( m_{E_t}(I) \) and \( N_0 \) do not depend on the prime \( p \). Thus, if one has any algorithm that can compute them, its running time will only affect the constants in the polynomial. Moreover, if one is interested in applying this procedure to a fixed \( \mathcal{E} \) and \( I \) with varying prime \( p \), one can perform all of the necessary computations of \( m_{E_t}(I) \) and \( N_0 \) before choosing \( p \), and then \( \delta \) will be positive if \( r \) and \( p \) are sufficiently large. We will generally not be able to compute \( m_{E_t}(I) \) and \( N_0 \) exactly, but we can find lower bounds on \( m_{E_t}(I) \) (see Algorithms 1 and 2) along with a corresponding analog of \( N_0 \). See Theorem 4.4.13 for a version of Theorem 1.3.9 in these terms.

We said that Proposition 1.3.6 was problematic because the resulting fiber we find, \( t_{out} \), has height exponential in \( p \). In Theorem 1.3.9, the \( t_{out} \) produced is of reasonable size in \( p \), but we had to assume that \( p \) is “large relative to \( I \)” (specifically for \( \delta > 0 \), we need \( p \) to be exponentially large with respect to \( N_0 \). The analog of Corollary 1.3.7 that corresponds to Theorem 1.3.9 is:

**Corollary 1.3.10.** Let \( \tilde{E} \) be an elliptic curve over a finite field \( \mathbb{F}_p \) \( (p > 23) \). Suppose there exist \( \mathcal{E}, C, k_0, \) and \( \epsilon \) as in Theorem 1.3.8 such that
Chapter 1. Introduction

- Proposition 1.1.10: Let \( E \) be a smooth projective curve over \( \mathbb{C} \). If \( \rho \) denotes the rank of \( E \) and \( t \) is an integer such that \( \rho(t) \) is a polynomial in \( t \), then \( \rho(t) \) is a polynomial in \( t \).

In Section 4.4.5 we will see examples in which we meet the requirements of this theorem. In particular,

**Example 1.3.11.** Let \( p > 6^{433} \) be a prime congruent to 1 mod 3 and let \( e \) be a rational number that does not reduce to zero mod \( p \). Then there is a curve \( C \) such that the surface

\[
E_t : y^2 = x^3 + (t^3 + e)^2
\]

satisfies the requirements of Theorem 1.3.8 with \( \rho = 3 \) and \( \tilde{E} \) the reduction over \( \mathbb{F}_p \) of any fiber of \( E_t \) of good reduction.
Chapter 2
Computational precision in the R1LP

In this chapter we will prove Theorem 1.1.12; namely, we will analyze the running time of the equivalence between the R1LP and the ECDLP that Miri and Murty proved under the assumption of Conjecture 1.1.10 (again, see [23, Propositions 4 and 5]). Note that in order to do so we have had to specify the level of precision with which we work with the (generally irrational) heights of points on our elliptic curves. This amounts to specifying the $\epsilon$ that we input into Problem 1.1.3 which, as we saw in the statement of Theorem 1.1.12, we choose as $\epsilon = p^{2e/(\ln p)}$. We demonstrate here that this level of precision is, in fact, sufficient.

Proof of Theorem 1.1.12 R1LP $\Rightarrow$ ECDLP

We know that our lifts of $\tilde{P}$ and $\tilde{Q}$, $P$ and $Q$ respectively are multiples of some unknown generator $R$ of $E(\mathbb{Q})$; $P = n_1 R$ and $Q = n_2 R$. Then, if $\tilde{Q} \equiv n\tilde{P}$ mod $p$,

$$n \equiv \frac{n_2}{n_1} = \sqrt{\frac{n_2^2 h(R)}{n_1^2 h(R)}} = \sqrt{\frac{h(Q)}{h(P)}} \mod \# \tilde{E}(\mathbb{F}_p).$$

Essentially, in this argument we will show that the precision with which we approximate $\hat{h}(P)$ and $\hat{h}(Q)$ is sufficient so that if we take the continued fraction expansion of our approximation of $\sqrt{\frac{h(Q)}{h(P)}}$, the true value of $\frac{n_2}{n_1}$ will appear as a convergent (within a reasonable number of steps). Denote

$$\epsilon_1 = h_P - \hat{h}(P) \text{ and } \epsilon_2 = h_Q - \hat{h}(Q).$$
Then,
\[
\left| \frac{h_Q}{h_P} - \frac{n_2^2}{n_1^2} \right| = \left| \frac{n_2^2 \hat{h}(R) + \epsilon_2 - n_2^2}{n_1^2 \hat{h}(R) + \epsilon_1} \right| = \left| \frac{\epsilon_2 n_1^2 - \epsilon_1 n_2^2}{n_1^2 \hat{h}(R) + \epsilon_1} \right| \\
\leq \frac{2 \max \{\epsilon_1, \epsilon_2\}}{\min \{n_1^2, n_2^2\} \left( \hat{h}(R) + \frac{\epsilon_1}{n_1^2} \right)} \leq \frac{2p^2}{\ell f(\ln p)}.
\]

Without loss of generality we assume that \(h_Q \geq h_P\). If this is not the case we interchange the roles of \(P\) and \(Q\), and at the end of the algorithm we will have found \(\hat{m}\) such that \(\hat{P} = \hat{m}\hat{Q}\). Then, we can solve our desired instance of the ECDLP by the Extended Euclidean algorithm over \(#\hat{E}(\mathbb{F}_p)\). \(#\hat{E}(\mathbb{F}_p)\) \(\leq 2p\) by Hasse’s bound as \(p > 23\), so this process takes at most \(O(\ln(\#\hat{E}(\mathbb{F}_p))^2) \leq O(\ln(2p)^2)\) steps. (Note that Schoof’s algorithm takes \(O((\ln p)^8)\) steps so we can efficiently compute \(#\hat{E}(\mathbb{F}_p)\).)

Then, \(n_2 / n_1 \in \left( \frac{\sqrt{\frac{h_Q}{h_P}} - \frac{2p^2}{\ell f(\ln p)}}{\sqrt{\frac{h_Q}{h_P}} + \frac{2p^2}{\ell f(\ln p)}} \right) \subseteq \left( \frac{\sqrt{\frac{h_Q}{h_P}} - \frac{2p^2}{\ell f(\ln p)}}{\sqrt{\frac{h_Q}{h_P}} + \frac{2p^2}{\ell f(\ln p)}} \right)^{-1} \subseteq \left( \frac{\sqrt{\frac{h_Q}{h_P}} - \frac{2p^2}{\ell f(\ln p)}}{\sqrt{\frac{h_Q}{h_P}} + \frac{2p^2}{\ell f(\ln p)}} \right) := I.\]

In order to have \(\frac{h_Q}{h_P} - \frac{2p^2}{\ell f(\ln p)} \geq 0\), we have used our observations that \(h_Q \geq h_P\) and that \(L \geq \frac{2p^2}{\ell f(\ln p)}\).

As \(\sqrt{\frac{h_Q}{h_P}}\) is generally irrational, we cannot access it exactly; however, we can compute an approximation \(\alpha\) to sufficient precision such that \(\alpha \in I\). Specifically we can use a binary search procedure to find a \(x_0\) such that \(|x_0 - \sqrt{\frac{h_Q}{h_P}}| \leq 1\). Then we can apply Newton’s method/Herod’s method which by the quadratic bound on successive errors:
\[
|x_{n+1} - \sqrt{\frac{h_Q}{h_P}}| \leq \frac{|x_n - \sqrt{\frac{h_Q}{h_P}}|^2}{2\sqrt{\frac{h_Q}{h_P}}}
\]
takes at most \(\log_2 \left( \frac{2}{\text{length}(I)} \right)\) iterations. All of this takes at most
\[
\max \{O(f(\ln p)), \text{poly}(\ln p)\}
\]
many steps. Note that we can make the constants here absolute, as we can without loss of generality take \(L \leq 1\).

We note, as \(\hat{h}(R) \geq L\), we know \(n_1^2 \leq \frac{\hat{h}(p)}{L}\) and \(n_2^2 \leq \frac{\hat{h}(Q)}{L}\). Then as \(|h_P - \hat{h}(P)|\) and \(|h_Q - \hat{h}(Q)|\) are each bounded by \(\frac{p^2}{\ell f(\ln p)} \leq 1\) as \(f\) is good, and \(h_P\) and \(h_Q\) are each at most
\[ 4p^2 h_W \leq L 2^{\sqrt{f(ln(p)+ln(L)-ln(8p^2)}-2-1}, \text{ each of } n_1^2 \text{ and } n_2^3 \text{ are at most } 2^{\sqrt{f(ln(p)+ln(L)-ln(8p^2)}-2}. \]

Recall that there is an interval around \( \frac{n_1}{n_2} \) such that the continued fraction expansion of any number in the interval takes \( \frac{n_1}{n_2} \) as a convergent. We lower bound the length of this interval. Consider the (finite) continued fraction expansion of \( \frac{n_1}{n_2} = [a_0; a_1, ..., a_l] \). We have two cases: when \( a_l \neq 1 \) and when \( a_l = 1 \). We consider the first case; the second is similar and yields bounds that are no worse. Then any real number strictly between \( [a_0; a_1, ..., a_l-1, 2] \) and \( [a_0; a_1, ..., a_l+1] \) must take \( \frac{n_1}{n_2} \) as a convergent. We call this interval \( J \). We denote the partial convergents as \( \frac{p_i}{q_i} = [a_0; a_1, ..., a_i] \). By well-known properties of continued fractions we have that the sequence \( (q_i) \) is increasing, \( q_{i+1} = a_i q_i - 1 + q_{i-2} \), and \( 2^{(i-1)/2} \leq q_i \leq n_i \) for \( i \leq l \). Hence \( l \leq 2 \log_2 n_1 + 1 \).

Furthermore, \( \frac{n_1}{n_2} \) and each of the two endpoints of \( J \) are rational, and they all have the same continued fraction expansion up through \( a_{l-2} \), and hence they share the same \( q_{l-1} \). Thus we compute

\[
q_{l, \text{endpoint1}} = (2a_l - 1)q_{l-1} + 2q_{l-2} \leq 3n_1 \quad \text{and} \quad q_{l+1, \text{endpoint2}} = (a_l + 1)q_{l-1} + q_{l-2} \leq 2n_1.
\]

Similarly (though less standard), given the finite continued fraction expansion \( [b_1, ..., b_w] \) of a rational number, we consider \( \frac{k}{h_i} = [b_1, ..., b_i] \), and by similar arguments as one uses for \( q_i \), we note \( h_w \leq h_{w-1} \leq ... \leq h_0 = q_w \), so our bounds on the \( q_i \)’s of the endpoints of \( J \) translate into bounds on each of their \( h_i \)’s.

Then,

\[
\frac{n_2}{n_1} - \text{endpoint1 of } J = \left| \left( a_0 + \frac{1}{a_1 + \frac{1}{...+a_l}} \right) - \left( a_0 + \frac{1}{a_1 + \frac{1}{...+a_l-1+\frac{1}{2}}} \right) \right|,
\]

which by repeatedly taking common denominators and canceling is of the form

\[
\frac{1/2}{\text{product of } l \ h_i \text{’s from } \frac{n_2}{n_1} \text{ and endpoint1 of } J}.
\]

Similarly,

\[
\frac{n_2}{n_1} - \text{endpoint2 of } J = \frac{1}{\text{product of } l \ h_i \text{’s from } \frac{n_2}{n_1} \text{ and endpoint2 of } J}.
\]
So $J$ contains the interval \( \left( \frac{n_2}{n_1} - \frac{1}{2(3n_1^2)^l}, \frac{n_2}{n_1} + \frac{1}{2(3n_1^2)^l} \right) \). However,

\[
\frac{1}{2(3n_1^2)^l} \geq \frac{1}{2 (3n_1^2)^{2 \log_2 n_1 + 1}} \geq \frac{4p^2}{Le^{f(lnp)}} \geq \left| \frac{n_2}{n_1} - \alpha \right|
\]

because

\[
n_1^2 \leq 2\sqrt{f(lnp) + \ln(L) - \ln(8p^2) - 2}
\]

\[
\Rightarrow \log_2 n_1 \leq \frac{\sqrt{\ln(e^{f(lnp)}) + \ln(L) - \ln(8p^2) - 2}}{2} \leq \frac{\sqrt{\log_2 \left( \frac{Le^{f(lnp)}}{8p^2} \right)} - 2}{2}
\]

\[
\Rightarrow \log_2 \left((3n_1^2)^{2 \log_2 n_1 + 1}\right) = (2 \log_2 n_1 + 1)(2 \log_2 n_1 + \log_2 3) \leq (2 \log_2 n_1 + 2)^2 \leq \log_2 \left( \frac{Le^{f(lnp)}}{8p^2} \right).
\]

Hence $\alpha \in J$, so by taking the first many convergents of $\alpha$, we eventually come upon the continued fraction expansion of $\frac{n_2}{n_1}$.

We can test each of these to see if it solves our instance of the ECDLP until we succeed. This runs in $\max \{O(f(lnp)), \text{poly}(lnp)\}$ many steps and again we can assume $L \leq 1$ so that the constants are absolute.

**ECDLP $\Rightarrow$ R1LP**

We use our ECDLP oracle to solve $\tilde{P} = n\tilde{W}$ for some $n$ where $\tilde{W}$ is the reduction of $W \text{ mod } p$. (Note that $\tilde{E}(\mathbb{F}_p)$ is cyclic because it is of prime order so such an $n$ can be found.) By Hasse’s bound, as $p > 23$, $\#\tilde{E}(\mathbb{F}_p) \leq 2p$. Hence, we can reduce $n$ so that it is without loss of generality less than $2p$. Then we will output $h = n^2h_W$. We note that $|h - \hat{h}(P)| = |n^2h - n^2\hat{h}(P)| = n^2|h_W - \hat{h}(W)| \leq \epsilon$ where $P = nW$ is a lift of $\tilde{P}$. Note that the numerator and denominator of $h$ are both at most $e^{f(lnp)}$, as we assumed the numerator of $h_W$ is at most $\frac{e^{f(lnp)}}{4p^2}$.
Chapter 3

A variant on the R1LP

3.1 Important background theorems

In this chapter we will prove Theorem 1.3.2. To do so we will find an elliptic surface of generic rank one, i.e. an elliptic curve of rank one over $\mathbb{Q}(t)$, which will serve as the analog of the lift we ask for in Problem 1.1.9. To this end we discuss some important theorems that will allow us to compute the generic rank of certain elliptic surfaces.

Our principal tool will be:

Conjecture 3.1.1 (Nagao, see [1], [27]). Let $E$ be an elliptic curve over $\mathbb{Q}$. For any given prime $q$, denote by $a_t(q)$ the $q$th coefficient of the $L$-series of the fiber $E_t$. Take

$$A_E(q) = \frac{1}{q} \sum_{t=0}^{q-1} a_t(q).$$

Then, one can find the rank of $E$ over $\mathbb{Q}(t)$ via the formula:

$$\text{rank}(E) = \lim_{X \to \infty} \frac{1}{X} \sum_{q \leq X} -A_E(q) \ln q.$$

Rosen and Silverman ([31]) proved Conjecture 3.1.1 for surfaces for which one knows Tate’s Conjecture:

Conjecture 3.1.2 (Tate, in our case, see [38]). Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface, and let $L_2(\mathcal{E}, s)$ be the $L$-series attached to $H^2_{et}(\mathcal{E}/\mathbb{Q}, \mathbb{Q}_l)$. Then, $L_2(\mathcal{E}, s)$ has a meromorphic continuation to $\mathbb{C}$ and satisfies

$$-\text{ord}_{s=2} L_2(\mathcal{E}, s) = \text{rank} NS(\mathcal{E}/\mathbb{Q})$$
where $NS(E/\mathbb{Q})$ is the $\mathbb{Q}$-rational part of the Néron-Severi group of $E$. Also, $L_2(E, s)$ does not have any zeros on the line $Re(s) = 2$.

Specifically, we know Conjecture 3.1.2 and hence Conjecture 3.1.1 for rational elliptic surfaces (see [1] and [31]).

Another important result that we will need in the course of our computation is:

**Theorem 3.1.3** (Weil, see [7]). Let $\mathbb{F}_q$ be a finite field, and let $\chi$ be a character of $\mathbb{F}_q$ of order $s$. Let $f(x)$ be a polynomial of degree $d$ over $\mathbb{F}_q$ that cannot be written in the form $c(h(x))^s$ for any $h(x) \in \mathbb{F}_q[x]$ and $c \in \mathbb{F}_q$. Then,

$$\left| \sum_{a \in \mathbb{F}_q} \chi(f(a)) \right| \leq (d - 1)\sqrt{q}.$$ 

### 3.2 Packaging rational lifts together into a surface

In this section, we further investigate the surface (1.2) considered by Cheng and Huang. We see that this surface will play the role of the rank one lift we needed to establish the equivalence between the R1LH and the ECDLP when we now consider the equivalence of the R1SLP to the ECDLP.

Suppose we had some elliptic curve $\tilde{E} : y^2 = x^3 + \tilde{a}x + \tilde{b}$ over $\mathbb{F}_p$. Fix some non-zero $\mathbb{F}_p$ point $(\tilde{x}_0, \tilde{y}_0)$ on $\tilde{E}$. Choose rational numbers $a$, $x_0$, and $y_0$ that reduce to $\tilde{a}$, $\tilde{x}_0$, and $\tilde{y}_0$ mod $p$. As we remarked in the Introduction, every fiber $E_t$ of

$$E : y^2 = x^3 + (a + tp)x + (y_0^2 - x_0^3 - (a + tp)x_0)$$  \hspace{1cm} (1.2 revisited)

is a rational lift of $\tilde{E}$ except for those $t$ such that $p$ divides the denominator of $t$. Furthermore, all of these lifts contain the non-zero rational point $(x_0, y_0)$. We will work with this surface throughout the remainder of the chapter.

On the other hand, every rational lift of $\tilde{E}$ that contains the rational point $(x_0, y_0)$ is a fiber of $E$. Indeed, if $y^2 = x^3 + a_1x + b_1$ is some lift of $\tilde{E}$ to $\mathbb{Q}$ that contains $(x_0, y_0)$, then $a_1$ is a lift of $\tilde{a}$, so $a_1 = a + tp$ for some $t \in \mathbb{Q}$ and $b_1 = y_0^2 - x_0^3 - a_1x_0 = y_0^2 - x_0^3 - (a + tp)x_0$.

We can equivalently consider $E$ as an elliptic curve $E$ over $\mathbb{Q}(t)$. We note:

**Lemma 3.2.1.** The elliptic curve $E$ over $\mathbb{Q}(t)$ has $j$-invariant

$$j(t) := j(E_t) = \frac{(-48(a + tp))^3}{-64(a + tp)^3 - 432(y_0^2 - x_0^3 - (a + tp)x_0)^2}.$$
and discriminant
\[ \Delta(t) := \Delta(E_t) = -64(a + tp)^3 - 432(y_0^2 - x_0^3 - (a + tp)x_0)^2. \]

Furthermore,
\[ c_4(t) := c_4(E_t) = -48(a + tp) \quad \text{and} \quad c_6(t) := c_6(E_t) = -864(y_0^2 - x_0^3 - (a + tp)x_0). \]

Proof. The quantities involved in these computations are:
\[ a_1 = a_2 = a_3 = 0, \quad a_4 = a + tp, \quad a_6 = y_0^2 - x_0^3 - (a + tp)x_0, \]
\[ b_2 = 0, \quad b_4 = 2(a + tp), \quad b_6 = a_3^2 + 4a_6 = 4(y_0^2 - x_0^3 - (a + tp)x_0), \]
\[ c_4 = b_2^2 - 24b_4 = -48(a + tp), \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6 = -864(y_0^2 - x_0^3 - (a + tp)x_0). \]

Then,
\[ \Delta(t) = -8b_4^3 - 27b_6^2 = -64(a + tp)^3 - 432(y_0^2 - x_0^3 - (a + tp)x_0)^2, \]
and
\[ j(t) = \frac{c_4^3}{\Delta(t)} = \frac{(-48(a + tp))^3}{-64(a + tp)^3 - 432(y_0^2 - x_0^3 - (a + tp)x_0)^2}. \]

We see that if \( j(t) \) is constant and equal to \( K \), then
\[ (a + tp)^3((-48)^3 + 64K) = -432K \left(y_0^2 - x_0^3 - (a + tp)x_0\right)^2. \]

Hence, we must have \( x_0 = 0, \ y_0^2 - x_0^3 = 0, \) and \((-48)^3 + 64K = 0\), otherwise we have a cubic polynomial in \((a + tp)\) identically equal to a quadratic polynomial in \((a + tp)\). So \( j(t) \) is non-constant unless \( x_0 = y_0 = 0 \). In this case our surface reduces to
\[ y^2 = x^3 + (a + tp)x \]

which is not a constant family \( \mathbb{Q} \), although it is over \( \overline{\mathbb{Q}} \).

We note:

**Proposition 3.2.2.** For any elliptic curve \( \tilde{E} : y^2 = x^3 + \tilde{a}x + \tilde{b} \) over \( \mathbb{F}_p \) (\( p \geq 5 \)) there exists a lift over \( \mathbb{Q} \) that has non-trivial reduction mod \( p \).
Chapter 3. A variant on the R1LP

Proof. As \( p \geq 5 \), by Hasse’s bound, there is a non-zero point \( \tilde{P} = (\tilde{x}_0, \tilde{y}_0) \) on \( \tilde{E} \) over \( \mathbb{F}_p \). Choose \( a, x_0 \), and \( y_0 \) in \( \mathbb{Q} \) that lift \( \tilde{a}, \tilde{x}_0, \tilde{y}_0 \), and choose \( t \in \mathbb{Z} \). Then, \( \Delta(E_t) \equiv \Delta(\tilde{E}) \mod p \), so \( E_t \) has good reduction mod \( p \) and \( (x_0, y_0) \in E_t \) reduces to \( \tilde{P} \) which is a non-zero point.

An elliptic surface is said to be rational if it is birational to \( \mathbb{P}^2 \). Recall that if
\[
y^2 = x^3 + A(t)x + B(t)
\]
is a minimal Weierstrass model of an elliptic surface over \( \mathbb{Q}(t) \), then this surface is rational if and only if one of the following conditions holds: (see [1] and [31])

- \( 0 < \max\{3 \deg A(t), 2 \deg B(t)\} < 12 \)
- \( 3 \deg A(t) = 2 \deg B(t) = 12 \) and \( \text{ord}_{t=0} t^{12}\Delta(t^{-1}) = 0 \).

So we see:

**Lemma 3.2.3.** Choose \( a, x_0, \) and \( y_0 \) in \( \mathbb{Q} \) as above such that \( x_0 \) and \( y_0 \) are not both zero. Then \( \mathcal{E} \) is a non-constant rational surface.

**Proof.** We see that \( \mathcal{E} \) is non-constant by the remarks following Lemma 3.2.1. Note \( E \) is of the form \( y^2 = x^3 + A(t)x + B(t) \) for \( A(t) \) and \( B(t) \) linear polynomials. Specifically, the orders of vanishing of \( A(t) \) and \( B(t) \) at any irreducible polynomial are less than 4 and 6 respectively, so our model is minimal (see [32, Section 4.8]). Hence, it gives a rational surface by the first case of the criterion.

**Proposition 3.2.4.** Choose \( a, x_0, \) and \( y_0 \) in \( \mathbb{Q} \) as above such that \( x_0 \) and \( y_0 \) are not both zero. Then generic rank \( (E) = 1 \).

**Proof.** We use methods of [1]. By Lemma 3.2.3, \( \mathcal{E} \) is a non-constant rational surface. So as noted in Section 3.1 by Rosen-Silverman ([31]) we know Tate’s Conjecture and hence Nagao’s Conjecture ([27]) for this surface.

For any prime \( q \) we denote by \( a_t(q) \) the \( q \)th coefficient of the \( L \)-series of the fiber \( E_t \). Then, \( a_t(q) = q + 1 - N_t(q) \) where \( N_t(q) \) is the number of points in \( E_t(\mathbb{F}_q) \) for \( q \) at which \( E_t \) has good reduction, and \( a_t(q) = 0, 1, \) or \(-1\) if \( E_t \) has bad reduction at \( q \).
(depending on the type of bad reduction). Thus, as we saw in Section 3.1, we compute:

\[ A_E(q) = \frac{1}{q} \sum_{t=0}^{q-1} a_t(q), \]

and then as this is a known case of Nagao’s Conjecture, we have

\[
\text{generic rank}(E) = \lim_{X \to \infty} \frac{1}{X} \sum_{q \leq X} -A_E(q) \ln q.
\]

Define \( f_p(x, t) = x^3 + (a + tp)x + (y_0^2 - x_0^3 - (a + tp)x_0) \). Then, for \( t \) such that \( \Delta(t) \not\equiv 0 \mod q \),

\[
a_t(q) = q + 1 - N_t(q) = q + 1 - \left( 1 + \sum_{x=0}^{q-1} \begin{cases} 2 & \text{if } \left( \frac{f_p(x, t)}{q} \right) = 1 \\ 1 & \text{if } \left( \frac{f_p(x, t)}{q} \right) = 0 \\ 0 & \text{if } \left( \frac{f_p(x, t)}{q} \right) = -1 \end{cases} \right) = \sum_{x=0}^{q-1} \left( \frac{f_p(x, t)}{q} \right).
\]

So,

\[
\text{rank}(E) = \lim_{X \to \infty} \frac{1}{X} \sum_{q \leq X} -A_E(q) \ln q
= \lim_{X \to \infty} \frac{1}{X} \sum_{q \leq X} \ln q \left( -\frac{1}{q} \sum_{t=0}^{q-1} a_t(q) \right)
= \text{Main Term} + \text{Error},
\]

where

\[
\text{Main Term} = \lim_{X \to \infty} \frac{1}{X} \sum_{q \leq X} \left( \frac{\ln q}{q} \sum_{t=0}^{q-1} \sum_{x=0}^{q-1} \left( \frac{f_p(x, t)}{q} \right) \right),
\]

and the error term corresponding to \( t \)’s such that \( \Delta(t) \equiv 0 \mod q \) is

\[
\text{Error} = -\lim_{X \to \infty} \frac{1}{X} \sum_{q \leq X} \left( \frac{\ln q}{q} \sum_{t=0}^{q-1} \sum_{x=0}^{q-1} \left( a_t(q) + \sum_{x=0}^{q-1} \left( \frac{f_p(x, t)}{q} \right) \right) \right).
\]

Then,
Main Term = \( \lim_{X \to \infty} \frac{1}{X} \sum_{q \leq X} \left( \frac{\ln q}{q} \sum_{x=0}^{q-1} \sum_{t=0}^{q-1} \left( \frac{x^3 + (a + tp)x + (y_0^2 - x_0^3 - (a + tp)x_0)}{q} \right) \right) \).

However,

\[
\sum_{t=0}^{q-1} \left( \frac{tp(x - x_0) + x^3 + ax + y_0^2 - x_0^3 - ax_0}{q} \right) = \begin{cases} 
q \left( \frac{x^3 + ax + y_0^2 - x_0^3 - ax_0}{q} \right) & \text{if } q | p(x - x_0) \\
0 & \text{otherwise}
\end{cases},
\]

so

\[
\text{Main Term} = \lim_{X \to \infty} \frac{1}{X} \left( \sum_{q \leq X} \frac{\ln q}{q} \left( \frac{x_0^3 + ax_0 + y_0^2 - x_0^3 - ax_0}{p} \right) + \text{term from } q = p \right)
\]

\[
= \lim_{X \to \infty} \frac{1}{X} \left( \sum_{q \leq X} \ln q + \text{term from } q = p \right)
\]

= 1 by the Prime Number Theorem.

To bound the error term we consider the \( t \) such that \( \Delta(t) \equiv 0 \mod q \). Note that \( \Delta(t) \) is a cubic polynomial whose coefficients depend on \( a, x_0, \) and \( y_0 \). We see that \( \Delta(t) \) is not the zero polynomial over \( \mathbb{Q} \), as it has a leading coefficient of \(-64p^3\). If \( q \) is 2 or \( p \), \( \Delta(t) \) may be the zero polynomial mod \( q \); however, for large \( q \) there are at most three roots \( t \) in \( \mathbb{F}_q \). Hence,

\[
|\text{Error}| \leq \lim_{X \to \infty} \frac{1}{X} \left[ \sum_{q \leq X} \frac{\ln q}{q} \left( 3 + 3 \sum_{x=0}^{q-1} \frac{f_p(x, t)}{q} \right) \right] + \text{term corresponding to finitely many } q.
\]

Note for all \( q \) large enough so that the leading coefficient of \( f_p(x, t) \) does not reduce to zero mod \( q \), \( f_p(x, t) \) is a cubic and hence has odd order over \( \mathbb{F}_q \). So, in particular, it is not equivalent to a constant times a square mod \( q \). Hence, Weil’s Theorem on character sums applies to \( f_p(x, t) \) mod \( q \) and \( \left| \sum_{x=0}^{q-1} \frac{f_p(x, t)}{q} \right| \leq 2\sqrt{q} \).

So,

\[
|\text{Error}| \leq \lim_{X \to \infty} \frac{1}{X} \left[ \sum_{q \leq X} \frac{\ln q}{q} (9\sqrt{q}) + \text{term corresponding to finitely many } q \right].
\]

However, for any \( \epsilon > 0 \), \( \frac{\ln q}{\sqrt{q}} \leq \epsilon \) for all but finitely many \( q \), so
\[|\text{Error}| \leq 9 \lim_{X \to \infty} \frac{1}{X} \left[ \sum_{q \leq X} \epsilon + \text{term corresponding to finitely many } q \right] \leq 9\epsilon.\]

As \( \epsilon \) is arbitrary, we must have \( \text{Error} = 0 \), so indeed \( \text{rank}(E) = 1 \).

We commented in the Introduction that according to Lang’s Conjecture it should be very straightforward to compute a lower bound for the height of the non-torsion points on an elliptic curve over \( \mathbb{Q} \). Hindry and Silverman have shown this conjecture to be true in the function field case ([16, Theorem 0.2]). We apply this to see:

**Lemma 3.2.5.** Let \( p > 23 \) and \( \tilde{E} \) an elliptic curve such that \( \#\tilde{E}(\mathbb{F}_p) = l \) is prime. Construct \( E \) from \( p \) and \( \tilde{E} \) as above such that \( x_0 \) and \( y_0 \) are not both zero. Then for all non-zero \( P \in E(\mathbb{Q}(t)) \),

\[ \hat{h}(P) \geq 3 \cdot 10^{-12.6}. \]

**Proof.** We saw that \((x_0, y_0)\) is a non-trivially reducing point on \( E_t \) for all \( t \in \mathbb{Z} \). As \( E_t \) reduces to \( \tilde{E} \) which has prime order, by Proposition 1.1.7 any non-zero point on \( E_t \) must be non-torsion. As \( P \) is non-zero, it can only specialize to zero on finitely many fibers. Choose some \( t_0 \in \mathbb{Z} \) where \( P \) specializes to a non-zero point; then specialization of \( P \) to the fiber \( E_{t_0} \) must be non-torsion. However, any torsion section specializes to torsion points at each non-singular fiber. Hence \( P \) is non-torsion as a point in \( E(\mathbb{Q}(t)) \). Note that the degree of \( \Delta(t) \) is three (regardless of our choices of \( a, x_0, \) and \( y_0 \)) by Lemma 3.2.1. Then the statement follows from [16, Theorem 0.2].

Following the notation of the Introduction we denote

\[ L := 3 \cdot 10^{-12.6} \quad (3.1) \]

and

\[ W := (x_0, y_0) \in E(\mathbb{Q}(t)). \quad (3.2) \]

**Lemma 3.2.6.** The canonical height of \( W \) as defined by equation (3.2) is absolutely bounded independent of \( \tilde{E} \) and \( p \) and independent of the choices of \( a, x_0, \) and \( y_0 \). Specifically, \( \hat{h}(W) \leq \frac{5}{2} \).
Proof. As \((x_0, y_0)\) has constant coordinate polynomials, the naive height, \(h(W)\), of \(W\) is zero. On the other hand, we compute

\[
h(E) = 3 \deg(a + tp) + 2 \deg \left( y_0^2 - x_0^3 - (a + tp)x_0 \right) = 5.
\]

However,

\[
\left| \hat{h}(W) - \frac{1}{2} h(W) \right| \leq \frac{1}{2} h(E).
\]

(See, for example, [36, Exercise 3.11].)

We see:

Lemma 3.2.7. Suppose \(f\) is a function such that

\[
f(x) \geq 2x + \left( \frac{1}{\ln 2} \left( 2x + \ln(5 \cdot 10^{12.6}) + 2 \right) \right)^2 + \ln 8 - \ln(3 \cdot 10^{-12.6})
\]

for all positive values of \(x\). Then, if \(L\) and \(W\) are as defined in equations (3.1) and (3.2),

\[
\hat{h}(W) \leq \frac{L 2\sqrt{f(\ln p) + \ln(8p^2) - 2}}{4p^2} - 1 - 1
\]

and

\[
L \geq \frac{2p^2}{e^{f(\ln p)}}.
\]

Proof. By Lemma 3.2.6, to see the first claim, it is sufficient to see that, under these assumptions,

\[
\frac{5}{2} \leq \frac{3 \cdot 10^{-12.6} 2\sqrt{f(\ln p) + \ln(3 \cdot 10^{-12.6}) - \ln(8p^2) - 2}}{4p^2} - 1 - 1.
\]

Solving for \(f(\ln p)\), this is equivalent to

\[
f(\ln p) \geq \left( \frac{1}{\ln 2} \ln \left( \frac{(14p^2 + 1)10^{12.6}}{3} \right) \right)^2 + \ln(8p^2) - \ln(3 \cdot 10^{-12.6})
\]

for which it is sufficient to have

\[
f(\ln p) \geq \left( \frac{1}{\ln 2} \ln \left( (5p^2)10^{12.6} \right) \right)^2 + \ln(8p^2) - \ln(3 \cdot 10^{-12.6}).
\]

We have this by plugging in \(x = \ln p\).

For the second claim, note that we have,
\[ f(\ln p) \geq 2\ln p - \ln \left( \frac{3}{8} \cdot 10^{-12.6} \right), \]

so

\[ e^{f(\ln p)} \geq \frac{p^2}{3 \cdot 10^{-12.6}} \Rightarrow \frac{2p^2}{e^{f(\ln p)}} \leq \frac{6p^2(10^{-12.6})}{8p^2} \leq 3 \cdot 10^{-12.6} \]

as desired.

\[ \]

Note that these are the same bounds on \( \hat{h}(W) \) and \( L \) that we wanted for the \( W \) and \( L \) found by the R1LH. This motivates the definition:

**Definition 3.2.8.** A function \( f : \mathbb{R}_{\geq 0} \to \mathbb{R} \) is said to be “very good” if

\[ f(x) \geq 2x + \left( \frac{1}{\ln 2} \left( 2x + \ln(21 \cdot 10^{12.6} + 1) + 2 \right) \right)^2 + \ln 8 - \ln(3 \cdot 10^{-12.6}) \]

for all (positive) \( x \).

As we noted in the Introduction, there are methods to efficiently compute the canonical heights of points on elliptic curves over \( \mathbb{Q}(t) \) (see, again, [37]). Thus, before using a R1SLP oracle to solve an instance of the ECDLP, one needs to compute \( h_W \) such that \( \left| h_W - \hat{h}(W) \right| \leq \frac{e^{f(\ln p)}}{4p^2} \) and such that the numerator and denominator of \( h_W \) are each of size at most \( f(\ln p) \), i.e. are at most \( e^{f(\ln p)} \). Note that the canonical heights of points on elliptic curves over \( \mathbb{Q}(t) \) are always rational (see [36] Ch. 3, Remark 4.3.1), so one can reasonably hope to just compute \( \hat{h}(W) \) exactly.

### 3.3 Equivalence of the R1SLP with the ECDLP

We now have the tools to prove Theorem 1.3.2 from the Introduction.

**Theorem 3.3.1.** Suppose \( f \) is a very good function. Let \( p > 23 \) and \( \tilde{E} \) an elliptic curve over \( \mathbb{F}_p \) such that \( \# \tilde{E}(\mathbb{F}_p) = l \) is prime. Construct \( E \) and \( W \) as in Section 3.2 such that \( x_0 \) and \( y_0 \) are not both zero. Compute \( h_W \) such that \( \left| h_W - \hat{h}(W) \right| \leq \frac{1}{4e^{f(\ln p)}} \) and such that \( H(h_W) \leq e^{f(\ln p)} \). Then there is an equivalence between ECDLP(\( \tilde{E}, p, -, - \)) and R1SLP(\( \tilde{E}, p, E, W, h_W, -, f, \frac{p^2}{e^{f(\ln p)}} \)) that runs in \( \max \{ O(f(\ln p)), \text{poly}(\ln p) \} \) many steps. Here \( \text{poly} \) is a fixed polynomial and the constant in the \( O \) is absolute.

**Proof.** We argue similarly to the proof of Theorem 1.1.12. The results of Section 3.2 essentially prove the R1LH in this case except that we do not have a theoretical bound.
on the time required to compute $h_W$. Note that $E_{t=0}$ is a lift of $E(\tilde{F}_p)$ (and in particular a fiber of good reduction) mod $p$ because $0 \in \mathbb{Z}$.

**R1SLP $\Rightarrow$ ECDLP**

Suppose we are given $\tilde{P}$ and $\tilde{Q}$ on $\tilde{E}(\mathbb{F}_p)$ and we want to find $n$ such that $\tilde{Q} = n\tilde{P}$. Then we use our R1SLP oracle to find $P$ and $Q$ in $E(\mathbb{Q}(t))$ such that $P(0)$ and $Q(0)$ on $E_{t=0}(\mathbb{Q})$ are lifts of $\tilde{P}$ and $\tilde{Q}$ respectively. We note that, by Proposition 3.2.4, $E(\mathbb{Q}(t))$ has rank one so $P$ and $Q$ are multiples of some unknown generator $R$ of $E(\mathbb{Q}(t))$: $P = n_1R$ and $Q = n_2R$. Hence upon specializing to the fiber $t = 0$: $P(0) = n_1R(0)$ and $Q(0) = n_2R(0)$, and then reducing mod $p$:

$$\tilde{P} \equiv n_1\overline{R(0)} \text{ and } \tilde{Q} \equiv n_2\overline{R(0)} \mod p,$$

where $\overline{R(0)}$ is the reduction of $R(0)$ mod $p$. Then,

$$n \equiv \frac{n_2}{n_1} = \sqrt{\frac{n_2^2h(R)}{n_1^2h(R)}} = \sqrt{\frac{h(Q)}{h(P)}} \mod \#\tilde{E}(\mathbb{F}_p).$$

Now we can argue that the precision with which we have approximated $\sqrt{\frac{h(Q)}{h(P)}}$ by $\sqrt{\frac{h(Q)}{h(P)}}$ is sufficient to correctly identify $\frac{n_2}{n_1}$ by an identical argument to that in the proof of Theorem 1.1.12.

**ECDLP $\Rightarrow$ R1SLP**

We use our ECDLP oracle to solve $\tilde{P} = n\tilde{W}(0)$ for some $n$ where $\tilde{W}(0)$ is the reduction mod $p$ of the specialization of $W$ to the fiber $E(0)$. (Note that $\tilde{E}(\mathbb{F}_p)$ is cyclic because it is of prime order so such an $n$ can be found.) By Hasse’s bound as $p > 23$, $\#\tilde{E}(\mathbb{F}_p) \leq 2p$, so we can reduce $n$ so that it is without loss of generality less than $2p$. Then we will output $h = n^2h_W$. We note that $|h - \tilde{h}(P)| = |n^2h - n^2\tilde{h}(P)| = n^2|h_W - \tilde{h}(W)| \leq \epsilon$ where $P = nW$ specializes to $nW(0)$ at $t = 0$, which is a lift of $\tilde{P}$. Note that the numerator and denominator of $h$ are both at most $e^{f(\ln p)}$, as we assumed the numerator of $h_W$ is at most $\frac{e^{f(\ln p)}}{4p^2}$.

Remark 3.3.2. So, as we have seen that the R1SLP is equivalent to the ECLP, the R1SLP is equivalent to the R1LP if we assume Conjecture 1.1.10. As the R1SLP and the R1LP are very similar, we might expect an equivalence between them that does not go through the ECDLP. Indeed, assuming Conjecture 1.1.10, we can intuitively see how we might reduce the R1LP from the R1SLP. Suppose we have found a lift $E$ of $\tilde{E}$ that contains a non-trivially reducing point $(x_0, y_0)$. Then we can use $(x_0, y_0)$ to construct a
surface of the form (1.2) and, as we saw above, $E$ must be one of its fibers. We do a change of variables (by changing our choice of $a$) so that this fiber is, in fact, the fiber corresponding to $t = 0$. Then we can use our R1SLP oracle to lift to a section $P(t)$. This section can be specialized to the point $P(0)$, which reduces to $\tilde{P}$ mod $p$; namely, we have found a rational lift on $E$ that reduces to $\tilde{P}$ mod $p$. It is not immediately obvious how $\hat{h}(P(t))$ relates to $\hat{h}(P(0))$ (where these are respectively the canonical heights over $\mathbb{Q}(t)$ and $\mathbb{Q}$), which prevents us from formalizing this argument, but it is intuitive that lifting to sections should be at least as hard as lifting to a single point. The other direction is less evident.

**Question 3.3.3.** If Conjecture [1.1.10] holds, is there a direct reduction from the R1LP to the R1SLP without going through the ECDLP?

### 3.4 Some comments on the rank distribution of surface (1.2)

As we commented in the Introduction, Cheng and Huang ([5]) hoped to be able to find rank one lifts with non-trivial reduction by choosing random fibers from surface (1.2). Indeed, according to folklore one expects

$$\frac{1}{2X} \sum_{|t| \leq X} \text{rank}E_t(\mathbb{Q}) = \text{rank}E(\mathbb{Q}(t)) + \frac{1}{2}.$$ 

On the other hand, we have Silverman’s Specialization Theorem:

**Theorem 3.4.1** (Silverman, see [33] and [35]). If $E$ is a non-constant elliptic curve over $\mathbb{Q}(t)$, then for all but finitely many $t_0 \in \mathbb{Q}$ the specialization map

$$E(\mathbb{Q}(t)) \rightarrow E_{t_0}(\mathbb{Q})$$

is injective and consequently

$$\text{rank}(E(\mathbb{Q}(t))) \leq \text{rank}(E_{t_0}(\mathbb{Q})).$$

We saw in Proposition [3.2.4] that $\text{rank}E(\mathbb{Q}(t)) = 1$ for our surface, so only finitely many of its fibers can have rank less than one. Thus, we expect that if we choose a random $t \in \mathbb{Z}$, that $E_t$ will be a lift of rank one with non-trivial reduction (at least) half of the time. Our understanding of the distribution of the ranks of the fibers of elliptic
surfaces is currently far from being able to prove that such a procedure will work. In this section, we will survey what the known results on rank distribution say about surface (1.2).

3.4.1 A bound on the average rank of surface (1.2)

We will apply the bound on average rank established by Silverman in [38]; following his notation we define the conductor polynomial of $E$ as:

\[ N(t) = \prod_{\Delta(\alpha)=0} (t - \alpha) \times \prod_{c_4(\alpha)=c_6(\alpha)=0} (t - \alpha). \]

Then one has:

**Theorem 3.4.2** (Theorem 1 from [38]). Assume the Birch and Swinnerton-Dyer Conjecture and Riemann Hypothesis for elliptic curves for all fibers $E_t$, $t \in \mathbb{Z}$ and Tate’s Conjecture for the surface $E$ (see [38]). Then, as $X \to \infty$,

\[ \frac{1}{2X} \sum_{|t| \leq X} \text{rank} E_t(\mathbb{Q}) \leq \left( \text{rank} E(\mathbb{Q}(t)) + \text{deg} N(t) + \frac{1}{2} \right) (1 + o(1)). \]

We saw in the proof of Proposition 3.2.4 that surface (1.2) satisfies Tate’s Conjecture. Furthermore, by Lemma 3.2.1 we see that $c_4$ and $c_6$ only have common zeros if $x_0^3 = y_0^2$. For any given $E$ over $\mathbb{F}_p$ ($p \geq 5$), we can construct $E$ as above such that $x_0^3 \neq y_0^2$. Then, for this surface, $\text{deg} N(t) \leq 3$, and we saw in Proposition 3.2.4 that $E(\mathbb{Q}(t))$ has rank one, so the average rank is asymptotically bounded by 4.5 as $X \to \infty$. Hence:

**Proposition 3.4.3.** Assume the Birch and Swinnerton-Dyer Conjecture and the Riemann Hypothesis for all elliptic curves over $\mathbb{Q}$. Let $E$ be an elliptic curve over $\mathbb{F}_p$, $p \geq 5$. Then there exists a lift of $E$ to $\mathbb{Q}$ that has non-trivial reduction mod $p$ and rank at most 4.

We note that the lift we have produced may, a priori, have very large coefficients (relative to $p$) if the convergence in Theorem 3.4.2 is slow.
3.4.2 The average root number of surface (1.2)

In this section we will use results of Helfgott in [15] to calculate the average root number of surface (1.2). We recall that the $L$-function of an elliptic curve $E$ is given by:

$$L(E, s) = \prod_{E \text{ has good reduction mod } p} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \prod_{E \text{ has bad reduction mod } p} \left(1 - a_p p^{-s}\right)^{-1}$$

where $a_p$ is as above. Then, by the modularity theorem ([4]), we know $L(E, s)$ has analytic continuation to all of $\mathbb{C}$ and satisfies the functional equation:

$$\mathcal{N}_E^{(2-s)/2} (2\pi)^{s-2} \Gamma(2-s) L(E, 2-s) = W(E) \mathcal{N}_E^{s/2} (2\pi)^{-s} \Gamma(s) L(E, s),$$

where $W(E)$ is called the root number and is either $+1$ or $-1$ and $\mathcal{N}_E$ is the conductor of $E$. From this one can see

$$W(E) = (-1)^{\text{ord}_s=1 L(E, s)}. $$

The Birch and Swinnerton-Dyer conjecture implies that $\text{rank}(E) = \text{ord}_s=1 L(E, s)$. Thus, the root number can be see as a conjectural proxy for whether the rank of a curve is odd or even.

We will now introduce some of the notation of [15, Ch. 1] and recap the results that we will need.

**Definition 3.4.4.** We define a sector $S \subset \mathbb{R}^2$ to be a connected component of

$$\mathbb{R}^2 - \{ \text{a finite number of lines through the origin} \}.$$ 

Given a lattice $n\mathbb{Z} \times m\mathbb{Z} \subset \mathbb{Z}^2$, we define a lattice coset $L$ to be the coset of a lattice as a subgroup of $\mathbb{Z}^2$; namely, as a set of the form $(a, b) + n\mathbb{Z} \times m\mathbb{Z}$. We define $[\mathbb{Z}^2 : L] = n \cdot m$.

**Definition 3.4.5.** Let $E \in \mathbb{Q}(t)$. For $t \in \mathbb{Q}$ denote $W(t) := W(E_t)$. Then we define the average root number of “the rational fibers of $E$ up to $N$” over a sector $S$ and a lattice coset $L$ as:

$$\text{av}_{S \cap L \cap [-N,N]^2} W(E) = \frac{1}{\# \left\{ (x, y) \in S \cap L \cap [-N,N]^2 \mid \gcd(x, y) = 1 \right\}} \sum_{(x, y) \in S \cap L \cap [-N,N]^2 \mid \gcd(x, y) = 1} W \left( \frac{y}{x} \right).$$
We consider, analogously to the situation over $\mathbb{Q}$, the places at which we can reduce an element of $\mathbb{Q}(t)$. Specifically, for $P(t) \in \mathbb{Q}(t)$, the infinite place is given by the valuation $v(P(t)) = \deg(\text{den}(P(t))) - \deg(\text{num}(P(t)))$. The finite places correspond to primitive irreducible polynomials and the valuation $v(P(t))$ at some finite place is given by the multiplicity with which the corresponding primitive irreducible polynomial divides $P(t)$.

Then, given an elliptic curve $E$ over $\mathbb{Q}(t)$, $\Delta(t)$, $c_4(t)$, and $c_6(t)$ can be computed as in Lemma 3.2.1. If our model of $E$ is minimal with respect to a valuation $v$ then, as in case of curves over $\mathbb{Q}$, we say that $E$ has good reduction at the place corresponding to $v$ if $v(\Delta(t)) = 0$ and that it has bad reduction at $v$ otherwise. Furthermore, $E$ is said to have multiplicative reduction if $v(\Delta(t)) > 0$ and $v(c_4(t)) = 0$ and additive reduction if $v(\Delta(t)) > 0$ and $v(c_4(t)) > 0$.

**Definition 3.4.6.** Consider $E \in \mathbb{Q}(t)$. Helfgott defines:

$$M_E(x, y) = \prod_{E \text{ has multiplicative \ reduction at } v} P_v(x, y),$$

where $P_v(x, y) = x$ if $v$ is the infinite place and $P_v(x, y) = x^{\deg Q}Q\left(\frac{y}{x}\right)$ if $v$ is the place corresponding to the primitive irreducible polynomial $Q$.

Further, Helfgott defines an elliptic surface:

$$E_t : y^2 = x^3 - \frac{c_4(t)}{48} - \frac{c_6(t)}{864}$$

to have “quite bad reduction at $v$” if there is no $d(t)$ for which

$$d(t)y^2 = x^3 - \frac{c_4(t)}{48} - \frac{c_6(t)}{864}$$

has good reduction. Then he writes

$$B'_E(x, y) = \prod_{E \text{ has quite bad \ reduction at } v} P_v(x, y).$$

Finally, for a polynomial $P = \prod Q_i^{k_i}$, define $\text{deg}_{\text{supp}} P = \max_i \{\deg(Q_i)\}$.

We can now introduce the major tool we draw from [15]:

**Theorem 3.4.7** (Theorem 1.3' of [15]). Let $E$ be a family of elliptic curves in one variable over $\mathbb{Q}$ (i.e. an elliptic curve over $\mathbb{Q}(t)$). Assume that $M_E$ is non-constant. Suppose that
Theorem 3.4.8. Let $\tilde{E}$ be an elliptic curve over $\mathbb{F}_p$ ($p \geq 5$) and construct $E$ as in Section 1.1.3 choosing $x_0$ and $y_0$ such that $x_0^3 \neq y_0^2$. Let $S = \mathbb{R}^2$ and $L = \mathbb{Z} \times (1 + p\mathbb{Z})$. Then

$$\lim_{N \to \infty} \frac{\text{av}}{S \cap L \cap [-N,N]^2} W(E) = 0.$$ 

Proof. We compute $\Delta(t)$ and $c_4(t)$ for this surface in Lemma 3.2.1. Note that the only irreducible polynomial that divides $c_4(t)$ is $a + tp$. However, $a + tp$ does not divide $\Delta(t)$ unless $y_0^2 = x_0^3$, which we have excluded. Thus, we must have that all of the irreducible factors of $\Delta(t)$ correspond to places of multiplicative reduction. As $\Delta(t)$ is non-constant in $t$ (its leading term in $t$ is $-64p^3t^3$), it has at least one irreducible factor that must divide $M_E$. Hence $M_E$ is non-constant.

Any contribution to $M_E$ coming from a finite place corresponds to an irreducible factor of $\Delta(t)$. However, note that $P_v(x,y)$ has the degree as the primitive irreducible polynomial $Q$ to which $v$ corresponds. Since $\text{deg}(\Delta(t)) = 3$, in order to see that $\text{deg}(M_E) \leq 3$, it suffices to see that $E$ does not have multiplicative reduction at the infinite place. Note that equation (1.2) is not a minimal Weierstrass equation at this place, as we compute:

$$v_\infty(\Delta_E) = \text{deg}(\text{den}(\Delta_E)) - \text{deg}(\text{num}(\Delta_E)) = 0 - 3 = -3$$

and

$$v_\infty(c_4) = \text{deg}(\text{den}(c_4)) - \text{deg}(\text{num}(c_4)) = 0 - 1 = -1.$$

The change of variables

$$(x, y) \mapsto (u^2 x, u^3 y),$$

which induces a change of Weierstrass form

$$E : y^2 = x^3 + a_4x + a_6 \to E' : y^2 = x^3 + u^4a_4x + u^6a_6,$$

yields

$$\Delta(E') = u^{12}\Delta(E) \text{ and } c_4(E') = u^6c_4(E).$$
(see [39, Ch. 3, Table 1.2]). So taking \( u = \frac{1}{t} \), we get
\[
v_{\infty}(\Delta_{E'}) = -3 + 12 = 9 \quad \text{and} \quad v_{\infty}(c_4) = -1 + 6 = 5.
\]
As both of these are positive, \( E \) has additive reduction at infinity. Hence, \( \deg(M_E) \leq 3 \).

Similarly,
\[
B'_E(x, y) \bigg| \prod_{E \text{ has bad reduction at } v} P_v(x, y).
\]
So, again, \( B'_E \) has at most degree three coming from finite place and degree one coming from the infinite place. Hence, \( \deg(B'_E) \leq 4 \). The result follows from Theorem 3.4.7.

\[\square\]

**Proposition 3.4.9.** Let \( \tilde{E} \) be an elliptic curve over \( \mathbb{F}_p \), \( p \geq 5 \). Let \( \epsilon = +1 \) or \( -1 \). Then, there exists a lift of \( \tilde{E} \) to \( \mathbb{Q} \) that has non-trivial reduction and whose root number is \( \epsilon \).

**Proof.** Note that \( E_t \) has non-trivial reduction for all \( t = \frac{x}{y} \) such that
\[
(x, y) \in L = \mathbb{Z} \times (1 + p\mathbb{Z})
\]
as \( p \) does not divide the denominator of such \( t \). Then the average
\[
\lim_{N \to \infty} \frac{1}{\mathbb{R}^2 \cap \mathbb{F}_p [-N,N]} W(E) = 0
\]
is an average of +1’s and −1’s that tends to zero as \( N \) goes to infinity. Thus, for sufficiently large \( N \) both +1 and −1 must appear in the sum.

\[\square\]

**Remark 3.4.10.** Note that we used the case of Theorem 3.4.7 where \( \deg(M_E) = 3 \). This is one of the deep aspects of Helgott’s work; he proved this case by proving a version of Chowla’s conjecture for cubic polynomials, which builds off the work of Friedlander and Iwaniec.

**Remark 3.4.11.** As we chose \( L = \mathbb{Z} \times (1 + p\mathbb{Z}) \), \( \mathbb{Z}^2 : L = p \). Hence, for a fixed constant \( A \), Theorem 3.4.7 only applies to \( N \) such that
\[
p \leq (\ln N)^A \iff e^{p^{1/A}} \leq N.
\]
Namely, in order to find a lift of \( \tilde{E} \) with a given root number, we would have to take an average over an extremely large number of lifts relative to \( p \), which will, in general, have extremely large coefficients.
Chapter 4

Diffusion of candidate lifts on cross-fibered surfaces

4.1 Cross-fibered surfaces

We recall some of the cases in which one has proven Conjecture 1.2.7. As we indicated in the Introduction, one type of special surface for which one has managed to prove this conjecture are surfaces with two distinct elliptic fibrations. Theorems of this form include:

**Theorem 4.1.1** (Theorem 3 from [30]). Let $a, b, c, e \in \mathbb{Q}$ such that $4a^3 + 27b^2 \neq 0$ and $c \neq 0$. Consider the elliptic surface

$$E_t : (ct^2 + e)y^2 = x^3 + ax + b.$$  \hfill (4.1)

Then, if there exists $t$ such that $ct^2 + e \neq 0$ and $\text{rank}(E_t) > 0$, then such $t$ are dense in $\mathbb{R}$.

**Theorem 4.1.2** (Theorem 1.9 from [24]). Let $\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, $ and $\theta \in \mathbb{Q}$ such that at least one of $\alpha$ or $\epsilon$ is non-zero. Consider the elliptic surface

$$E_t : y^2 = x^3 + C_1(t)x + C_2(t),$$  \hfill (4.2)

where $C_1(t) = \alpha t^3 + 3\beta t^2 + \gamma t + \delta$ and $C_2(t) = \epsilon t^3 + 3\zeta t^2 + \eta t + \theta$. Then, there exists an efficiently computable constant $M$ such that if this surface has more than $M$ fibers of positive rank, then such fibers are dense in $\mathbb{R}$.

**Theorem 4.1.3** (Theorem 1.7 from [24]). Let $b, \alpha, $ and $\beta \in \mathbb{Q}$ such that $b > 0$. Consider an elliptic surface of the form
$E_t : y^2 = x^3 + bC(t)^2,$

where $C(t) = t^3 + \alpha t + \beta$. Then, there exists an efficiently computable constant $M$ such that if there are more than $M$ fibers of positive rank, then such fibers are dense in $\mathbb{R}$.

All of these theorems depend on the fact that they concern surfaces with multiple fibrations in which the fibrations interact in well-behaved ways. We defined cross-fibered surfaces in Definition 1.3.4 of the Introduction to have the properties necessary for a similar argument to work. In this section we will further study such surfaces.

We defined cross-fibered surfaces as elliptic surfaces $E$ which are birational to some elliptic surface $E^*$ such that the fibrations of these two surfaces interact in certain ways. However, in many of the proofs it will be helpful to take explicit Weierstrass equations for the fibrations of $E$ and $E^*$ and to consider the birational map $\Phi$ and its inverse $\Phi^*$ in explicit variables. Here we fix notation that we will use to refer to these objects throughout this chapter when needed.

We write the fibration of the elliptic surface $E$ as:

$$\{E_t\} = \{(x, y, t) : y^2 = x^3 + a(t)x + b(t)\},$$

where $a(t)$ and $b(t)$ are rational functions in $t$, and the projection map $\pi$ is given by $\pi(x, y, t) = t$.

Similarly, we write the fibration of the elliptic surface $E^*$ as

$$\{E^*_s\} = \{(u, v, s) : v^2 = u^3 + c(s)u + d(s)\},$$

where $c(s)$ and $d(s)$ are rational functions in $s$, and the projection map $\pi^*$ is given by $\pi^*(u, v, s) = s$. Note that we have chosen affine models of $E$ and $E^*$. However, in doing so we lose little because most of our results will be about the diffusion of certain properties (see Definition 1.2.10), and the single fiber at $\infty$ does not affect such results.

Then we can write

$$\Phi(x, y, t) = (v(x, y, t), \nu(x, y, t), \sigma(x, y, t))$$

with coordinate functions defined by rational functions in $x$, $y$, and $t$ (that are globally defined except possibly off a finite number of closed curves) and

$$\Phi^*(u, v, s) = (\xi(u, v, s), \iota(u, v, s), \tau(u, v, s)).$$
with coordinate functions defined by rational functions in $u$, $v$, and $s$ (that are globally defined except possibly off a finite number of closed curves). Note that these birational maps are assumed to be defined over $\mathbb{Q}$; namely, all of the coefficients of the coordinate functions are rational.

Often, when we have a point $P = (x, y) \in E_t$ or a point $P^* = (u, v) \in E^*_s$, we condense notation by writing $\sigma(x, y, t) = \sigma(P)$, $v(x, y, t) = v(P)$, $\tau(u, v, s) = \tau(P^*)$, $\xi(u, v, s) = \xi(P^*)$ etc. Note that this matches the definitions of $\sigma(P)$ and $\tau(P^*)$ in the Introduction.

Further, recall that in Section 1.3 we introduced notation to abbreviate the action of the conversion maps $\Phi$ and $\Phi^*$. For $P \in \mathcal{E}$ (at which the map $\Phi$ is defined), we write $\Phi(P) = P^* \in E^*_\sigma(P)$, and for $P^* \in \mathcal{E}^*$ (at which the map $\Phi^*$ is defined) we similarly write $\Phi^*(P^*) = P^{**} \in E_{\tau(P)}$.

The essence of the proof of Theorems 4.1.1-4.1.3 is that rational non-torsion points “diffuse” from one fiber to another across the cross-fibers. We will see in this chapter that other properties are also diffusive (see Definition 1.2.10) from one fiber to another. This diffusion often takes the form of the following iterative process:

**Diffusion Process 4.1.4.** Take a starting point $P$ on some starting fiber $E_t$ of a cross-fibered surface. Then one can perform the following steps:

1. Multiply $P$ as a point on $E_t$ to get $nP$.

2. Convert $nP$ to the other fibration to get $(nP)^*$ on the fiber $E^*_\sigma(nP^*)$.

3. Multiply $(nP)^*$ as a point on $E^*_\sigma(nP^*)$ to get $m(nP)^*$.

4. Convert this point back to the original fibration to get $(m(nP)^*)^*$ on the fiber $E_{\tau(m(nP)^*)}$.

We write $t_{n,m} = \tau(m(nP)^*)$, so that $E_{t_{n,m}}$ is the resulting fiber of this process. Note that $t_{n,m}$ depends on the choice of $P \in E_t$ with which one starts.

For fixed $n$ and $m$, Diffusion Process 4.1.4 gives a map $\Phi_{n,m} : \mathcal{E} \rightarrow \mathcal{E}$ given by

$$P \mapsto (m(nP)^*)^* \in E_{t_{n,m}}.$$ 

Note that

$$\Phi_{n,m} = \Phi^* \circ [m] \circ \Phi \circ [n],$$

where $[n]$ and $[m]$ are the multiplication maps by $n$ and $m$ on their respective fibers. As the multiplication maps are dominant rational maps ([12, Remark 13.5.4]), $\Phi_{n,m}$ is a rational map.
Figure 4.1: An abstraction of the process of generating a point on a different fiber using the $\ast$ fibration. Multiply starting point by $n$, convert to the $\ast$ fibration, multiply by $m$, and convert back.

As all of the maps that define a pre-cross-fibration ($\Phi, \Phi^\ast, \pi, \pi^\ast$, and the coefficients of $E$ and $E^\ast$) are rational over $\mathbb{Q}$, we can reduce them mod $p$ for some prime $p$. Note that $\Phi$ and $\Phi^\ast$ still give a correspondence, and computing $\Phi$ and $\Phi^\ast$ commutes with reduction modulo $p$. Then, as long as $E_t$ and $E^\ast_{\pi(nP)}$ have good reduction mod $p$ and $\Phi$ and $\Phi^\ast$ are still defined at $nP$ and $m(nP)^\ast$ respectively after reducing mod $p$, we can perform the above Diffusion Process 4.1.4 over $\mathbb{F}_p$. In this chapter, we will often be concerned with, when performing this process, what is going on at the $\mathbb{Q}$ and $\mathbb{F}_p$ levels and how these pictures interact. As we mentioned in the Introduction, in these circumstances we shall treat $\mathcal{E}$ as having some fixed Weierstrass model over $\mathcal{E}$ so that the reduction mod $p$ is fixed.

We see we can lighten slightly the topological properties we require of cross-fibered surfaces in Property 3 of Definition 4.3.4.

**Proposition 4.1.5.** Let $\mathcal{E}$ be an elliptic surface with a pre-cross-fibration ($\mathcal{E}^\ast, \Phi, \Phi^\ast$), and assume $\mathcal{E}$ satisfies Properties 1 and 2 of Definition 4.3.4. Then, Property 3 of Definition 4.3.4 holds if and only if for all intervals $I \subseteq \mathbb{R}$ and for all but finitely many $t \in \mathbb{Q}$ such that $E_t$ has positive rank, there exists a non-empty open subset $U$ of $E_t^0(\mathbb{R})$ such that:

- there exists some point $P$ in $U$ at which $\Phi$ is defined and
- for all $P \in U \cap E_t(\mathbb{Q})$ (at which $\Phi$ is defined) such that $rk(E^\ast_{\sigma(P)}) > 0$, there exists a non-empty open subset $U^\ast$ of $E^0_{\sigma(P)}$ such that if $P^\ast \in U^\ast \cap E^0_{\sigma(P)}(\mathbb{Q})$ and $\Phi^\ast$ is defined at $P^\ast$, then $\tau(P^\ast) \in I$.

**Proof.** Suppose $\mathcal{E}$ satisfies the criteria of this proposition. Let $I \subset \mathbb{R}$ and let $E_t$ be a fiber (that is not one of the finitely many exceptions) of positive rank. Take $U$ to be the non-empty open set of $E_t^0(\mathbb{R})$ given to us by the assumption. Then, there exists some
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

$P \in U$ at which $\Phi$ is defined. By Proposition 1.2.4 the rational points of an elliptic curve with positive rank are dense on the identity component of the curve. However, $\Phi$ is only undefined on a finite collection of closed curves, so then there exist infinitely many such $P \in U \cap E(\mathbb{Q})$ where $\Phi$ is defined. By Property 1 of cross-fibered surfaces, for all but finitely many of these points, $rk(E^s_{\sigma(P)}) > 0$. Furthermore, as $\sigma$ is a non-constant rational function, these points are taken to infinitely many distinct $E^s_{\sigma(P)}$. We note $\Phi^*$ is only undefined on a finite collection of closed curves, and these closed curves can intersect only finitely many times with a given $E^s_{\sigma}$ for all but finitely many $E^s_{\sigma}$. Hence there exists $U^*$ such that for infinitely many points $P^* \in U^* \cap E^0_{\sigma(P)}(\mathbb{R}) \cap E_{\sigma(P)}(\mathbb{Q})$, $\Phi^*$ is defined and $\tau(P^*) \in I$.

On the other hand, suppose $\mathcal{E}$ satisfies Property 3 of cross-fiberedness. Specifically, for $t_0$ such that $E_{t_0}$ is not one of the exceptions, there exists

$$P_0 = (x_0, y_0) \in E^0_t(\mathbb{R}) \cap E_t(\mathbb{Q}) \text{ and } P_0^* = (u_0, v_0) \in E^0_{(x_0, y_0, t_0)}(\mathbb{R}) \cap E_{(x_0, y_0, t_0)}(\mathbb{Q})$$

such that $\tau(P_0^*) \in I$. Then as $\tau = \tau(u, v, s)$ is continuous, there exists some open set $V$ of $\mathbb{R}^3$ containing $(u_0, v_0, \sigma(x_0, y_0, t_0))$ such that if $(u, v, s) \in V$, then $\tau(u, v, s) \in I$. Without loss of generality, we assume that $V$ is an (open) cube (any open set in $\mathbb{R}^3$ contains a cube). Take $I^*_1$ to be the projection of $V$ to the $s$ coordinate, so $V = V_{u,v} \times I^*_1$. Furthermore, as the surface is defined by polynomials $c(s)$ and $d(s)$ and is hence continuous around the point $(u_0, v_0, \sigma(x_0, y_0, t_0))$, there is some interval $I^*_2$ of values of $s$ including $\sigma(x_0, y_0, t_0)$ such that if $s \in I^*_2$, then $V_{u,v} \cap E^s_{\sigma}(\mathbb{R}) \neq \emptyset$. Then, let $s \in I^* := I^*_1 \cap I^*_2$ (a non-empty interval as it contains $\sigma(x_0, y_0, t_0)$) such that $rk(E^s_{\sigma}) > 0$. The multiples of any non-torsion point on $E^s_{\sigma}$ are dense in the identity component of $E^s_{\sigma}(\mathbb{R})$, and hence there are (infinitely many) rational points in $U^* := V_{u,v} \cap E^s_{\sigma}(\mathbb{R})$ (an open subset of $E^s_{\sigma}(\mathbb{R})$) and hence in $V$. All points in $U^*$ such that $\Phi^*$ is defined are sent to $I$ under $t$. However, the map $\sigma$ is also continuous (specifically in $x$ and $y$ holding $t_0$ fixed). Thus, there exists $W$ open in $\mathbb{R}^2$ containing $(x_0, y_0)$ such that if $(x, y) \in W$ and $\Phi$ is defined, then $\sigma(x, y, t_0) \in I^*$. Then, $U := W \cap E^t_\sigma(\mathbb{R})$ is the non-empty open set of $E^0_t(\mathbb{R})$ that we want.

This proposition tells us that, when choosing $n$, we can “aim” for $U$ so that we will be guaranteed to have good choices for $m$.

It may seem odd, in Definition 1.3.4 and Proposition 4.1.5, that we treat the two components of $E_t(\mathbb{R})$ and $E^s_{\sigma}(\mathbb{R})$ differently when one of these is isomorphic to $(\mathbb{R}/\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. This is because the multiples of a non-torsion point on the non-identity component are
dense in all of $E_t(\mathbb{R})$, whereas multiples of a non-torsion point on the identity component are only dense in the identity component. Specifically, no multiple of a point on the identity component will ever go to the non-identity component. So, if we had a situation where we had $(nP)^*$ on the identity component of its curve and we were aiming for $U^*$ on the non-identity component, we would not be able to find a satisfactory $m$.

Then we see:

**Theorem 4.1.6.** Any cross-fibered surface satisfies Mazur’s Conjecture 1.2.7 (where the fibration in the statement of Conjecture 1.2.7 is the main fibration of the surface).

**Proof.** Take some fiber $E_t$ such that $t$ is not one of the finitely many exceptions to conditions 1 and 3 of Definition 1.3.4 (some such fiber is guaranteed to exist, otherwise the second alternative of Conjecture 1.2.7 holds) and such that the exceptional curve at which $\Phi$ is not defined intersects $E_t$ in, at most, finitely many points. Let $U$ be the non-empty open set of $E_0^0(\mathbb{R})$ given to us by Proposition 4.1.5. Then we can find $P$ in $U \cap E_t(\mathbb{Q})$.

Only finitely many $n$ are such that $\Phi$ is undefined at $nP$ or such that $(nP)^*$ is torsion. Furthermore, only finitely many $n$ will be such that the exceptional curves where $\Phi^*$ is not defined intersect $E^0_{i(nP)}$ at more than finitely many points. Then, as the multiples of $P$ are dense in $E^0_0(\mathbb{R})$, choose one of the infinitely many $n$ such that $nP \in U$ that avoids these cases.

Now, take the non-empty open set $U^*$ of $E^0_{\sigma(nP)}$ given to us by Proposition 4.1.5. By our choice of $n$ only finitely many $m$ are such that $\Phi^*$ is undefined at $m(nP)^*$, and only finitely many $m$ are such that $(m(nP)^*)^*$ is torsion. Then, for some other $m$, $(m(nP)^*)^*$ is a non-torsion point on the fiber $E_{t_{n,m}}$ where, by the choice of $U^*$,

$$t_{n,m} = \tau(m(nP)^*) \in I.$$ 

\[\square\]

Note that the requirements for a surface to be cross-fibered and the argument for Theorem 4.1.6 are particularly drawn from the arguments Munshi used to prove Theorem 4.1.2; however, there are elements of these ideas in the proofs of all of Theorems 4.1.1 - 4.1.3.

### 4.1.1 Showing that a surface is cross-fibered

With a careful reading of their proofs, we can restate Theorems 4.1.1, 4.1.2 and 4.1.3 as:
**Theorem 4.1.7.** Surfaces of the form (4.1), (4.2), and (4.3) are cross-fibered.

Towards the end of proving Theorem 4.1.7, we introduce a set of conditions sufficient for a surface to be cross-fibered that will be relatively easy to check. These mimic the properties proved by Munshi in [24] to prove that surfaces of the form (4.2) satisfy Mazur’s Conjecture.

A critical tool in his argument are the division polynomials (see, for example, [40, Theorems 3.10.1-3.10.3]); namely, the polynomials $\psi_m, \theta_m, \omega_m \in \mathbb{Q}[x, y]$ such that if $P = (x, y) \in E(\overline{\mathbb{Q}})$ is a non-zero point, one can express

$$mP = \left( \frac{\theta_m(x, y)}{\psi_m(x, y)^2}, \frac{\omega(x, y)}{\psi_m(x, y)^3} \right)$$

(supposing that $mP \neq O$, which happens if and only if $\psi_m(x, y) \neq 0$.)

The (denominator) polynomials are given recursively by:

- $\psi_1 = 1$
- $\psi_2 = 2y$
- $\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$
- $\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$
- $\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_m^2\psi_{m+1}^2, m \geq 2$
- $2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$

Note that $\psi_m^2$ does not depend on $y$, thus we think of it as a function in three variables: $\psi_m^2(x, A, B)$ that is homogeneous with weighting $x$ - weighted as one, $A$ - weighted as two, and $B$ weighted as three. Furthermore, the leading term in $x$ is $m^2x^{m^2-1}$.

Then for an elliptic surface with a pre-cross-fibration, we want to consider torsion and hence the division polynomials on both fibrations. Thus, if (following the notation of Definition 1.3.3) we have an elliptic surface $E$, whether a given point $P = (x, y) \in E_t$ is such that $P^* \in E^*_{s}$ is $m$-torsion will depend on the $m$-division polynomial with inputs $v(x, y, t), c(\sigma(x, y, t)),$ and $d(\sigma(x, y, t))$ in place of $x, A, and B$ respectively. Thus $P^*$ is $m$-torsion if and only if

$$\psi_m^2(x, y, t) := \psi_m^2\left(v(x, y, t), c(\sigma(x, y, t)), d(\sigma(x, y, t))\right)$$

is zero.
Similarly if $P^* = (u, v) \in E_s^*$, then $P^{**} \in E_t^{**}$ is $m$-torsion if and only if

$$\psi^*_m(u, v, s) := \psi_m^2(\xi(u, v, s), a(\tau(u, v, s)), b(\tau(u, v, s)))$$

is zero.

When possible, we use the elliptic curve equations

$$y^2 = x^3 + a(t)x + b(t) \quad \text{and} \quad v^2 = u^3 + c(s)u + d(c)$$

to reduce powers of $y^2$ and $v^2$ in $\psi^*_m$ and $\psi^{**}_m$ respectively so that the resulting rational functions are at most linear in $y$ respectively $v$.

We can also control whether the image of a point under the transformation goes to a singular fiber or not. Thus, if $(x, y) \in E_t$ is transformed to a point on $E_s^*$, this fiber is singular if and only if

$$\Delta^*(x, y, t) := \Delta(E_s^*) = 4c(\sigma(x, y, t))^3 + 27d(\sigma(x, y, t))^2$$

is zero. As $\sigma(x, y, t)$ is a rational function in $x$, $y$, and $t$, so is $\Delta^*(x, y, t)$.

Similarly, $(u, v) \in E_s^*$ is transformed to a point on a singular fiber if and only if

$$\Delta^{**}(u, v, s) := \Delta(E_t^{**}) = 4a(\tau(u, v, s))^3 + 27b(\tau(u, v, s))^2$$

is zero.

Again, we use the elliptic curve equations to reduce powers of $y^2$ and $v^2$ so that the resulting rational functions are at most linear in $y$ respectively $v$.

Furthermore, to get a handle on the degrees of these rational functions (where, as usual, the degree of a rational function is its highest power after reduction) that define a (pre)-cross-fibration, it is useful to define:

$$L(\mathcal{E}) = \max \left\{ \deg_x v, \deg_y v, \deg_x u, \deg_y u, \deg_x \nu, \deg_y \nu, \deg_x \sigma, \deg_y \sigma, \deg_x \xi, \deg_y \xi, \deg_x \xi, \deg_y \xi, \deg_y \xi, \deg_x \xi, \deg_x \tau, \deg_y \tau, \deg_x \tau, \deg_y \tau \right\}.$$

This will serve us as a useful measure of the “size” of $\mathcal{E}$ as a cross-fibered surface in terms of the sizes of the polynomials that give the conversions. Note that $L(\mathcal{E})$ will depend on the model of $E_t$ and $E_s^*$ that we choose. In general we will fix a model, but one might hope to minimize $L(\mathcal{E})$ by choosing a minimal model for $E_t$.

As we will often be considering composites of these functions as we convert back and forth between fibrations and we will want to know the degree of the result, we recall:
Proposition 4.1.8. Let $f$ and $g$ be rational functions.

- $\deg(f + g) \leq \deg(f) + \deg(g)$
- $\deg(fg) \leq \deg(f) + \deg(g)$
- Suppose $f$ is a rational function in $n$ variables and $g_1, \ldots, g_n$ are rational functions, then

$$\deg(f(g_1, \ldots, g_n)) \leq \sum_{i=1}^{n} \deg_{g_i}(f) \deg(g_i).$$

Now we can translate the requirements of cross-fibered surfaces into the following conditions:

Proposition 4.1.9. Let $\mathcal{E}$ be an elliptic surface with a pre-cross-fibration. Then,

1. If there exists at least one point $(x, y, t) \in \mathcal{E}$ at which the polynomial $\text{den}(\sigma(x, y, t))$ takes a non-zero value, then there are at most $3L(\mathcal{E})^2 + L(\mathcal{E})$ many values of $t$ such that the conversion $\ast$ is undefined at all points on $E_t$. On any other fiber $E_t$, there are at most $5L(\mathcal{E}) + 3$ many points at which $\ast$ is undefined.

2. If there exists at least one point $(x, y, t) \in \mathcal{E}$ at which $\Delta^*(x, y, t)$ takes a finite non-zero value, there are at most $72L(\mathcal{E})^3 + 24L(\mathcal{E})^2$ values of $t$ for which all points on $E_t$ are sent to singular fibers. For any other $t$, there are at most $120L(\mathcal{E}) + 6$ points on $E_t$ that are sent to singular fibers.

3. If there exists at least one point $(u, v, s) \in \mathcal{E}^*$ at which the polynomial $\text{den}(\tau(u, v, s))$ takes a non-zero value, then there are at most $3L(\mathcal{E})^2 + L(\mathcal{E})$ many values of $s$ such that the conversion $\ast$ is undefined at all points on $E_s^*$. On any other fiber $E_s^*$, there are at most $5L(\mathcal{E}) + 3$ many points at which $\ast$ is undefined.

4. If there exists at least one point $(u, v, s) \in \mathcal{E}^*$ at which $\Delta^{**}(u, v, s)$ takes a finite non-zero value, there are at most $72L(\mathcal{E})^3 + 24L(\mathcal{E})^2$ values of $s$ for which all points on $E_s^*$ are sent to singular fibers. For any other $s$, there are at most $120L(\mathcal{E}) + 6$ points on $E_s^*$ that are sent to singular fibers.

Proof. First we prove (2). $\Delta^*$ is a polynomial in $s$, which is a rational functions in $x$, $y$, and $t$, so we write

$$\Delta^* = \frac{\sum p_{k,i}(t)x^ky^i}{\sum q_{i,j}(t)x^iy^j}.$$
Here, as we can replace $y^2$ using the equation of the elliptic curve $y^2 = x^3 + a(t)x + b(t)$, we have $0 \leq i, j \leq 1$. As $\Delta^*$ takes at least one finite, non-zero value, at least one of the $p_{k,i}(t)$ and at least one of the $q_{l,j}(t)$ must be non-zero as functions in $t$. We will see that the only $t$ for which infinitely many points on $E_t$ can be transformed to points on singular fibers are those for which all the $p_{k,i}(t)$ or all the $q_{l,j}(t)$ are simultaneously zero.

The total number of such $t$ is at most twice the highest exponent of $t$ that occurs in

$$\Delta^* = (4c(\sigma(x, y, t))^3 + 27d(\sigma(x, y, t))^2).$$

Before the substitution replacing the powers of $y^2$, this has degree in $t$ at most

$$3 \deg_c \sigma + 2 \deg_c d \cdot \deg_t \sigma \leq 12L(\mathcal{E})^2.$$

Similarly, its degree in $y$ is at most

$$3 \deg_c \sigma + 2 \deg_c d \cdot \deg_y \sigma \leq 12L(\mathcal{E})^2.$$

Then, as each $y^2$ is replaced by a polynomial of degree at most $\deg_x a + \deg_x b \leq 6L(\mathcal{E})$, the total degree in $t$ is at most $12L(\mathcal{E})^2 + \frac{12L(\mathcal{E})^2}{2} \cdot 6L(\mathcal{E})$, so this gives us at most

$$72L(\mathcal{E})^3 + 24L(\mathcal{E})^2$$

total values of $t$ at which all the $p_{k,i}(t)$ or all the $q_{l,j}(t)$ can be simultaneously zero.

Suppose $t_0$ is some other value of $t$. If all of the $p_{k,i}(t_0)$ are zero (namely, if there is no power of $y$ in the numerator of $\Delta^*$) then num$(\Delta^*)(x, y, t_0)$ is a non-zero polynomial in $x$ of degree at most $30L(\mathcal{E})^2$ by similar reasoning to above, noting that we replace $y^2$ with a degree three polynomial in $x$. Hence, there are at most $30L(\mathcal{E})^2$ many values of $x$ at which $\Delta^*(x, y, t_0)$ can be zero. As each $x$-coordinate can correspond to up to two $y$ values on an elliptic curve, this gives us at most $60L(\mathcal{E})^2$ many points at which $\Delta^*(x, y, t_0)$ can be zero.

Alternatively, assume there is a non-zero $p_{k,i}(t_0)$. Then, as $y$ occurs to exactly the first power in the numerator of $\Delta^*$, we can solve num$(\Delta^*) = 0$ for $y$ as a rational function in $x$. Then, any point $(x, y) \in E_{t_0}$ such that $\Delta^*(x, y, t_0) = 0$ has to satisfy:

$$\left(\frac{\text{polynomial in } x \text{ of degree at most } \deg_x \Delta^*}{\text{polynomial in } x \text{ of degree at most } \deg_x \Delta^*}\right)^2 = x^3 + a(t_0)x + b(t_0).$$

Note this equation cannot be trivial as the left hand side has even degree and the right
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

hand side has odd degree. Thus, as again the degree of $\Delta^*$ in $x$ is at most $30L(\mathcal{E})$, the number of such $x$ is bounded by $60L(\mathcal{E})^2 + 3$. But then (as we had an equation expressing $y$ in terms of $x$ for these points) each $x$-coordinate corresponds to at most one point at which $\Delta^*(x, y, t_0) = 0$.

So, in either case, there are at most $60L(\mathcal{E})^2 + 3$ pairs $(x, y)$ such that $\Delta^*(x, y, t_0) = 0$. We prove similarly that there at most $60L(\mathcal{E})^2 + 3$ many pairs where $\Delta^*(x, y, t_0)$ is undefined. Hence, for $t_0$ not one of the $36L(\mathcal{E})^3 + 24L(\mathcal{E})^2$ many exceptional values, there are at most $120L(\mathcal{E}) + 6$ points on $E_{t_0}$ that are sent to singular fibers under $\ast$.

In order to prove (1), (3), and (4), we apply the same argument to the polynomials $\text{den}(\sigma(x, y, t))$, $\text{den}(\tau(x, y, t))$, and $\Delta^{**}$ respectively in place of $\Delta^*$. □

Thus we control the points on which the conversion $\ast$ is not defined (including when it sends a point to a singular fiber in the other fibration). Note Proposition 4.1.9 works over any field, so if we consider our pre-cross-fibration structure over $\mathbb{F}_p$, this proposition gives us bounds on bad reduction mod $p$.

Similarly, we have:

**Proposition 4.1.10.** Let $\mathcal{E}$ be an elliptic surface with a pre-cross-fibration. Then,

1. If there exists at least one point $(x, y, t) \in \mathcal{E}$ at which the polynomial $\text{den}(\nu(x, y, t))$ takes a non-zero value, then there are at most $3L(\mathcal{E})^2 + L(\mathcal{E})$ many values of $t$ such that all points on $E_t$ are sent to the zero point under $\ast$. On any other fiber $E_t$, there are at most $5L(\mathcal{E}) + 3$ many points that are sent to the zero point under $\ast$.

2. For $2 \leq m \leq 16$, if there exists at least one point $(x, y, t) \in \mathcal{E}$ at which $\psi_m^2(x, y, t)$ takes a finite non-zero value, then there are at most

$$2(m^2 - 1)(2L(\mathcal{E})^2 + L(\mathcal{E}))(3L(\mathcal{E}) + 1)$$

many values of $t$ such that all points on $E_t$ are sent to $m$-torsion points under $\ast$. On any other fiber $E_t$, there are at most

$$10(m^2 - 1)(2L(\mathcal{E})^2 + L(\mathcal{E})) + 6$$

many points that are sent to $m$-torsion points under $\ast$.

3. If there exists at least one point $(u, v, s) \in \mathcal{E}^*$ at which the polynomial $\text{den}(\xi(u, v, s))$ takes a non-zero value, then there are at most $3L(\mathcal{E})^2 + L(\mathcal{E})$ many values of $s$ such that all points on $E^*_s$ are sent to the zero point under $\ast$. On any other fiber $E^*_s$, there are at most $5L(\mathcal{E}) + 3$ many points that are sent to the zero point under $\ast$. 
4. For $2 \leq m \leq 16$, if there exists at least one point $(u, v, s) \in \mathcal{E}^*$ at which $\psi_m^{*2}(u, v, s)$ takes a finite non-zero value, then there are at most

$$2(m^2 - 1)(2L(\mathcal{E})^2 + L(\mathcal{E}))(3L(\mathcal{E}) + 1)$$

many values of $s$ such that all points on $E_s^*$ are sent to $m$-torsion points under $\ast$. On any other fiber $E_s^*$, there are at most

$$10(m^2 - 1)(2L(\mathcal{E})^2 + L(\mathcal{E})) + 6$$

many points that are sent to $m$-torsion points under $\ast$.

Proof. This is similar to the proof of Proposition 4.1.9. For (2), $\psi_m^{*2}$ is a polynomial in $u$, $v$, and $s$, which are rational functions in $x$, $y$, and $t$, so we can write

$$\psi_m^{*2} = \frac{\sum p_{m,k,i}^*(t)x^ky^i}{\sum q_{m,l,j}^*(t)x^ly^j}$$

using the equation of the elliptic curve $y^2 = x^3 + a(t)x + b(t)$ to replace any $y^2$ terms so that we have $0 \leq i, j \leq 1$. Then, we proceed to a similar analysis of the number of values of $t$ at which the $p_{m,k,i}^*(t)$ or the $q_{m,l,j}^*(t)$ are simultaneously zero, and, for $t_0$ not one of these values, the number of points $(x, y) \in E_{t_0}$ where $\psi_m^{*2}$ can be zero or undefined. When computing the degrees of the rational functions used in this computation, note we have that the degree of $\psi_m^{*2}$ is $m^2 - 1$, and by homogeneity, we know the largest power of $u$ is $m^2 - 1$ and the largest powers of $c(s)$ and $d(s)$ are at most $\frac{m^2 - 1}{2}$ and $\frac{m^2 - 1}{3}$ respectively.

To prove (1) we apply the same argument to the polynomial $\text{den}(\nu(x, y, t))$ which controls whether a $(x, y)$ is sent to the zero point. Then, to prove (3) and (4) we use the polynomials $\text{den}(\xi(u, v, s))$ and $\psi_m^{*2}(u, v, s)$ in place of $\text{den}(\nu(x, y, t))$ and $\psi_m^{*2}(x, y, t)$.

Note that for a cross-fibered elliptic surface $\mathcal{E}$ with maps $\nu$, $\sigma$, $\xi$, $\iota$, and $\tau$, as above, one cannot have $\text{den}(\sigma(x, y, t))$, $\Delta^*(x, y, t)$, $\text{den}(\nu(x, y, t))$, $\psi_m^*(x, y, t)$, $\text{den}(\tau(u, v, s))$, $\Delta^{**}(u, v, s)$, $\text{den}(\xi(u, v, s))$, or $\psi_m^{**}(u, v, s)$ identically zero on $\mathcal{E}$, as this would violate the requirements of parts 1 and 2 of Definition 1.3.4 that on all but finitely many fibers (of each fibration), only finitely many points can be sent to torsion points or points on singular fibers. We have now seen that this is, in fact, sufficient for a surface to satisfy parts 1 and 2 of this definition.
**Definition 4.1.11.** Let $\mathcal{E}$ be a cross-fibered elliptic surface. We call a fiber $E_t$ an exceptional fiber if it is one of the finitely many exceptions to part 1 of Definition 1.3.4. Similarly, we call a fiber $E_s^*$ an exceptional fiber if it is one of the finitely many exceptions to part 2 of Definition 1.3.4. In particular, singular fibers are exceptional.

Thus, Propositions 4.1.9 and 4.1.10 give us a bound on the number of exceptional fibers in terms of the degrees that define the cross-fibration.

Moreover, as we said that Proposition 4.1.9 made sense over any field, we define:

**Definition 4.1.12.** Let $p$ be a prime. We say a cross-fibered surface $\mathcal{E}$ has non-trivial reduction as a cross-fibered surface mod $p$ if none of $\text{den(\upsilon)}$, $\text{den(\sigma)}$, $\text{den(\xi)}$, $\text{den(\tau)}$, $\Delta^*$ and $\Delta^{**}$ are identically zero over $\mathbb{F}_p$.

Note that to have non-trivial reduction as a cross-fibered surface it is sufficient that there exist at least one non-zero point $(x, y)$ on a fiber $E_t$ of good reduction mod $p$, such that $(x, y)^*$ is a non-zero point on a fiber $E_s^*$ of good reduction mod $p$. Moreover, if $p$ is sufficiently large (relative to the number of exceptions in Proposition 4.1.9 and 4.1.10), then the existence of such a point is actually equivalent to non-trivial reduction as a cross-fibered surface.

Thus (for $p$ sufficiently large), this property is symmetric in the two fibrations; by converting the point given to us in one fibration to the other, it fulfills the requirement in the other fibration. Basically, a cross-fibered surface will have good reduction mod $p$ as long as it does not have too many exceptional curves on which $\Phi$ and $\Phi^*$ are undefined of too high degree relative to $p$.

### 4.1.2 Examples of cross-fibered surfaces

Now we can quickly exhibit the cross-fibrations of the above surfaces.

**Surfaces of the form (4.1)**

Let $a$, $b$, $c$ and $e$ be constants such that $4a^3 + 27b^2 \neq 0$ and $c \neq 0$. The two fibrations are:

$$E_t : y^2 = x^3 + \frac{a}{(ct^2 + e)^2} x + \frac{b}{(ct^2 + e)^3}$$

and

$$E_s^* : v^2 = u^3 + \frac{a}{c^2} u + \frac{b - es^2}{c^3}$$
with transition maps given by
\[
\Phi : (x, y) \in E_t \mapsto \left( \frac{x(ct^2 + e)}{c}, \frac{yt(ct^2 + e)}{c} \right) \in E_{g(ct^2 + e)}^* \\
\]
and
\[
\Phi^* : (u, v) \in E_s^* \mapsto \left( \frac{cus^2}{c^3v^2 + es^2}, \frac{s^3}{c^3v^2 + es^2} \right) \in E_{c^3v^2 + es^2}^*
\]
off the curves \( s = 0, c^3v^2 + es^2 = 0 \).

**Proof of Cross-fibration Properties**

We note
\[
\text{den}(\sigma) = 1, \text{den}(\upsilon) = c, \text{den}(\tau) = s, \text{ and} \\
\text{den}(\xi) = c^3v^2 + es^2 = c^3 \left( u^3 + \frac{a}{c^2} u + \frac{b - es^2}{c^3} \right) + es^2,
\]
which are all non-zero as functions on \( E \) as \( c \neq 0 \).

When computing \( \psi_2^{*2} \), we have formulas for the values of \( u \) and the coefficient polynomials \( C = c(s) \) and \( D = d(s) \) resulting from the conversion of \((x, y) \in E_t \) to the * fibration:
\[
u = \frac{x(ct^2 + e)}{c}, \quad C = \frac{a}{c},
\]
and
\[
D = b - es^2 \frac{c^3}{c^3} = \frac{b - e(y(ct^2 + e))^2}{c^3} = \frac{b(ct^2 - e) - e ((ct^2 + e)^3x^3 + a(ct^2 + e)x + b)}{c^3(ct^2 + e)}.
\]

Then, we note that for each \( m \), the \( m^2u^{m^2-1} \) term of \( \psi_m^{*2} \) is \( \left( \frac{x(ct^2 + e)}{c} \right)^{m^2-1} \) and contributes the highest power of \( t \) (as, after adjusting for the weighting, each power of \( u \) contributes degree two in \( t \), each power of \( C \) contributes nothing, and each power of \( D \) contributes \( \frac{1}{3} \)) and hence cannot be canceled. Thus, \( \psi_m^{*2} \neq 0 \) and its denominator will just be some power of \( c \) times some power of \((ct^2 + e)\) and hence not identically zero.

Furthermore,
\[
\Delta(E_s^*) = 4c(s)^3 + 27d(s)^2 \\
= 4 \left( \frac{a}{c^2} \right)^3 + 27 \left( \frac{b(ct^2 - e) - e ((ct^2 + e)^3x^3 + a(ct^2 + e)x + b)}{c^3(ct^2 + e)} \right)^2
\]
has degree 12 in \( t \) if \( e \neq 0 \) and constant term \( \frac{4c^3 + 27d^2}{c^2} \neq 0 \) if \( e = 0 \). Hence \( \Delta^* \neq 0 \) and its denominator will again just be some power of \( c \) times some power of \((ct^2 + e)\).

Similarly, when computing \( \psi^{**2} \neq 0 \), we have formulas for the values of \( x \) and the coefficient polynomials \( A = a(t) \) and \( B = b(t) \) resulting from the conversion of \((u, v) \) on
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

\( E^*_s: \)

\[
x = \frac{cus^2}{c^3v^2 + e^2} = \frac{cus^2}{c^3(u^3 + \frac{a}{c^2}u + \frac{b-es^2}{c^3})^2 + e^2},
\]

\[
A = \frac{a}{(ct^2 + e)^2} = \frac{as^4}{(c^3(u^3 + \frac{a}{c^2}u + \frac{b-es^2}{c^3})^2 + e^2)^2},
\]

and

\[
B = \frac{b}{(ct^2 + e)^3} = \frac{bs^6}{(c^3(u^3 + \frac{a}{c^2}u + \frac{b-es^2}{c^3})^2 + e^2)^3}.
\]

Thus, by homogeneity, when determining if this is zero, we can ignore the denominators and, as \( x \) contributes the only powers of \( u \), the \( m^2x^m - 1 \) term cannot be canceled for any \( m \). Further, the denominator is not the zero function as it is just a multiple of

\[
\left( c^3\left(u^3 + \frac{a}{c^2}u + \frac{b-es^2}{c^3}\right)^2 + e^2 \right)^3,
\]

and \( c \neq 0 \).

Finally,

\[
\Delta(E_t) = 4a(t)^3 + 27b(t)^2 = \frac{4a^3 + 27b^2}{(c^3(u^3 + \frac{a}{c^2}u + \frac{b-es^2}{c^3})^2 + e^2)^5} = \frac{(4a^3 + 27b^2)s^{12}}{(c^3(u^3 + \frac{a}{c^2}u + \frac{b-es^2}{c^3})^2 + e^2)^6},
\]

so the only fiber on which all points are transformed to points on singular curves is \( s = 0 \). For other values of \( s \) this is a non-zero rational function in \( u \) of degree eighteen.

Next, take any \( t_0 \) such that \( E_{t_0}^* \) has positive rank that is not one of the exceptions to Proposition 4.1.10 (note particularly we should have \( ct^2 + e \neq 0 \), otherwise \( E_{t_0}^* \) is singular). Then we know that for all but finitely many points \((x, y) \in E_{t_0}^0(\mathbb{R}) \cap E_{t_0}(\mathbb{Q})\), \( E_s^* \) has positive rank where \( s = \sigma(x, y, t_0) \); particularly, as \( \sigma(x, y, t) = y(ct^2 + e) \), we have such \( s \)'s that are non-zero whenever we take a point \((x, y) \) such that \( y \neq 0 \) under the correspondence. For such \( s \), the \( y \) coordinates of \( E_{s_0}^* \) are dense in \( \mathbb{R} \). Thus the set

\[
\left\{ \tau(u, v, s) : (u, v) \in E_{s_0}^0(\mathbb{R}) \cap E_{s}^*(\mathbb{Q}) \right\} = \left\{ \frac{cv}{s} : (u, v) \in E_{s_0}^0(\mathbb{R}) \cap E_{s}^*(\mathbb{Q}) \right\}
\]

is also dense in \( \mathbb{R} \) (as \( c \neq 0, s \neq 0 \)). Hence property 3 of Definition 1.3.4 holds.

Note that this surface is also cross-fibered if we switch the fibrations; namely, if we view the * fibration as being the main fibration. Take any \( s_0 \) such that \( E_{s_0}^* \) has positive rank that is not one of the exceptions to Proposition 4.1.10, particularly \( s_0 \neq 0 \). Then,
we know that for all but finitely many points \((u, v) \in E_{s_0}^* (\mathbb{R}) \cap E_{s_0}^* (\mathbb{Q})\), \(E_t\) has positive rank where \(t = \tau(u, v, s_0)\). As there are at most two values of \(v\) and hence six points on \(E_{s_0}^*\) such that \(c t^2 + e = c(v_{s_0})^2 + e = 0\), we can find some \((u, v) \in E_{s_0}^* (\mathbb{R}) \cap E_{s_0}^* (\mathbb{Q})\) that transforms to a point on a fiber of positive rank such that \(c t^2 + e \neq 0\). For such \(t\), the y-coordinates of \(E_0^t\) are dense in \(\mathbb{R}\). Thus the set

\[
\{ \sigma(x, y, t) : (x, y) \in E_0^t (\mathbb{R}) \cap E_t (\mathbb{Q}) \} = \{ y(c t^2 + e) : (x, y) \in E_0^t (\mathbb{R}) \cap E_t (\mathbb{Q}) \}
\]

is also dense in \(\mathbb{R}\).

**Surfaces of the form (4.2)**

Let \(\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \theta\) be constants such that at least one of \(\alpha\) and \(\epsilon\) is non-zero. Then we have fibrations:

\[
E_t : y^2 = x^3 + C_1(t)x + C_2(t),
\]

where \(C_1(t) = \alpha t^3 + 3\beta t^2 + \gamma t + \delta\) and \(C_2(t) = \epsilon t^3 + 3\zeta t^2 + \eta t + \theta\), and

\[
E_s^* : v^2 = u^3 + A(s)u + B(s),
\]

where we rearrange the coefficients to form \(A(s) = (\alpha s + \epsilon)(\gamma s + \eta) - 3(\beta s + \zeta)^2\) and \(B(s) = (\alpha s + \epsilon)^2(s^3 + \delta s + \theta) - (\beta s + \zeta)[(\alpha s + \epsilon)(\gamma s + \eta) - 2(\beta s + \zeta)^2]\).

Then transition maps are given by:

\[
\Phi : (x, y) \in E_t \mapsto ((\alpha x + \epsilon)t + (\beta x + \zeta), (\alpha x + \epsilon)y) \in E_x^*
\]

and

\[
\Phi^* : (u, v) \in E_x^* \mapsto \left(s, v / (\alpha s + \epsilon)\right) \in E_{(u - \beta s - \zeta)/(\alpha s + \epsilon)}
\]

off the curve \(\alpha s + \epsilon = 0\).

The properties necessary to see that this surface is cross-fibered are shown in [24, Section 5].

**Surfaces of the form (4.3)**

Let \(b > 0, \alpha, \text{ and } \beta\) be constants. Then we have a correspondence between the fibrations:

\[
E_t : y^2 = x^3 + bC(t)^2,
\]
where \( C(t) = t^3 + \alpha t + \beta \) and

\[
E_s^* : v^2 = v^3 + A(s)u + B(s),
\]

where \( A(s) = \alpha s^2 \) and \( B(s) = \beta s^3 + b \). The transition maps are given by:

\[
(x, y) \in E_t \mapsto \left( \frac{xt}{C(t)}, \frac{y}{C(t)} \right) \in E^*_{t(3t+3)}
\]

and

\[
(u, v) \in E_s^* \mapsto \left( sC\left(\frac{u}{s}\right), vC\left(\frac{u}{s}\right) \right) \in E^*_{u(3s+3)}
\]

off the curves \( C(t) = 0 \) and \( s = 0 \).

The properties necessary to see that this surface is cross-fibered are shown in [24, Section 6].

**A non-example**

We now consider an example of a surface that has a pre-cross-fibration, but is not cross-fibered: the cubic isotrivial surfaces. Note that even though these surfaces are not cross-fibered, they were shown in [19, Theorem 3] to satisfy Conjecture 1.2.7 via an argument involving viewing a curve as sections in the different fibrations.

Let \( a, b, c, \) and \( e \) be such that

\[
y^2 = x^3 + ax + b \quad \text{and} \quad y^2 = x^3 + cx + e
\]

are both (non-singular) elliptic curves. There is a (pre-cross-fibered) correspondence between:

\[
E_t : y^2 = x^3 + \frac{a}{(t^3 + ct + e)^2}x + \frac{b}{(t^3 + ct + e)^3}
\]

and

\[
E_s^* : v^2 = u^3 + \frac{c}{(s^3 + as + b)^2}u + \frac{e}{(s^3 + as + b)^3},
\]

with transition maps given by

\[
\Phi : (x, y) \in E_t \mapsto \left( \frac{t}{(x(t^3 + ct + e))^3 + a(x(t^3 + ct + e)) + b}, \frac{1}{y(t^3 + ct + e)((y(t^3 + ct + e))^3 + a(x(t^3 + ct + e)) + b)} \right) \in E^*_{x(t^3 + ct + e)}
\]
and \( \Phi^* : (u, v) \in E^*_s \mapsto \)
\[
\left( \frac{s}{(u(s^3+as+b))^3 + c(u(s^3+as+b)) + e} + \frac{1}{v(s^3+as+b)((u(s^3+as+b))^3 + c(u(s^3+as+b)+e))} \right) \in E_{u(s^3+as+b)}
\]
off the curves \( t^3 + ct + e = 0, y = 0, s^3 + as + b = 0, \) and \( v = 0. \)

**Proposition 4.1.13.** Surfaces of the form \( (4.4) \) are not cross-fibered by the above correspondence.

**Proof.** We show for all \( t, \)
\[
\bigcup_{s:rk(E^*_s(Q))>0} \{ \tau(u, v, s) : (u, v) \in E^*_s(\mathbb{R}) \cap E^*_s(\mathbb{Q}) \} \neq \mathbb{R}.
\]
Suppose we have \( (x, y) \in E^0_0(\mathbb{R}) \cap E_t(\mathbb{Q}). \) Take \( s = \sigma(x, y, t) = x(t^3 + ct + e). \) Then, if \( u = r_0 \) is a real root of
\[
u^3 + \frac{c}{(s^3 + as + b)^2} u + \frac{e}{(s^3 + as + b)^3} = 0,
\]
\( U = r_0(s^3 + as + b) \) is a real root of
\[
U^3 + cU + e = 0.
\]
Hence,
\[
r_0 = \frac{\text{funct}(c, e)}{s^3 + as + b},
\]
where \( \text{funct}(c, e) \) is some function of \( c \) and \( e. \) Namely, if \( (u, v) \in E^*_s(\mathbb{R}), \) then
\[
u \in \left[ \frac{\text{funct}(c, e)}{s^3 + as + b}, \infty \right).
\]
So,
\[
\tau(u, v, s) = u(s^3 + as + b) \in [\text{funct}(c, e), \infty)
\]
or
\[
\tau(u, v, s) = u(s^3 + as + b) \in (-\infty, \text{funct}(c, e)]
\]
depending on the sign of \( s^3 + as + b. \) However,
\[
s^3 + as + b = (x(t^3 + ct + e))^3 + ax(t^3 + ct + e) + b
\]
Thus, the sign of \( s^3 + as + b \) only depends on the fiber \( E_t \).

\[ (t^3 + ct + e)^3 \left( x^3 + \frac{a}{(t^3 + ct + e)^2}x + \frac{b}{(t^3 + ct + e)^3} \right) = (t^3 + ct + e)^3y^2. \]

Improving on the bounds of Propositions 4.1.9 and 4.1.10 in special cases

For specific surfaces, one can often do better than the bounds of Propositions 4.1.9 and 4.1.10. For example:

**Proposition 4.1.14** (Munshi’s results in \([24]\), as he indicates they can be refined in \([25]\) with attention to specific bounds). For all fibers \( E_t \) of surfaces of the form (4.2), only finitely many points on \( E_t \) are taken to torsion points under the map \( \Phi \). (That is to say there are no exceptions to property 1 of Definition 1.3.4, and then for each fiber \( E_t \), the number of points that go to torsion is still bounded by the same bound as in Proposition 4.1.10.)

For surfaces of the form (4.1) we can also improve our bounds using these ideas.

**Proposition 4.1.15** (Theorem 3 of \([30]\) re-proved in a manner more analogous to the methods of \([24]\) with attention to specific bounds). For all fibers \( E_t \) of surfaces of the form (4.1) except where \( t = 0 \), only finitely many points on \( E_t \) are taken to torsion points under the map \( \Phi \). (That is to say there is only one exception to property 1 of Definition 1.3.4: all points on \( E_{t=0} \) are taken to 2-torsion under \( \Phi \).) For each \( t \neq 0 \), the number of points on \( E_t \) that go to torsion under the transformation is bounded by the same bound as in Proposition 4.1.10.

Similarly, for all \( s \neq 0 \), \( E^*_s \) has at most 1480 points which go to torsion under \( \Phi^* \) and at most 6 points at which \( \Phi^* \) is not defined (the transformation \( \Phi^* \) is not defined on the curve \( s = 0 \)).

**Proof.** Again, if for some \( t_0 \) there are infinitely many points on \( E_{t_0} \) which go to torsion points under \( \Phi \), it is because \( \psi^m_2(x, y; t_0) \) is the zero function for some \( m \). However, in that case all \( (x, y) \in E_{t_0} \) go to \( m \)-torsion points and we have a morphism

\[ \mathbb{P}^2 \to X_1(1), \quad (x, y) \mapsto (E^*_s, \Phi((x, y))). \]

Thus, the map \( (x, y) \mapsto j \left( E^*_{y(ct^2 + e)} \right) \) factors as \( \mathbb{P}^2 \to X_1(m) \to X_1(1) \). But for this
surface, we can compute
\[ j(E^*_s) = \frac{(-24 \alpha^3)}{-8(\alpha^3)3 - 27(b - e(y(ct^2_0 + e))^2)^2}, \]
which is a rational function of degree exactly four in \( y \) as \( c, e \neq 0 \) (note \( ct^2_0 + e \neq 0 \) because \( E_{t_0} \) is a non-singular fiber). Then, again, as the degree of the second map of this composition is
\[ m^2 \prod_{p|m} \left(1 - \frac{1}{p^2}\right) \]
for \( 3 \leq m \leq 16 \), we can only have such a torsion section for \( m = 2 \) or \( m = 3 \).

For \( m = 2 \) we compute
\[ \psi^*_2(x, y, t_0) = 2v = 2 \left( \frac{yt_0(c t^2_0 + e)}{c} \right)^2, \]
which is zero if \( t_0 = 0 \). Otherwise, this is non-zero as a polynomial in \( y \) and hence in \( x \) as \( c t^2_0 + e = 0 \) only for singular fibers.

For \( m = 3 \),
\[ \psi^*_3(x, y, t_0) = 3u^4 + 6c(s)u^2 + 12d(s)u - c(s)^2 \]
\[ = \left(3 \left( \frac{x}{ct^2_0 + e} \right)^4 + 6 \frac{a}{c^2} \left( \frac{x}{ct^2_0 + e} \right)^2 + 12 \frac{b - e(x^3 + \frac{a}{(ct^2_0 + e)^2} + \frac{b}{ct^2_0 + e})}{c} \left( \frac{x}{ct^2_0 + e} \right)^2 \left( \frac{x}{ct^2_0 + e} \right)^2 \right). \]
For \( a \neq 0 \), this has constant term \(-\left( \frac{a}{ct^2_0 + e} \right)^2 \neq 0 \) and hence is not the zero polynomial for any \( t_0 \).

If \( a = 0 \), then for fixed \( t_0 \), \( \psi^*_3(x, y, t_0) \) is a polynomial of degree at most four in \( x \) with leading term
\[ x^4 \left( 3 \left( \frac{(ct^2_0 + e)}{c} \right)^4 - \frac{12e(ct^2_0 + e)^3}{c^4} \right) = x^4 \left( \frac{(ct^2_0 + e)}{c} \right)^3 \left( 3 \left( ct^2_0 + e \right) - 12e \right). \]
For non-singular fibers, this is only zero if \( t_0 = \pm \sqrt{\frac{3e}{c}} \). However, in this case the polynomial reduces to
\[ \psi^*_3(x, y, t_0) = 12 \left( \frac{b - e \left( \frac{b}{(4e)^3} \right) (4e)^2}{c^3} \right) \left( \frac{x(4e)}{c} \right) = 36 \frac{eb}{c^4} x, \]
which is only zero as a polynomial if \( b = 0 \), but as \( a = 0 \) already, \( b \neq 0 \), otherwise (4.1).
would not define an elliptic surface.

So for \( t_0 = 0 \) all points on \( E_{t_0} \) are sent to 2-torsion. For all other \( t_0 \), \( \psi^2(x, y, t_0) \neq 0 \), so the number of points on \( E_{t_0} \) that go to torsion under \( \Phi \) is bounded by the same bound as in Proposition 4.1.10.

Finally,

\[
\Delta(E^*_s) = 4c(s)^3 + 27d(s)^2 = 4 \left( \frac{a}{c^2} \right)^3 + 27 \left( \frac{b - e(y(ct^2 + e))}{c^3} \right)^2
\]

has constant term

\[
\frac{4a^3 + 27b^2}{c^6} \neq 0,
\]

and hence is not the zero function in \( x \) and \( y \) for any choice of \( t \). Thus, for any \( t \) there are at most four values of \( y \) and hence twelve points on \( E_t \) that are transformed to points on singular fibers.

Similarly, the image of a point \((u, v) \in E^*_{s_0}\) under \( \Phi^* \) is \( m \)-torsion if and only if the division polynomial \( \psi^{**2}(u, v, s_0) = 0 \). So the \( x \)-coordinate and coefficient polynomials \( A = a(t) \) and \( B = b(t) \) resulting from this conversion are given by:

\[
x = \frac{cus_0^2}{c^3u^2 + es_0^2} = \frac{cus_0^2}{c^3 \left( u^3 + \frac{a}{c^2}u + \frac{b - es_0^2}{c^3} \right) + es_0^2},
\]

\[
A = \frac{a}{(ct^2 + e)^2} = \frac{a}{\left( c \left( \frac{ct}{s_0} \right)^2 + e \right)^2} = \frac{as_0^4}{c^3 \left( u^3 + \frac{a}{c^2}u + \frac{b - es_0^2}{c^3} \right) + es_0^2},
\]

and

\[
B = \frac{b}{(ct^2 + e)^3} = \frac{bs_0^6}{c^3 \left( u^3 + \frac{a}{c^2}u + \frac{b - es_0^2}{c^3} \right) + es_0^2}.
\]

So, \( \psi^{**2}(u, v, s_0) \) is of the form:

polynomial in \( u \) with leading term \( m^2(cus_0^2)^{m^2-1} \)

\[
\left( c^3 \left( u^3 + \frac{a}{c^2}u + \frac{b - es_0^2}{c^3} \right) + es_0^2 \right)^{m^2-1}
\]

and is hence non-zero as a function in two variables as \( c \neq 0 \). In fact, as the weighting
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

of $x$, $A$, and $B$ is twice the degree of these polynomials in $s$, we can factor

$$s_0^{2m^2-2} \cdot \text{polynomial only in } u \text{ with degree at most } m^2 - 1,$$

$$c^3 \left( u^3 + \frac{a}{c^2} u + \frac{b-es_0^2}{c^3} \right)^2 + es_0^2.$$ 

Note that the transformation $\Phi^*$ is not defined on the curve $s_0 = 0$. Similarly, the
denominator of $\psi_m^{**}(u, v, s_0)$ is only zero when $c^3 v^2 + es_0^2 = 0$, on which $\Phi^*$, again, is not
defined. Thus, for $s_0 \neq 0$, there are at most two values of $v$ and hence at most six points
on which $\Phi^*$ is not defined. For all $s_0 \neq 0$, $\psi_m^{**}(u, v, s_0) \neq 0$, so the number of points on
$E^*_s$ that go to $m$-torsion under $\Phi^*$ is at most $m^2 - 1$. Then, the total number of points
that go to torsion per fiber is at most $\sum_{m} m^2 - 1 = 1480$. Additionally, as we saw above,
there are at most 36 points that go to singular fibers. So, on any fiber other than $s = 0$
all but at most 1516 points are transformed to non-torsion points.

4.1.3 Comments on elliptic surfaces with multiple fibrations

In this section, we will discuss the some of the geometric implications of a surface being
cross-fibered. We note the following result:

Proposition 4.1.16 (Lemma 12.18 of [32] and its proof). Assume that an elliptic surface
$E$ admits two distinct elliptic fibrations with section. Then $E$ has trivial canonical bundle,
and the fibrations are either of product type or $E$ is a $K3$ surface.

By “distinct fibrations,” one means here fibrations such that the fibers of one fibration
are not all algebraically equivalent to the fibers of the other fibrations (whereas the fibers
of a single fibration are all algebraically equivalent to each other, see [32, Section 6.4]).
By the criterion of Section 3.2 surfaces of the form (4.1) are rational and hence have
non-trivial canonical bundle. We will look at these surfaces in more detail and see how
the fibrations we exhibited on them can exist.

We projectivize the fibers in each fibration of surface (4.1). So, off the fiber $t = \infty$,
our surface corresponds to:

$$\left\{ ([x : y : z], t) \in \mathbb{P}^2 \times \mathbb{P}^1 : t \neq \infty, z y^2 = x^3 + \frac{a}{(ct^2 + e)^2} x z^2 + \frac{b}{(ct^2 + e)^3} z^3 \right\}.$$ 

We have a projection map given by

$$\pi : E \to \mathbb{P}^1 : ([x : y : z], t) \mapsto t.$$
and zero section given by

\[ \iota : \mathbb{P}^1 \to \mathcal{E} : t \mapsto ([0 : 1 : 0], t). \]

Similarly, off the fiber \( s = \infty \), in the \( * \) fibration our surface corresponds to:

\[
\left\{ ([u : v : w], s) \in \mathbb{P}^2 \times \mathbb{P}^1 : s \neq \infty, wv^2 = u^3 + \frac{a}{c^2}uw^2 + \frac{b - es^2}{c^3}w^3 \right\}.
\]

We have a projection map given by

\[ \pi^* : \mathcal{E}^* \to \mathbb{P}^1 : ([u : v : w], s) \mapsto s \]

and zero section given by

\[ \iota^* : \mathbb{P}^1 \to \mathcal{E}^* : s \mapsto ([0 : 1 : 0], s). \]

Now the transition maps are given by

\[
\Phi : [x : y : z] \in E_t \mapsto \left[ \frac{x(ct^2 + e)}{c} : \frac{yt(ct^2 + e)}{c} : z \right] \in E_s^{\frac{ct^2 + e}{z}}
\]

and

\[
\Phi^* : [u : v : w] \in E_s^* \mapsto \left[ \frac{cus^2}{c^3v^2 + es^2w^2} : \frac{s^3w}{c^3v^2 + es^2w^2} : \frac{1}{w} \right] \in E_s^{\frac{cv}{sw}}.
\]

Note that the zero section in the \( E_t \) fibration is sent to

\[ \left[ 0 : \frac{t(ct^2 + e)}{c} : 0 \right] \in E_s^* \]

Namely, the entire zero section is sent to a single point. Hence, if we view the images of the fibers of \( E_t \) under \( \Phi \):

\[ \Phi(E_t) = \left\{ ([u : v : w], s) \in \mathbb{P}^2 \times \mathbb{P}^1 : wv^2 = u^3 + \frac{a}{c^2}uw^2 + \frac{b - es^2}{c^3}w^3, \frac{cv}{sw} = t \right\} \]

as corresponding to a projection:

\[ \mathcal{E} \to \mathbb{P}^1 : ([u : v : w], s) \mapsto \frac{cv}{sw} \]

the image of the zero section we had in \( E_t \) under \( \Phi \) does not provide us with an acceptable zero section.
As $\Phi$ is only assumed to be birational, it is allowed to behave badly on a finite number of closed curves of $E$ and still satisfy Definition 1.3.4. In this case, it happens to behave badly on the closed curve that is given by the zero section of $E_t$. So even if one has two surfaces that are birationally equivalent, each with an elliptic fibration, one does not necessarily have two elliptic fibrations with section when viewed natively in either of the two surfaces.

4.2 The probability that $t_{n,m} \in I$

Recall Diffusion Process 4.1.4 from Section 4.1. Given a starting point on a starting fiber and an interval $I \subset \mathbb{R}$, we might ask if we can find $n$ and $m$ such that, when performing this process, the output fiber $t_{n,m} \in I$. We have:

**Proposition 4.2.1.** Let $\{E_t\}$ be the main fibration of a cross-fibered surface. Let $P_0$ be a non-torsion point on a non-exceptional fiber $E_{t_0}$, and let $I$ be an interval in $\mathbb{R}$. Then, if one uses $P_0$ and $E_{t_0}$ as the starting point and fiber respectively for Diffusion Process 4.1.4 there exist $n$ and $m$ such that $t_{n,m} \in I$ where $E_{t_{n,m}}$ is the output fiber produced by the process.

**Proof.** Note that in the proof of Theorem 4.1.6 we, essentially, perform Diffusion Process 4.1.4. Then, as we assume $P_0$ is a non-torsion point and $E_{t_0}$ is a non-exceptional fiber, we can perform exactly the same argument to choose $n$ and $m$. The output fiber produced in the proof of Theorem 4.1.6, $E_{t_{n,m}}$, had positive rank and $t_{n,m} \in I$.

A priori, the $n$ and $m$ that we have produced may be very large, leading to a $t_{n,m}$ that has a large height as a rational number. This is a reflection of the fact that, even though they are dense in the topological sense, fibers produced by Diffusion Process 4.1.4 may be very sparse in the measure theoretic sense. Thus, it is interesting to examine the size of $n$ and $m$ required to have $t_{n,m} \in I$, and, in so doing, understand the “rate of diffusion” of positive rank fibers that is given to us by the cross-fibration structure. Moreover, the percentage of $n$ and $m$ such that $t_{n,m} \in I$ can be thought of as a time average of the map $\Phi_{n,m}$, which as this map is built out of irrational rotations and hence ergodic transformations, retains nice properties relating its time and space averages. In this section we will develop the tools necessary to explore such ideas.

We recall:
**Definition 4.2.2.** A measure preserving transformation $T : X \rightarrow X$ on a measure space $(X, \Sigma, \mu)$ is said to be ergodic if for every measurable set $E \in \Sigma$ such that $T^{-1}E = E$ we have $\mu(E) = 0$ or $\mu(E) = 1$.

Then, a fundamental result of ergodic theory gives us:

**Theorem 4.2.3** (Birkhoff Ergodic Theorem, see Theorem 1.14 in [46]). Suppose a measure preserving transformation $T : X \rightarrow X$ on a probability space $(X, \Sigma, \mu)$ is ergodic and $f \in L^1(m)$. Then

$$
\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} f(T^i x) = \int f dm \text{ for almost all } x.
$$

The irrational circle rotation $T_\theta : [0, 1] \rightarrow [0, 1]$ given by $T_\theta(x) = x + \theta$ is ergodic if $\theta$ is irrational (see [28, Section 2.4]). Taking $f$ to be the characteristic function of an interval $I \subseteq [0, 1]$, we have

$$
\lim_{N \rightarrow \infty} \frac{\# \{ k \leq N : k\theta \in I \mod 1 \}}{N} = \operatorname{length}(I) \quad (4.5)
$$

for $\theta$ irrational and $x \in [0, 1]$. That this holds for all $x$ rather than just almost every $x$ as one would have a priori by Theorem 4.2.3 comes from the translation properties of irrational rotations (again, see [28, Section 2.4]). This result can be seen as a strengthening of Theorem 1.2.5.

We note:

**Proposition 4.2.4.** Let $P \in E_t$ be a point in an elliptic surface with a pre-cross-fibration at which the conversion map $*$ is defined. Then, $\hat{h}(P^*) \leq \operatorname{poly}(\hat{h}(P), \hat{h}(t))$ (where the polynomial depends only on the objects that define the pre-cross-fibration, namely, $\cal{E}$, $\cal{E}^*$, $\Phi$, and $\Phi^*$).

*Proof.* The conversion maps are polynomial maps in the coordinates of $P$ and in $t$. \hfill \Box

In the rest of this section, we will make frequent use of the fact that the identity component of the real locus of an elliptic curve is homeomorphic to a circle (see, for example, [36, Ch. 5, Corollary 2.3.1]). In particular, let $E_t$ be a non-exceptional fiber of a cross-fibered surface $\cal{E}$. Then, we have a homeomorphism

$$
\psi_t : E_t^0(\mathbb{R}) \rightarrow S^1.
$$
However, as $E_t$ is non-exceptional, for all but finitely many points $P \in E_t$, we can convert $P$ to $P^* \in E_{\sigma(P)}^*$, where $E_{\sigma(P)}^*$ is a fiber of $E^*$. Then, we also have a homeomorphism

$$
\psi_{\sigma(P)}^* : E_{\sigma(P)}^0(\mathbb{R}) \to S^1.
$$

The map $\psi_{\sigma(P)}^*$ will, of course, vary as $P$ varies. However, in a certain sense this shows us that the real points of the “identity component part” of a cross-fibered surface looks like a torus. Recall the remarks preceding Theorem 4.1.6 for why we focus on the identity components. This will be a useful perspective when considering the dynamics of Diffusion Process 4.1.4 because this process is composed of multiplications of points on elliptic curves, and the dynamics of multiplication on elliptic curves is related to that of the irrational circle rotations by the above homeomorphisms.

Now, for a given target interval $I \subset \mathbb{R}$, we think of a region $I$ in $E$ as consisting of the points that are projected to $I$ via $\pi$. Namely, for $n, m \in \mathbb{N}$, $t_{n,m} \in I$ is equivalent to $(m(nP)^*)^* \in I$. Under the above homeomorphisms, we can think of $I$ as corresponding to a region $I_t$ in the torus $S^1 \times S^1$. Explicitly, for any $t$ such that $E_t$ is a non-exceptional fiber, we define

$$
I_t = \left\{ (\alpha, \beta) \in S^1 \times S^1 : \begin{array}{l}
\psi_t(\alpha) = P \in E_t^0(\mathbb{R}) \\
\psi_{\sigma(P)}^*(\beta) = P^* \in E_{\sigma(P)}^0(\mathbb{R}) \\
\tau(P^*) \in I
\end{array} \right\}.
$$

We will see via Proposition 4.2.8 that the area of $I_t$ (where the entire torus is normalized to have area one) is the right notion of the size of $I$ “as seen by a cross-fibration.”

We will define

$$
m_{E_t}(I) = vol(I_t).
$$

We proceed by building up the tools that will show us that the region $I_t$ is, in fact, measurable and that $m_{E_t}$ induces a measure on $\mathbb{R}$.

Remark that while $\mathcal{I}$ does not make a reference to a base fiber $E_t$, $I_t$ does. This is natural as, a priori, we can start with a fiber which is biased in such a way such that points on that fiber are more or less likely to go to $I$ under Diffusion Process 4.1.4.

We note that $I_t$ naturally decomposes into cross-sections: $I_t = \bigcup_{\alpha \in S^1} I_{t,\alpha}^*$, where

$$
I_{t,\alpha}^* = \{ \beta \in S^1 : (\alpha, \beta) \in I_t \} = \left\{ \begin{array}{l}
\psi_t(\alpha) = P \in E_t^0(\mathbb{R}) \\
\psi_{\sigma(P)}^*(\beta) = P^* \in E_{\sigma(P)}^0(\mathbb{R}) \\
\tau(P^*) \in I
\end{array} \right\}.
$$
The union over the $\alpha \in S^1$ corresponds, under $\psi_t$, to taking the union over the points $P \in E_t^0(\mathbb{R})$. Then for each such $P$, we can consider the cross-fiber that “goes through $P$”; namely, the cross-fiber $E^*_\sigma(P)$. Then, the $\beta \in I^*_{t,\alpha}$ correspond, under $\psi^*_\sigma(P)$, exactly to the points $P^* \in E^0_{\sigma(P)}(\mathbb{R})$ that are in $\mathcal{I}$. The region $I^*_{t,\alpha}$ will, of course, vary with $\alpha$. In fact, there may be some values of $\alpha$ for which no point (in the identity component) of the corresponding cross-fiber $E^0_{\sigma(P)}(\mathbb{R})$ projects to $I$, and hence $I^*_{t,\alpha} = \emptyset$ (see Figure 4.2).

Figure 4.2: For each $\alpha$ in the base circle corresponding to $E^0_t$, we have shaded the region $I^*_\alpha$ of $S^1$, namely, the points that go to $I$. Note $I^*_{t,\alpha}$ can be empty, as is the case for $\alpha_3$. The union of the shaded regions, as $\alpha$ varies, is $\mathbb{I}_t$.

We see:

Lemma 4.2.5. Let $\mathcal{E}$ be a cross-fibered elliptic surface of which $E_{t_0}$ is a non-exceptional fiber. Let $I$ be an open interval of $\mathbb{R}$ ($I = (a, b)$ for $a, b \in \mathbb{R} \cup \{\infty\}$). Then the function

$$f(\alpha) = m(I^*_{t_0,\alpha})$$

is continuous from $S^1 \to \mathbb{R}$ (except possibly at a finite number of points of $S^1$) where $m$ is the Haar measure on $S^1$.

Proof. We write $g : E_{t_0} \to [0, 1]$ given by:

$$g(x, y) = m \left( \psi^*_\sigma(x, y, t_0) \left( \{ (u, v) \in E^0_{\sigma(x, y, t_0)}(\mathbb{R}) : \tau(u, v, \sigma(x, y, t_0)) \in I \} \right) \right).$$

Then, $f(\alpha) = g(\psi_{t_0}^{-1}(\alpha))$. As $\psi_{t_0}$ is a homeomorphism, it suffices to consider the continuity of $g$. Then, if we consider the function $h : \mathbb{R} \to [0, 1]$ given by:

$$h(s) = m \left( \psi^*_s \left( \{ (u, v) \in E^0_s(\mathbb{R}) : \tau(u, v, s) \in I \} \right) \right),$$
we note that \( g(x, y) = h(\sigma(x, y, t_0)) \). As \( \sigma(x, y, t_0) \) is rational, it is continuous except possibly at points where its denominator is zero. Then, as \( E_{t_0} \) is assumed to be non-exceptional, there are only finitely many pairs \((x, y) \in E_{t_0} \) where \( \sigma(x, y, t_0) \) is discontinuous.

Consider the set

\[
D_a := \{ (x, y) \in E_{t_0}(\mathbb{R}) : \tau(u, v, \sigma(x, y, t_0)) = a \ \forall (u, v) \in E^s_{\sigma(x,y,t_0)}(\mathbb{R}) \}.
\]

We argue that \( D_a \) is finite. For a given \( s_0 \), \( \tau(u, v, s_0) = a \) defines a (possibly singular) curve \( C_{s_0} \) in \( \mathbb{R}^2 \). As \( E^s_{s_0} \) is an irreducible curve, by Bézout’s Theorem either there are a finite number of points \((u, v) \in E^s_{s_0}(\mathbb{R}) \) such that \( \tau(u, v, s_0) = a \), or \( \tau(u, v, s_0) = a \) for all points in \( E^s_{s_0}(\mathbb{R}) \). However, \( E^s_{s_0}(\mathbb{R}) \) being a component of \( C_{s_0} \) is equivalent to polynomial conditions on the coefficients as (functions in \( s_0 \)) that define \( C_{s_0} \). Then, these conditions either only hold for a finite number of \( s_0 \) or they hold for all \( s_0 \). In the latter case, \( \tau(u, v, s) = a \) identically as a function on \( \mathbb{R}^3 \), and so \( D_a \) is all of \( E_{t_0}(\mathbb{R}) \). If there are only finitely many \( s_0 \) at which \( E^s_{s_0}(\mathbb{R}) \) is a component of \( C_{s_0} \), then for each of these \( s_0 \), \( \sigma(x, y, t_0) = s_0 \) defines a (possibly singular) curve in \( \mathbb{R}^2 \). Then as \( E_{t_0} \) is an irreducible curve by the same argument as above, either \( \sigma(x, y, t_0) = s_0 \) for all \((x, y) \in E_{t_0} \) or for only finitely many such \((x, y) \). In the former case \( D_a \) is all of \( E_{t_0}(\mathbb{R}) \), and in the latter case \( D_a \) is finite.

However, if \( D_a \) is all of \( E_{t_0}(\mathbb{R}) \), then \( E_{t_0} \) would fail property 3 of Definition 1.3.4 and hence would be an exceptional fiber which we have excluded. Thus, \( D_a \) is finite. We can similarly define \( D_b \) for the other endpoint of \( I \), which we see to be finite by the same argument.

So, it will be sufficient to see that \( h \) is continuous at all \( s \) of the form \( s = \sigma(x, y, t_0) \) except for the finitely many points \((x, y) \in E_{t_0} \) that are sent to torsion points or points on singular curves under \( * \) and the finitely many \((x, y) \) in \( D_a \) or \( D_b \).

For each \( s \), \( U_s = \{ (u, v) \in \mathbb{R}^2 : \tau(u, v, s) \in I \} \) is an open set of \( \mathbb{R}^2 \). The function \( h \) is measuring how much of \( E^s_{s_0} \) passes through the set \( U_s \). Then, as \( s \) changes, both \( E^*_s \) and \( U_s \) change. We control these effects separately by bounding

\[
| m \left( \psi^*_s (E^s_{s_0}(\mathbb{R}) \cap U_s) \right) - m \left( \psi^*_s (E^s_{s_0}(\mathbb{R}) \cap U_{s_0}) \right) |
\]

and

\[
| m \left( \psi^*_s (E^s_{s_0}(\mathbb{R}) \cap U_{s_0}) \right) - m \left( \psi^*_{s_0} (E^s_{s_0}(\mathbb{R}) \cap U_{s_0}) \right) |
\]

Then, we use the triangle inequality to bound \(| h(s) - h(s_0) | \).
First we control the term in which we have a changing curve $E^*_{s_0}$ passing through a fixed open set $U_{s_0}$. Given a point $(u_0, v_0) \in E^*_{s_0}$, we define $\phi_{u_0,v_0} : \mathbb{R} \to \mathbb{R}^2$ by:

$$\phi_{u_0,v_0}(s) = \psi_{s_0}^{s-1}(\psi_{s_0}(u_0, v_0)).$$

We claim that $\phi_{u_0,v_0}$ is continuous (again, at all $s$ of the form $s = \sigma(x,y,t_0)$ except for the finitely many exceptional points $(x,y) \in E_{t_0}$). To see this, we have to study in detail how $\psi^*_s$ is defined.

Following Sections 1 and 2 of Chapter 5 of [36], we can find an isomorphism:

$$E^*_s \cong E_q,$$

where $0 < |q| < 1$ parameterizes a family

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

that contains exactly one representative from each isomorphism class of elliptic curves over $\mathbb{R}$. Here $a_4(q)$ and $a_6$ are given by power series in $q$ (see [36, Ch. 5, Theorem 1.1]). For this family, the $j$-invariant is given by:

$$j(q) = \frac{1}{q} + \sum_{n \geq 0} c(n)q^n,$$

where $c(n) \in \mathbb{Z}$. This formula for $j$ in terms of $q$ from $(-1,0) \cup (0,1)$ to $\mathbb{R}$ is continuous and 2 to 1, and if we restrict to one of the two branches, it has a continuous inverse. We have $\text{sign} (\Delta(E_q)) = \text{sign}(q)$, so which branch we should choose is determined by the sign of $\Delta(E^*_s)$.

On the other hand, the $j$-invariant of $E^*_s$ is given by a rational function in its coefficients $c(s)$ and $d(s)$ and hence in $s$. As $s = \sigma(x,y,t_0)$ for some non-exceptional point $(x,y) \in E_{t_0}$, $E^*_s$ must be non-singular, so the denominator of the rational function defining its $j$-invariant cannot be zero. Thus $j(E^*_s)$ and hence $q$ are continuous functions at these $s$.

Then (again as in [36, Ch. 5]), we can find a sequence of isomorphisms such that either:

$$E_q \cong \mathbb{R}^*/q \cong \mathbb{R}/\mathbb{Z} \times \{\pm 1\}$$
or

\[ E_q \cong \mathbb{R}^*/q^\mathbb{Z} \cong \mathbb{R}/\mathbb{Z} \]

depending on whether \( \Delta(E_q) > 0 \) or \( \Delta(E_q) < 0 \) respectively. In either case, the identity component of \( E_q \) and hence \( E_s^* \) is homeomorphic to \( S^1 \).

The isomorphism \( \mathbb{R}^*/q^\mathbb{Z} \to \mathbb{R}/\mathbb{Z} \) is given by

\[
z \mapsto \frac{1}{2} \left( \frac{\log |z|}{\log |q|} - \text{sign}(z) + 1 \right) \mod \mathbb{Z}
\]

if \( \Delta(E_q) < 0 \), and the isomorphism \( \mathbb{R}^*/q^\mathbb{Z} \to \mathbb{R}/\mathbb{Z} \times \{ \pm 1 \} \) is given by

\[
z \mapsto \left( \frac{\log |z|}{\log |q|} \mod \mathbb{Z}, \text{sign}(z) \right)
\]

if \( \Delta(E_q) > 0 \). Again, by our choice of \( s \), \( \Delta(E_q) \neq 0 \iff q \neq 0 \), so around \( s \) we will only be in one of these two situations. If \( \Delta(E_q) < 0 \), when taking the map

\[ S^1 \cong \mathbb{R}/\mathbb{Z} \to \mathbb{R}^*/q^\mathbb{Z} \]

we choose \( \text{sign}(z) = 1, -1 \) if \( \gamma \in \mathbb{R}/\mathbb{Z} \) is in \((0, 1/2)\) or \((1/2, 1) \mod \mathbb{Z} \) respectively. If \( \Delta(E_q) > 0 \), when taking the map

\[ S^1 \to \mathbb{R}/\mathbb{Z} \times \{ \pm 1 \} \to \mathbb{R}^*/q^\mathbb{Z} \]

given by restricting our isomorphism to the \( S^1 \) corresponding to the identity component of \( E_q \), we choose \( \text{sign}(z) = +1 \). In either case, \( z \) considered as a function of \( s \) will be continuous at our values of \( s \) because \( q \) is, and because \( q \neq 0 \).

Then, the isomorphism \( \mathbb{R}^*/q^\mathbb{Z} \to E_q(\mathbb{R}) \) is given by a restriction of a holomorphic function in \( z \) and \( q \) (see [36, Ch. 5, Theorem 1.1]). Hence, \( \gamma \in S^1 \) is mapped to \( (X(z,q), Y(z,q)) \in E^0_q \), where \( X(z,q) \) and \( Y(z,q) \) will be continuous functions of \( s \) at all \( s \) of the form \( s = \sigma(x,y,t_0) \) for non-exceptional points \( (x,y) \in E_{t_0} \).

Finally, we complete the map \( \psi_{s^{-1}}^* \) by performing the substitution

\[
(u, v) \in E^{*0}_s = \left( w^2 \left( X(z,q) + \frac{1}{12} \right), w^4 \left( Y(z,q) + \frac{X(z,q)}{2} \right) \right),
\]

where

\[
w = \left( \frac{c(s)}{a_4(q) - \frac{1}{48}} \right)^{1/4} = \left( \frac{d(s)}{a_6(q) - \frac{1}{1728}} \right)^{1/6}
\]
unlike $j(E^*_s) = 0$ or 1728 in which case $w$ is \( \left( \frac{d(s)}{a_0(q)-1} \right)^{1/6} \) or \( \left( \frac{c(s)}{a_4(q)-1} \right)^{1/4} \) respectively (see [39, Ch. 3, Proposition 1.4]). As our two expressions for $w$ are continuous in $s$ and equal except at the points where one of them is undefined, their discontinuities must be removable. Hence, $u$ and $v$ vary continuously in $s$ at all of our relevant $s$. Thus, we conclude that $\phi_{u_0,v_0}(s)$ does, in fact, have the claimed continuity.

Now let $\epsilon > 0$. As $U_{s_0}$ is an open set in $\mathbb{R}^2$, we can write it as the (possibly infinite) union of a collection of open rectangles $V_i$ (i.e. each $V_i$ is the product of an interval of values of $u$ with an interval of values of $v$). When we intersect a $V_i$ with $E^*_0$, we get a connected subset of $E^*_0$ unless the curve exits $V_i$ and re-enters. In this case one of the two coordinate functions (namely $y$ viewed locally as a function of $x$ or $x$ viewed locally as a function of $y$) must be non-monotonic on the intervals that define $V_i$. Thus, this coordinate function must take a local extremum on this interval that is outside $V_i$ (see Figure 4.3). On the identity component of an elliptic curve there is one local extremum of $x$ viewed as a function of $y$ and at most four local extrema of $y$ viewed as a function of $x$. Denote these points by $P_j$. By computing the first derivatives of these functions and checking for critical points, we can only have a point $P_j$ at a value of $x$ such that $3x^2 + c(s) = 0$ or $x^3 + c(s)x + d(s) = 0$. We view these potential local extrema as changing as we vary $s$; so we see that $x$-coordinate and hence the $y$-coordinate of each $P_j$ are locally continuous in $s$.

Denote the connected subsets of $E^*_0 \cap U_{s_0}$ by $\tilde{V}_k$. As $\psi^*_s$ is a homeomorphism, the image of $\tilde{V}_k$ is an interval in $S^1$. The image of $E^*_0 \cap U_{s_0}$ may consist of infinitely many intervals in $S^1$, but we can choose finitely many $\psi^*_s(\tilde{V}_1), \ldots, \psi^*_s(\tilde{V}_N)$ such that

$$m \left( \psi^*_s \left( E^*_0 \cap U_{s_0} \right) \setminus \bigcup_{k=1,\ldots,N} \tilde{V}_k \right) < \frac{\epsilon}{4}.$$ 

Note, for each $V_i$, $E^*_0 \cap V_i$ has only finitely many connected components as there are only finitely many $P_j$'s. So there are only finitely many $V_i$'s that contribute to the finitely many $\tilde{V}_k$'s. For each of the finitely many $\tilde{V}_k$'s, take $V_{ik}$ to be its corresponding $V_i$.

Then, for each of $\psi^*_s(\tilde{V}_1), \ldots, \psi^*_s(\tilde{V}_N)$, choose a closed subset $\bar{W}_k \subset \tilde{V}_k$ such that

$$m \left( \tilde{V}_k \setminus \bar{W}_k \right) \leq \frac{\epsilon}{4N},$$ 

and choose two points $\gamma_{k1}$ and $\gamma_{k2}$ in $\psi^*_s(\tilde{V}_k) \subset S^1$ such that

$$\left( \gamma_{k1}, \gamma_{k2} \right) \cap \psi^*_s(\tilde{V}_k \setminus \bar{W}_k).$$
Figure 4.3: A situation where $E^s_{s_0} \cap V_i$ is not connected

is disconnected.

So, for each of the finitely many $\psi_{s_0}^s(\gamma_{kl}) \in \mathbb{R}^2$, we use the continuity of $\phi_{\psi_{s_0}^s(\gamma_{kl})}$ to choose $\delta_{kl}$ such that if $|s - s_0| < \delta_{kl}$ we have

$$\psi_{s}^s(\gamma_{kl}) \in V_{ik}.$$ 

Also choose $\delta_j$’s such that if $|s - s_0| < \delta$, neither the $x$-coordinate, nor the $y$-coordinate of any of the finitely many $P_j$ enter or exit either of the intervals defining one of the finitely many $V_i$’s. Let $\delta$ be the minimum of the $\delta_{kl}$’s and the $\delta_j$’s. Then, for $|s - s_0| < \delta$, the configuration of the $N$ many “large intervals” in $S^1$ corresponding to $E^s_{s_0} \cap U_{s_0}$ stays unchanged, with only the endpoints of these intervals being allowed to change. Finally, note that on the other intervals outside of the finitely many on which the measure was clustered only a measure of $\frac{\epsilon}{4}$ can be lost between $s_0$ and $s$. On the other hand, the same argument could be applied in reverse, so only a measure of at most $\frac{\epsilon}{4}$ can be gained from such “small intervals”. As a result

$$|m \left(\psi_s^s \left(E_s^{s_0}(\mathbb{R}) \cap U_{s_0}\right)\right) - m \left(\psi_{s_0}^s \left(E_{s_0}^{s_0}(\mathbb{R}) \cap U_{s_0}\right)\right)| < \frac{\epsilon}{2}.$$

Now we will control

$$|m \left(\psi_{s_0}^s \left(E_{s_0}^{s}(\mathbb{R}) \cap U_{s}\right)\right) - m \left(\psi_{s_0}^s \left(E_{s_0}^{s_0}(\mathbb{R}) \cap U_{s_0}\right)\right)|.$$

Namely, we consider the situation when we have a fixed curve passing through a changing

\footnote{Source: The underlying elliptic curve in this image was produced by the WolframAlpha command: “plot $y^2 = x^3 + 4x^2 + 3$. “}
open set. Let $\epsilon > 0$. Take $K$ to be some compact set in $\mathbb{R}^2$ such that

$$m(\psi^*(E_{s_0}^* \cap K^c)) < \frac{\epsilon}{2}.$$ 

By our choice of $s_0$ and the argument above we have that $D_a$ and $D_b$ are finite, namely there are only $M$ many $(u, v)$ such that $\tau(u, v, s_0)$ is equal to $a$ or $b$ where $M$ is finite. Consider the images of each of these $M$ points in $S^1$ under $\psi_{s_0}^*$. Choose an open interval of length $\frac{\epsilon}{2M}$ around each point in $S^1$. Then, the inverse images of these intervals in $S^1$ consists of a finite collection of open intervals $W_1, \ldots, W_M$ in $E_{s_0}^* \cap K$. Thus, $E_{s_0}^* \cap K \setminus \bigcup_{i=1,\ldots,M} W_i$ is a compact set of $\mathbb{R}^2$.

Let $(u, v) \in E_{s_0}^* \cap K \setminus \bigcup_{i=1,\ldots,M} W_i$. First we suppose that $\tau(u, v, s_0) \in I$. Then, as $I$ is open, there exists some $\epsilon_1$ such that the ball $B(\tau(u, v, s_0), \epsilon_1) \subset I$. By the continuity of $\tau$, there exists some $\delta_{u,v} > 0$ such that if $|s - s_0| < \delta_{u,v}$ then $|\tau(u, v, s) - \tau(u, v, s_0)| < \epsilon_1$. Hence $(u, v) \in U_s$. On the other hand, suppose $(u, v) \notin U_{s_0}$, i.e. $\tau(u, v, s_0) \notin I$. We know $\tau(u, v, s_0)$ is equal neither to $a$ nor $b$, as such $(u, v)$ would be in one of the $W_i$’s. Then, as before, we can find some $\delta_{u,v} > 0$ such that if $|s - s_0| < \delta_{u,v}$ $(u, v) \notin U_s$. As $E_{s_0}^* \cap K \setminus \bigcup_{i=1,\ldots,M} W_i$ is compact, take:

$$\delta = \inf_{u,v} \{\delta_{u,v}\} > 0.$$ 

Then, if $|s - s_0| < \delta$, the only points $(u, v) \in E_{s_0}^*$ that can change from $U_s$ to $U_{s_0}$ or vice versa are in a region of the curve whose measure after converting to $S^1$ is less than $\epsilon$.

Then, let $I$ be an interval of $\mathbb{R}$. Let $E_i$ be a fiber of the main fibration of a cross-fibered surface. We decompose $m_{E_i}(I) = vol(I_i)$ as an integral of sections

$$m_{E_i}(I) = vol(I_i) = \int_{\alpha \in S^1} m(I_{i,\alpha}^*),$$

(where the integral is the line integral over $S^1$ with respect to Haar measure). This decomposition is valid as long as $I_i$ is measurable, or equivalently, as long as the integral

$$\int_{\alpha \in S^1} m(I_{i,\alpha}^*)$$

exists.

However, as we have shown in Lemma 4.2.5 that $f(\alpha)$ is continuous except at finitely many points, the line integral is well-defined. Suppose $a$ is one of the endpoints of $I$. We
saw in the proof of Lemma 4.2.5 that the set
\[ D_a := \{(x, y) \in E_t(\mathbb{R}) : \tau(u, v, \sigma(x, y, t_0)) = a \ \forall (u, v) \in E^*_{\sigma(x, y, t_0)}(\mathbb{R})\} \]
is finite. Furthermore, we saw in this argument that for \((x, y) \notin D_a\) there are only finitely many \((u, v) \in E^*_{\sigma(x, y, t_0)}\) such that \(\tau(u, v, \sigma(x, y, t_0)) = a\). Hence if \(\alpha \in S^1\) does not correspond to \((x, y)\) in \(D_a\), subtracting or adding \(a\) to \(I\) will only change \(m(I_{t, \alpha})\) by finitely many points, and hence its measure will stay the same. So, subtracting or adding \(a\) to \(I\) will only change \(m(I_{t, \alpha})\) at finitely many values of \(\alpha\), and hence \(m_{E_t}(I)\) will not be affected. Thus, the value of \(m_{E_t}(I)\) does not depend on whether we include the endpoints of \(I\).

**Proposition 4.2.6.** As we have defined it on intervals \(I\), \(m_{E_t}(I)\) extends to a probability measure on \(\mathbb{R}\) and the Borel measure generated by open sets.

**Proof.** Note, \(f(\alpha) \geq 0\) for all \(t\) and \(\alpha\), so \(m_{E_t}(I) \geq 0\) for all \(I\). Clearly,
\[ m_{E_t}(\emptyset) = \int_{\alpha \in S^1} m(\emptyset) = 0 \]
and
\[ m_{E_t}(\mathbb{R}) = \int_{S^1} m(S^1) = 1. \]

Let \((I_k)_{k \in \mathbb{N}}\) be a countable collection of pairwise disjoint half-open intervals of \(\mathbb{R}\). Then the corresponding \(I^*_{t, \alpha}\) are disjoint sets (as \(\tau(u, v, \sigma(x, y, t))\) can only be in at most one \(I_k\) by the disjointness of the \(I_k\)'s). So, by the countable additivity of Haar measure and of the integral \(m_{E_t}(\bigcup I_k) = \sum m_{E_t}(I_k)\).

The half-open intervals form a ring of sets on which we have shown that \(m_{E_t}\) is a pre-measure. So by Carathéodory’s extension theorem, \(m_{E_t}\) extends to a measure on the \(\sigma\)-algebra generated by the half-open intervals, namely the Borel algebra generated by open sets.

**Proposition 4.2.7.** Let \(I\) be a non-empty interval of \(\mathbb{R}\) and \(E_t\) be a non-exceptional fiber of positive rank of the main fibration of a cross-fibered surface. Then \(m_{E_t}(I) > 0\).

**Proof.** Consider the open set \(U\) of \(E_t^0\) given to us by Proposition 4.1.5. There is at least one point in \(U\) at which \(\Phi\) is defined, and for all but finitely many \(P \in U\) at which \(\Phi\) is defined, there exists a non-empty open set \(U^*\) of \(E_{\sigma(P)}^0\) such that if \(P^* \in U^* \cap E_{\sigma(P)}^*(\mathbb{Q})\) (and \(\Phi^*\) is defined at \((P^*)\)), then \(\tau(P^*) \in I\). Choose such a \(P\), avoiding the images
under $\psi_t^{-1}$ of the $\alpha \in S^1$ at which $f(\alpha)$ is discontinuous, of which we know there are only finitely many by Lemma 4.2.5. Then denote $\alpha_0 = \psi_t(P)$. As $\psi_{\sigma(P)}^*$ is a homeomorphism, $\psi_{\sigma(P)}^*(U^*)$ gives a non-empty open set of $S^1$. Moreover, $\psi_{\sigma(P)}^*(U^*) \subset I_{t,\alpha_0}$; hence, $I_{t,\alpha_0}$ must have positive measure. Then, by Lemma 4.2.5, $\alpha \mapsto m(I_{t,\alpha})$ is a non-negative function on $S^1$ that is continuous at $\alpha_0$, at which it takes a positive value. Thus, the line integral of this function over $S^1$, and hence $m_{E_t}(I)$, must be positive.

We will now justify our intuition that this measure is a good representation of how large “$I$ is seen to be” by the cross-fibration structure.

**Proposition 4.2.8.** Let $P$ be a non-torsion point on a non-exceptional fiber $E_t$ in the main fibration of a cross-fibered surface, and let $I \subset \mathbb{R}$ be an interval. Let $a_1 + b_1 \mathbb{N}$ and $a_2 + b_2 \mathbb{N}$ be fixed arithmetic progressions such that $b_1$ and $b_2$ are odd. Then,

$$\lim_{N \to \infty} \lim_{M \to \infty} \frac{\# \left\{ (n, m) : n \equiv a_1 \mod b_1, n \leq N, m \equiv a_2 \mod b_2, m \leq M, n, m \text{ even}, \tau(m(nP)^*) \in I \right\}}{(N/2b_1)(M/2b_2)} = m_{E_t}(I).$$

Furthermore, if $\omega \in \mathbb{N}$,

$$\lim_{N \to \infty} \lim_{M \to \infty} \frac{\# \left\{ (n, m_1, \ldots, m_\omega) : m_j \equiv a_2 \mod b_2, m_j \leq M, n, m_j \text{ even} \right\}}{(N/2b_1)(M/2b_2)^\omega} \geq m_{E_t}(I)^\omega.$$  

**Proof.** Let $\epsilon > 0$. Denote by $\beta_1, \ldots, \beta_M$ in $S^1$ the finitely many points of discontinuity of $f(\alpha)$ from Lemma 4.2.5. Around each $\beta_g$, take an interval with endpoints $\zeta_g$ and $\eta_g$ such that $|\zeta_g - \eta_g| < \frac{\epsilon}{2M}$. We write

$$S^1_0 = S^1 \setminus \bigcup_{g=1,\ldots,M} (\zeta_g, \eta_g).$$

Note that $f^\omega$ is bounded by 1, so

$$\left| \int_{\alpha \in S^1} m(I_{t,\alpha})^\omega - \int_{\alpha \in S^1_0} m(I_{t,\alpha})^\omega \right| = \int_{\alpha \in S^1 \setminus S^1_0} m(I_{t,\alpha})^\omega \leq \frac{\epsilon}{2M} \cdot M = \frac{\epsilon}{2}.$$

Take $\epsilon_1 = \min \left( \frac{\epsilon}{4(2^{\omega}+1)}, \frac{1}{2} \right)$. Then, around any point $\alpha \in S^1_0$ there is an interval neighborhood $U_\alpha$ (note that this is possibly a half-open interval if $\alpha$ is one of the $\zeta_g$ or
such that $\alpha_1, \alpha_2 \in U_\alpha$ implies

$$|f(\alpha_1) - f(\alpha_2)| < \epsilon_1.$$  

As $S^1_0$ is compact, we can take a finite sub-covering $\mathcal{F}$ of the $U_\alpha$'s that cover it.

We approximate the integral $\int_{\alpha \in S^1_0} m(I^*_t,\alpha)^\omega$ via a step function such that

$$\left| \int_{\alpha \in S^1_0} m(I^*_t,\alpha)^\omega - \sum_{i=1}^K a_i \text{length}(I_i) \right| < \epsilon_1.$$  

We can assume that each of the $K$ many intervals $I_i$ is contained in an element of $\mathcal{F}$ such that $a_i = m(I^*_l,\lambda)^\omega$ for some $\lambda_i$ in $I_i$.

Take $\epsilon_2 = \min\left(\frac{\epsilon}{2\pi + 2\pi}, \frac{1}{2}\right)$. If $E_t(\mathbb{R})$ has two components, under the isomorphism

$$E_t(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

the point $P$ will go to either a pair of the form $(\gamma,0)$ or $(\gamma,1)$, where $\gamma$ is an irrational number because $P$ is a non-torsion point. In either case, $2P$ is sent to a pair of the form $(2\gamma,0)$ (and generally any even multiple of $P$ will automatically be on the identity component). Alternatively, if $E_t(\mathbb{R})$ has one component, take $\gamma = \psi_i^{-1}(P)$. In either case, we can apply our observations about irrational rotations above to the rotation corresponding to addition of $2b_1\gamma$ for each $I_i$. In the case where $a_1$ is odd (and using the fact that $b_1$ is odd):

$$\lim_{N \to \infty} \frac{\#\{n \leq N, n \equiv a_1 \mod b_1, n \text{ even : } n\gamma \in I_i\}}{N/2b_1}$$

$$= \lim_{N \to \infty} \frac{\#\{k : a_1 + (2k + 1)b_1 \leq N, (a_1 + (2k + 1)b_1)\gamma \in I_i\}}{N - \frac{a_1 - b_1}{2b_1}}$$

$$= \lim_{N \to \infty} \frac{\#\{k \leq \frac{N - a_1 - b_1}{2b_1} : k(2b_1\gamma) \in I_i - (a_1 + b_1)\gamma\}}{N - \frac{a_1 + b_1}{2b_1}}$$

$$= \text{length}(I_i - (a_1 + b_1)\gamma) = \text{length}(I_i).$$

If $a_1$ is even:

$$\lim_{N \to \infty} \frac{\#\{n \leq N, n \equiv a_1 \mod b_1, n \text{ even : } n\gamma \in I_i\}}{N/2b_1}$$
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

\[
= \lim_{N \to \infty} \# \left\{ k : a_1 + 2kb_1 \leq N, (a_1 + 2kb_1)\gamma \in I_i \right\}
\]

\[
= \lim_{N \to \infty} \# \left\{ k \leq \frac{N-a_1}{2b_1} : k(2b_1\gamma) \in I_i - a_1\gamma \right\}
\]

\[
= \text{length}(I_i - a_1\gamma) = \text{length}(I_i).
\]

Choose \( N_0 \) such that if \( N \geq N_0 \):

\[
\left| \frac{\# \{ n \leq N, n \equiv a_1 \mod b_1, n \text{ even} : n\gamma \in I_i \}}{N/2b_1} - \text{length}(I_i) \right| < \epsilon_2.
\]

Then, for each \( n = 1, ..., N \), denote \( \alpha_n = n\gamma \). Note

\[
\psi_t^{-1}(\alpha_n) = \psi_t^{-1}(n\gamma) =nP = (x_n, y_n).
\]

Further, denote

\[
\theta_n = \psi_{\sigma(x_n, y_n, t)}^*(nP) \in S^1.
\]

Now, for each \( N \), by the same argument as above applied to the (finitely many) irrational rotations corresponding to addition of \( 2b_2\theta_n \) for \( n = 1, ..., N \), we can choose \( M_N \) such that if \( M \geq M_N \):

\[
\left| \frac{\# \{ m \leq M, m \equiv a_2 \mod b_2, m \text{ even} : m\theta_n \in I_{t,\omega_n}^* \}}{M/2b_2} - m(I_{t,\omega_n}^*) \right| < \epsilon_2.
\]

Then, by the triangle inequality, if \( \alpha_n \in I_i \):

\[
\left| \frac{\# \{ m \leq M, m \equiv a_2 \mod b_2, m \text{ even} : m\theta_n \in I_{t,\omega_n}^* \}}{M/2b_2} - m(I_{t,\omega_n}^*) \right| < \epsilon_1 + \epsilon_2.
\]

However,

\[
\# \left\{ (n, m_1, ..., m_\omega) : n \leq N, n \equiv a_1 \mod b_1, m_j \leq M, m_j \equiv a_2 \mod b_2,
\text{\( n, m_j \) even, } \alpha_n \in I_i \text{ and } m_j\theta_n \in I_{t,\omega_n}^* \forall j = 1, ..., \omega \right\}
\]

\[
\leq \# \left\{ n \leq N, \text{ even : } n\gamma \in I_i \right\} \cdot \max_{n,\omega_n \in I_i} \left\{ \# \left\{ m \leq M, \text{ even : } m\theta_n \in I_{t,\omega_n}^* \right\} \right\}^\omega
\]
So,

\[
\# \left\{ (n, m_1, \ldots, m_\omega) : \begin{array}{l}
  n \leq N, n \equiv a_1 \mod b_1, m_j \leq M, m_j \equiv a_2 \mod b_2, \\
  n, m_j \text{ even}, \alpha_n \in I_i \text{ and } m_j \theta_n \in I_{t,\alpha_n}^* \forall j = 1, \ldots, \omega
\end{array} \right\}
\]

\[
\frac{(N/2b_1)(M/2b_2)^\omega}{\omega}
\]

\[
< (\text{length}(I_i) + \epsilon_2) \left( m(I_{t,\lambda_i}^*) + \epsilon_1 + \epsilon_2 \right)^\omega
\]

\[
\leq \text{length}(I_i)m(I_{t,\lambda_i}^*)^\omega + \epsilon_2 2^\omega + \text{length}(I_i)(\epsilon_1 + \epsilon_2)2^\omega,
\]

where we used the facts that

\[
0 \leq m(I_{t,\lambda_i}^*) \leq 1, 0 \leq \epsilon_1, \epsilon_2 \leq \frac{1}{2}, \text{ and } \sum_{s=1}^\omega \binom{\omega}{s} = 2^\omega - 1.
\]

Establishing a similar lower bound, we have:

\[
\# \left\{ (n, m_1, \ldots, m_\omega) : \begin{array}{l}
  n \leq N, n \equiv a_1 \mod b_1, \\
  m_j \leq M, m_j \equiv a_2 \mod b_2, \\
  n, m_j \text{ even}, \alpha_n \in I_i \text{ and } m_j \theta_n \in I_{t,\alpha_n}^* \forall j = 1, \ldots, \omega
\end{array} \right\}
\]

\[
\frac{(N/2b_1)(M/2b_2)^\omega}{\omega}
\]

\[
- m(I_{t,\lambda_i}^*)^\omega \text{length}(I_i)
\]

\[
< \epsilon_2 2^\omega + \text{length}(I_i)(\epsilon_1 + \epsilon_2)2^\omega.
\]

Then,

\[
\# \left\{ (n, m_1, \ldots, m_\omega) : \begin{array}{l}
  n \leq N, n \equiv a_1 \mod b_1, m_j \leq M, m_j \equiv a_2 \mod b_2, \\
  n, m_j \text{ even}, \text{ and } m_j \theta_n \in I_{t,\alpha_n}^* \forall j = 1, \ldots, \omega
\end{array} \right\}
\]

\[
\frac{(N/2b_1)(M/2b_2)^\omega}{\omega}
\]

\[
= \sum_{i=1}^K \frac{(N/2b_1)(M/2b_2)^\omega}{\omega}
\]

\[
= \sum_{i=1}^K \# \left\{ (n, m_1, \ldots, m_\omega) : \begin{array}{l}
  n \leq N, n \equiv a_1 \mod b_1, m_j \leq M, m_j \equiv a_2 \mod b_2, \\
  n, m_j \text{ even}, \alpha_n \in I_i \text{ and } m_j \theta_n \in I_{t,\alpha_n}^* \forall j = 1, \ldots, \omega
\end{array} \right\}
\]

\[
\frac{(N/2b_1)(M/2b_2)^\omega}{\omega}.
\]
So,

\[
\begin{align*}
\# \left\{ (n, m_1, \ldots, m_\omega) : & \quad n \leq N, m_j \leq M, n, m_j \text{ even}, \\
& \quad n \equiv a_1 \mod b_1, m_j \equiv a_2 \mod b_2, \\
& \quad \text{and } m_j \theta_n \in I_{i,\alpha}^t \forall j = 1, \ldots, \omega \right\} &\leq \sum_{i=1}^{K} a_i \text{length}(I_i) - \frac{K}{2} \left(\frac{N}{2b_1}\right) \left(\frac{M}{2b_2}\right) \omega
\end{align*}
\]

\[
\begin{align*}
< & \sum_{i=1}^{K} (\epsilon_2 2^\omega \text{length}(I_i)) (\epsilon_1 + \epsilon_2) 2^\omega \\
\leq & \ K \cdot 2^\omega \epsilon_2 + 2^\omega (\epsilon_1 + \epsilon_2),
\end{align*}
\]
as \[
\sum_{i=1}^{K} \text{length}(I_i) = 1.
\]

Now finally,

\[
\begin{align*}
\# \left\{ (n, m_1, \ldots, m_\omega) : & \quad n \leq N, n \equiv a_1 \mod b_1, m_j \leq M, m_j \equiv a_2 \mod b_2, \\
& \quad n, m_j \text{ even, and } m_j \theta_n \in I_{i,\alpha}^t \forall j = 1, \ldots, \omega \right\} &\leq \int_{\alpha \in S^1} m(I_{i,\alpha}^t)^\omega
\end{align*}
\]

\[
\begin{align*}
< & \ K \cdot 2^\omega \epsilon_2 + 2^\omega (\epsilon_1 + \epsilon_2) + \epsilon_1 + \int_{\alpha \in S^1} m(I_{i,\alpha}^t)^\omega - \int_{\alpha \in S^1_0} m(I_{i,\alpha}^t)^\omega \\
\leq & \ (K + 1) 2^\omega \epsilon_2 + (2^\omega + 1) \epsilon_1 + \frac{\epsilon}{2}
\end{align*}
\]

\[
\leq \frac{\epsilon}{4} + \frac{\epsilon}{4} + \frac{\epsilon}{2} = \epsilon.
\]

However, note that the condition \(m \theta_n \in I_{i,\alpha_m}^t\) is equivalent to

\[
\left\{ \begin{array}{l}
\psi^{-1}_t(\alpha_n) = (x, y) \in E_t^0(\mathbb{R}) \\
\psi^{-1}_{\sigma(x,y,t)}(m \theta_n) = (u, v) \in E_{\sigma(x,y,t)}^0(\mathbb{R}) \\
\tau(u, v, \sigma(x,y,t)) \in I
\end{array} \right\}
\]

for any of the all but finitely many \(n\) such that the conversion map \(\Phi\) is defined at \((x, y, t)\) and such that \(rk(E_{\sigma(x,y,t)}^0(\mathbb{Q})) \geq 1\), and for each such \(n\) the all but finitely many \(m\) such that the conversion map \(\Phi^*\) is defined at \((u, v, \sigma(x, y, t))\). Note that these \(n\) and \(m\) do not
affect the limit. Furthermore, as \( \psi_i^{-1}(\alpha_n) = \psi_i^{-1}(n\gamma) = nP \) (where the multiplication on the right is in \( S^1 \) and the multiplication on the left is elliptic curve multiplication, and noting that \( nP \in E_t^0(\mathbb{R}) \) because \( n \) is even), and

\[
\psi_{\sigma(nP)}^*(m\theta_n) = m(nP)^*
\]

(which similarly is in \( E_{\sigma(nP)}^0(\mathbb{R}) \) because \( m \) is even). Namely, \( m\theta_n \in I_{\sigma(nP)}^* \) is equivalent to \( \tau(m(nP)^*) \in I \). This shows that

\[
\lim_{N \to \infty} \lim_{M \to \infty} \# \left\{ (n, m_1, ..., m_\omega) : \begin{array}{l}
\quad n \equiv a_1 \mod b_1, n \leq N, \\
\quad m_j \equiv a_2 \mod b_2, m_j \leq M, n, m_j \text{ even} \\
\quad \tau(m_j(nP)^*) \in I \forall j = 1, ..., \omega \\
\end{array} \right\} = \int_{\alpha \in S^1} m(I_\alpha^*)^\omega \frac{(N/2b_1)(M/2b_2)}{\omega} - m_{E_1}(I) < \epsilon.
\]

from which the \( \omega = 1 \) case gives the first claim of the statement.

Note that adding the assumption that the \( m_j \) be distinct does not change the limit. But then by Hölder’s inequality, as the integral is over \( S^1 \), a finite measure space of measure 1,

\[
\left( \int_{\alpha \in S^1} m(I_\alpha^*)^\omega \right)^{1/\omega} \geq \int_{\alpha \in S^1} m(I_\alpha^*) = m_{E_1}(I)
\]

We impose the conditions that \( b_1 \) and \( b_2 \) be odd, and we only include even \( n \) and \( m \) in our count, so that, when applying the irrational circle rotation arguments, we know a priori that the point we are adding is on the identity component.

Then, a fiber \( E_t \) in the main fibration of a cross-fibered surface \( \mathcal{E} \), \( P \in E_t(\mathbb{R}) \), \( a_1 + kb_1 \) and \( a_2 + kb_2 \) arithmetic progressions with \( b_1, b_2 \) odd, and \( \epsilon > 0 \), we denote \( N(\mathcal{E}, E_t, P, I, a_1, b_1, a_2, b_2, \epsilon) \) such that if \( N, M > N(\mathcal{E}, E_t, P, I, a_1, b_1, a_2, b_2, \epsilon) \),

\[
\begin{vmatrix}
\# \left\{ (n, m) : \begin{array}{l}
\quad n \equiv a_1 \mod b_1, m \equiv a_2 \mod b_2, n \leq N, \\
\quad m \leq M, n, m \text{ even} , \tau(m(nP)^*) \in I \\
\end{array} \right\} - m_{E_1}(I) \\
\end{vmatrix}_{(N/2b_1)(M/2b_2)} < \epsilon. 
\]

When there is no ambiguity, we abbreviate this notation by writing

\[
N(P, I, \epsilon) = N(\mathcal{E}, E_t, P, I, a_1, b_1, a_2, b_2, \epsilon).
\]
Generally, we do not have good methods to compute \( m_{E_t}(I) \) and \( N(P, I, \epsilon) \) given \( E_t \), \( P \), \( I \), and \( \epsilon \). A naive approach would be to take larger and larger \( N \) and \( M \) and compute the ratio of Proposition 4.2.8 until it seems to converge. However, doing this we will never know if the \( N \) and \( M \) we are taking are sufficiently large to get convergence, and hence we cannot prove that the approximations we compute are actually close to \( m_{E_t}(I) \).

We present in Algorithm 1 a way to compute a (verifiable) lower bound for \( m_{E_t}(I) \), using ideas from the proof of Lemma 4.2.5. We find an interval \( U \) of \( E_t \) and a constant \( \delta^* > 0 \) such that for any \( P \in U \), \( I_{t, \psi_t(P)}^* \) contains an interval \( U_n^* \) with

\[
m(\psi_t^*(U_n^*) \cap \tau^{-1}(I)) \geq \delta^*.
\]

Then, \( \delta^* \cdot m(\psi_t(U)) \) provides a lower bound for \( m_{E_t}(I) \). We essentially find a rectangle in \( \mathbb{I}_t \).

Note that we will use the reasoning we employed in Lemma 4.2.5 and in Figure 4.3 related to the positioning of the extrema of the \( x \) and \( y \) coordinate functions to be able to say that our intervals \( U_n^* \cap \tau^{-1}(I) \) are mapped to intervals in \( S^1 \) under \( \psi_s^* \), so that we can bound \( m(\psi_s^*(U_n^*) \cap \tau^{-1}(I)) \) by the length of an interval in \( S^1 \). We use the continuity of the functions we examined in Lemma 4.2.5. Luckily, these are fairly explicit functions, so given an \( \epsilon > 0 \), we can find explicit \( \delta \)-balls. Note that this includes the functions which were defined as power series that were used in the computation of \( \phi_{u_0, v_0} \), as their tails can be approximated by geometric series leaving us with rational functions.

We could now try to find an upper bound on \( m_{E_t}(I) \) by finding lower bounds on \( m_{E_t}(\mathbb{R}\setminus I) \) (where we should first split \( \mathbb{R}\setminus I \) into intervals and bound the measure of each), but Algorithm 1 is far from optimal, so it is unlikely that these two bounds will be the same.

We cannot generally compute \( N(P, I, \epsilon) \), so instead we consider how many terms we must take in equation (4.6) to guarantee that the ratio is greater than some fixed lower bound. Then, given a fiber \( E_t \) in the main fibration of a cross-fibered surface \( \mathcal{E} \), \( P \in E_t(\mathbb{R}) \), \( a_1 + kb_1 \) and \( a_2 + kb_2 \) arithmetic progressions with \( b_1, b_2 \) odd, and \( z > 0 \), we denote by \( N_0(\mathcal{E}, E_t, P, I, a_1, b_1, a_2, b_2, z) \) the quantity such that if \( N, M > N_0(\mathcal{E}, E_t, P, I, a_1, b_1, a_2, b_2, z) \),

\[
\#
\left\{(n, m) : \begin{align*}
n &\equiv a_1 \mod b_1, n \leq N, m \equiv a_2 \mod b_2, m \leq M, \\
n, m &\text{ even }, \tau(m(nP)^*) \in I \\
(N/2b_1)(M/2b_2) &\geq z
\end{align*}\right\} \geq z. \tag{4.7}
\]

As above, when there is no ambiguity, we abbreviate \( N_0(\mathcal{E}, E_t, P, I, a_1, b_1, a_2, b_2, z) \) by
function FIND_LOWER_BOUND_FOR_mE_t(I)(E_t, E_t, P, I) = L

a, b ← the endpoints of I

while t_output ∉ I do
  ⊢ First we try to find some n and m that yield a point in I
  n, m ← randomly chosen element of 2N (up to some reasonable size)
  (x_n, y_n) ← nP
  (u_n, v_n) ← (nP)*
  (u_n,m, v_n,m) ← m(nP)*
  t_output = τ(u_n,m, v_n,m, σ(x_n, y_n, t))

end while

(x0, y0) ← (x_n, y_n), (w0, z0) ← (u_n, v_n), (u0, v0, s0) ← (u_n,m, v_n,m, σ(nP))

ε_1 ← min {∥a - τ(u0, v0, s0)∥, ∥b - τ(u0, v0, s0)∥}

δ_1 ← Positive value such that

(u_0 - δ_1, u_0 + δ_1) × (v_0 - δ_1, v_0 + δ_1) × (s_0 - δ_1, s_0 + δ_1)

⊂ τ^{-1}((τ(u0, v0, s0) - ε_1, τ(u0, v0, s0) + ε_1))

u_j ← Find the (up to five) u that solve 3u^2 + c(s_0) = 0 or u^3 + c(s_0)u + d(s_0) = 0

v_j ← Approximate value of v = √{u_j^3 + c(s_0)u_j + d(s_0)} for each j

if u_j = u_0 or v_j = v_0 for some j (to within known bounds) then
return Algorithm fails for this n and m. Choose n and m differently and repeat.

end if

δ_2 ← δ_1

▷ We found the local extrema P_j as in Lemma 4.2.5

for j = 1, ..., 5 do
  ⊢ We shrink target region to R to avoid P_j's
  while u_j ∈ (u_0 - δ_2, u_0 + δ_2) or ±v_j ∈ (v_0 - δ_2, v_0 + δ_2) do
    δ_2 ← δ_2/2
  end while

end for

R ← (u_0 - δ_2, u_0 + δ_2) × (v_0 - δ_2, v_0 + δ_2)

for j = 1, ..., 5 do

ε_j' ←

min {∥u_j - (u_0 + δ_2)∥, ∥u_j - (u_0 - δ_2)∥, |±v_j - (v_0 + δ_2)|, |±v_j - (v_0 - δ_2)|}

δ_j' ← 1

success ← 0

while success = 0 do
  Bound solutions u to 3u^2 + c(s) = 0 and u^3 + c(s)u + d(s) = 0 for |s-s_0| < δ_j'
  Bound corresponding v = √{u_j^3 + c(s)u_j + d(s)}
  if Bounds are such that for these (u, v): |u - u_j| ≤ ε_j and |±v - v_j| ≤ ε_j' then
    success ← 1
  else
    δ_j' ← δ_j'/2
  end if

end while

end for

Algorithm 1: Algorithm to lower bound m_{E_t}
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

$m \leftarrow$ randomly chosen number in $2N$ different from $m$ that produced $(u_0, v_0)$

**while** $m(nP)^* \not\in \mathcal{R}$ **do**    
  ▷ Find some other $m$ that yields a point on $E^*_s$ in $\mathcal{R}$
  $m \leftarrow$ randomly chosen number in $2N$ different from $m$ that produced $(u_0, v_0)$
  $(u_{n,m}, v_{n,m}) \leftarrow m(nP)^*$
  $t_{output} = \tau(u_{n,m}, v_{n,m}, \sigma(x_n, y_n, t))$
  **end while**

$(u_1, v_1, s_0) \leftarrow (u_{n,m}, v_{n,m}, \sigma(nP))$

$\delta^* \leftarrow$ length between $\psi^*_s(u_0, v_0)$ and $\psi^*_s(u_1, v_1)$

$\delta_3 \leftarrow$ Positive value such that $|s - s_0| < \delta_3$ implies

$$||\phi_{u_0,v_0}(s) - \phi_{u_0,v_0}(s_0)||_{\mathbb{R}^2} < \delta_2$$

$\delta_4 \leftarrow$ Positive value such that $|s - s_0| < \delta_4$ implies

$$||\phi_{u_1,v_1}(s) - \phi_{u_1,v_1}(s_0)||_{\mathbb{R}^2} < \delta_2$$

▷ This guarantees that the points in $S^1$ corresponding to $(u_0, v_0)$ and $(u_1, v_1)$ stay in $\mathcal{R}$ as $s$ varies

$\delta_5 \leftarrow \min \{\delta_1, \delta_3, \delta_4, \delta_5's\}$

$\delta_6 \leftarrow$ Positive value such that $||(x, y) - (x_0, y_0)||_{\mathbb{R}^2} < \delta_6$ implies

$$|\sigma(x, y, t_0) - \sigma(x_0, y_0, t_0)| < \delta_5$$

$x_l \leftarrow$ Find the (up to five) $x$ that solve $3x^2 + a(t) = 0$ or $x^3 + a(t)u + b(t) = 0$

$y_l \leftarrow$ Approximate value of $y = \sqrt{x_l^2 + a(t)x_l + b(t)}$ for each $l$

if $x_l = x_0$ or $y_l = y_0$ for some $l$ (to within known bounds) then

**return** Algorithm fails for this $n$. Choose $n$ differently and repeat.

  **end if**

$\delta_7 \leftarrow \min \{|x_l - x_0|, |\pm y_l - y_0|\}$

▷ Now we bound away from the local extrema in $E^0_t(\mathbb{R})$

$\delta_8 \leftarrow \min \{\delta_6, \delta_7\}$

$n \leftarrow$ randomly chosen number in $2N$ different from $n$ that produced $(x_0, x_0)$

success $\leftarrow 0$

**while** success $= 0$ **do**

$(x_n, y_n) \leftarrow nP$

if $||(x_n, y_n) - (x_0, y_0)||_{\mathbb{R}^2} < \delta_8$ then

success $\leftarrow 1$

else $n \leftarrow$ randomly chosen number in $2N$ different from $n$ that produced $(x_0, y_0)$

**end if**

**end while**

$(x_1, y_1) \leftarrow (x_n, y_n)$

$\delta \leftarrow$ length between $\psi_t(x_0, y_0)$ and $\psi_t(x_1, y_1)$ in $S^1$

**return** $L = \delta \cdot \delta^*$ which is a lower bound for $m_{E_t}(I)$

**end function**

Algorithm to lower bound $m_{E_t}$ (continued)
Algorithm 1 allows us to produce a lower bound $L$ for $m_{E_i}(I)$, but it is not quite sufficient to find a bound on $N_0(P, I, L)$. However, in Algorithm 2 we will see that we can modify Algorithm 1 so that it does give such a bound.

Finding such bounds is related to the rate of convergence of the limit in the Ergodic Theorem for irrational circle rotations that we considered in equation (4.5) in the beginning of this section. However, this rate of convergence depends greatly on the irrational number $\theta$. Values of $\theta$ that well-approximate rational numbers lead to very slow convergence. For a given $\theta$ and $\epsilon > 0$, the smallest $k_0 \in \mathbb{N}$ such that $k_0 \theta \in [0, \epsilon)$ can be calculated in terms of the continued fraction expansion of $\theta$ (see [17]). Then, for $I$ an interval of length $\epsilon$ and $N \in \mathbb{N}$, if one computes $\epsilon_1 = k_0 \epsilon > 0$, the set $\{nk_0 \theta \in I : n \leq N\}$ will have at least $\lfloor N\epsilon_1 \rfloor$ elements. So the set $\{n\theta \in I : n \leq N\}$ has at least $\lfloor \frac{N\epsilon_1}{k_0} \rfloor$ elements. If $N \geq \frac{k_0}{\epsilon_1}$,

$$\left\lfloor \frac{N\epsilon_1}{k_0} \right\rfloor \geq \frac{N\epsilon_1}{2k_0}.$$

Thus,

$$\frac{\# \{n\theta \in I : n \leq N\}}{N} \geq \frac{\epsilon_1}{2k_0}.$$

The major difficulty in Algorithm 2 is that the rate of convergence will depend on the continued fraction expansion of $\psi_s^*(nP)^{*}$. We will be able to choose our $n$ so that these all give roughly the same rate of convergence. Our target interval for these points will have length $\delta^*$, which we compute in Algorithm 1. In Algorithm 1 we also produce a point $P$, $n$, and $m$ such that $t_{n,m}(P) \in I$. Take $\beta = \psi_{s_n}^*((nP)^{*}) \in S^1$. Then, if we find that $k_0$ is the smallest natural such that $k_0 \beta \in [0, \delta^*)$, we define $\epsilon_0 = \delta^* - k_0 \beta > 0$. Then, we will restrict ourselves to only choosing further $n$ such that $\psi_{s_n}^*((nP)^{*}) \in \left(\beta, \beta + \frac{\epsilon_0}{k_0}\right)$. For such $n$, $k_0 \psi_{s_n}^*((nP)^{*}) \in (k_0 \beta, \delta^*) \subset [0, \delta^*)$.

Now suppose for a fixed $\mathcal{E}$, $P$, and $I$ we have performed Algorithm 2 to produce $z > 0$ and $N_0(P, I, z)$. Then, if we were to perform the process of Theorem 4.1.6 we can state its running time in terms of $z$ and $N(P, I, z)$. We note in Algorithm 3

$$\hat{h}(W) = \hat{h}((m(nP)^{*}) \leq \text{poly}(m^2 \hat{h}(nP)^{*}), ht(s_n)) \leq \text{poly}(m^2 \text{poly}(n^2 \hat{h}(P), ht(t)), \text{poly}(ht(x_n), ht(y_n), ht(t))) \leq \text{poly}(N_0(P, I, z), \hat{h}(P), ht(t)).$$

Then, the maximum size of the intermediate values with which we are doing computations is $\text{poly}(\ln p, N(P, I, z), \hat{h}(P), ht(t))$, where the polynomial only depends on the cross-fibered surface $\mathcal{E}$ (and not on our choices of $p$, $I$, $t$, and $P$).
function \textsc{find}_z \textsc{and}_{\mathcal{N}_0}(P, I, z)(\mathcal{E}, E_t, P, I)= (z, K)

We perform Algorithm 1 up until the computation of $\delta_8$

Hence we have $x_0, y_0, w_0, u_0, v_0, s_0, \delta^*$, and $\delta_8$

$\beta \in S^1 \leftarrow \psi^*_{s_0}(w_0, z_0)$

$k_0 \leftarrow$ smallest natural number such that

$$k_0 \beta \in [0, \delta^*)$$

(computed, for example, by the methods of [17])

$\epsilon_0 \leftarrow k_0 \beta$

$\epsilon \leftarrow \delta^* - k_0 \beta > 0$

$n \leftarrow$ randomly chosen number in $2\mathbb{N}$ different from $n$ that produced $(x_0, x_0)$

success $\leftarrow 0$

\textbf{while} success $= 0$ \textbf{do}

\hspace{1em} $(x_n, y_n) \leftarrow nP$

\hspace{1em} $(u_n, v_n) \in E_{s_n} \leftarrow (nP)^*$

\hspace{1em} if $|| (x_n, y_n) - (x_0, y_0) ||_{\mathbb{R}^2} < \delta_8$ and $\psi^*_{s_n}((nP)^*) \in (\beta, \beta + \frac{\epsilon_0}{k_0})$ then

\hspace{1em} success $\leftarrow 1$

\hspace{1em} else $n \leftarrow$ randomly chosen number in $2\mathbb{N}$ different from $n$ that produced $(x_0, y_0)$

\textbf{end while}

$(x_1, y_1) \leftarrow (x_n, y_n)$

$\delta \leftarrow$ length between $\psi_t(x_0, y_0, t)$ and $\psi_t(x_1, y_1, t)$ in $S^1$

$\alpha \leftarrow \psi_t(x_0, y_0) \in S^1$

$k_1 \leftarrow$ smallest natural number such that

$$k_1 \alpha \in [0, \delta)$$

$\epsilon_1 \leftarrow k_1 \alpha$

\textbf{return} $z \leftarrow \frac{\epsilon_0 \epsilon_1}{16 \delta_0 k_1}$

\textbf{return} $K = \max \left\{ \frac{2k_0}{\epsilon_0}, \frac{2k_1}{\epsilon_1} \right\}$

\textbf{end function}

Algorithm 2: Algorithm to find $\mathcal{N}_0(P, I, z)$ for some $z > 0$
Furthermore, every \( \frac{4}{z} \) attempts at the while loop, we expect to find \( t_{\text{output}} \in I \). Hence, Algorithm 3 is a randomized algorithm with average running time bounded by

\[
\frac{1}{z} \text{poly}(\ln p, N_0(P, I, z), \hat{h}(P), ht(t)).
\]

If we had access to \( m_{E_t}(I) \) and \( N(P, I, m_{E_t}(I)/2) \), then the average running time would be bounded by

\[
\frac{1}{m_{E_t}(I)} \text{poly}(\ln p, N(P, I, m_{E_t}(I)/2), \hat{h}(P), ht(t)).
\]

```
function FIND_POS_RANK_FIBER_IN_I_RAND(\( \mathcal{E}, E_{t_0}, P, \mathbb{F}_p, I \)) = (E_{t_{\text{output}}}, W)
    (x, y) ← P
    s ← \sigma(x, y, t)
    N ← N_0(\mathcal{E}, E_{t_0}, P, 1, 1, 1, 1, z) by Algorithm 2
    t_{\text{output}} ← t_0
    W ← P
    while \( t_{\text{output}} \not\in I \) do
        n ← random natural number in \([1, N]\)
        m ← random natural number in \([1, N]\)
        (x_n, y_n) ← nP
        (u_{n,m}, v_{n,m}) ← m(nP)^
        t_{\text{output}} = \tau(u_{n,m}, v_{n,m}, \sigma(x_n, y_n, t))
        W ← (m(nP))^
    end while
    return E_{t_{\text{output}}} and W
end function
```

Algorithm 3: Algorithm to find a fiber of positive rank in fixed interval \( I \) given a non-torsion point on a fiber a priori outside \( I \) by choosing random \( n \) and \( m \)

### 4.3 Other diffusive properties on cross-fibered surfaces

In this section we consider other properties that, like non-torsion points, are spread to other fibers by a cross-fibration.
4.3.1 Candidate lifts

We are now in position to prove what we stated in Proposition 1.3.6 of the Introduction, namely, that on cross-fibered surfaces, the property of being a candidate lift (plus an additional technical condition) is diffusive in the sense of Mazur’s conjecture. Thus, we see that the structure of cross-fiberedness spreads other properties than just that of having positive rank. We state a slightly more precise version of this result:

Proposition 4.3.1. Let \( \tilde{E} \) be an elliptic curve over a finite field \( \mathbb{F}_p \) (where \( p > 23 \)) such that \( \# \tilde{E}(\mathbb{F}_p) \) is prime. Let \( E \) be a cross-fibered elliptic surface of which \( \{E_t\} \) is the main fibration. Then fibers \( E_t \) such that:

- \( E_t \) is a candidate lift of \( \tilde{E} \) and
- \( \exists \) a non-zero point \( \tilde{P} \in E_t(\mathbb{F}_p) \) such that \( \tilde{P}^* \) is a non-zero point of odd order on its cross-fiber \( E_{\sigma(\tilde{P})}^*(\mathbb{F}_p) \)

are diffusive. Namely,

\[
\left\{ t \in \mathbb{Q} : E_t \text{ is a candidate lift of } \tilde{E} \text{ on which } \exists \text{ a non-zero point } \tilde{P} \in E_t(\mathbb{F}_p) \text{ such that } \tilde{P}^* \text{ is a non-zero point of odd order on } E_{\sigma(\tilde{P})}^*(\mathbb{F}_p) \right\}
\]

is dense in \( \mathbb{R} \) or finite. In fact, if this set is finite, its number of elements is bounded by the sum of the bounds of Propositions 4.1.9 and 4.1.10.

Note that the existence of a point on \( E_t(\mathbb{F}_p) \) for some \( t \) that is converted to a non-zero point on a non-singular cross-fiber implies already that \( E \) has non-trivial reduction mod \( p \) as a cross-fibered surface. (Thus, if \( E \) does not have good reduction as cross-fibered surface, the set of such fibers will be empty and we will satisfy the second possibility of diffusion.)

Proof. The proof of this proposition is similar to the proof of Theorem 4.1.6. We will just choose \( n \) and \( m \) subject to additional conditions. Furthermore, we can now take advantage of Proposition 4.2.8 to simplify the argument.

Denote \( \# \tilde{E}(\mathbb{F}_p) = l \), which by assumption is prime. Take \( E_t \) to be a fiber satisfying all of the properties of the statement (if only finitely many such fibers exist, then we satisfy the second alternative) that is not one of the finitely many exceptional fibers. We have seen that the number of exceptional fibers is bounded by the bounds in Propositions 4.1.9 and 4.1.10. Further, consider \( \tilde{P} \in E_t(\mathbb{F}_p) \), the non-zero point given to us such that
\( \tilde{P}^* \) has odd order in \( E_{\sigma(\tilde{P})}^*(\mathbb{F}_p) \). (In particular, this implicitly assumes that \( * \) is defined at \( \tilde{P} \) and that \( E_{\sigma(\tilde{P})}^*(\mathbb{F}_p) \) is non-singular.)

As \( E_t \) is a candidate lift of \( \tilde{E} \), we know it has non-torsion points with non-trivial reduction. Suppose we have such a point \( R \). As \( l \) is prime, the subgroup of \( E_t(\mathbb{F}_p) \) generated by \( \tilde{R} \) is the whole group. Thus, we can lift \( \tilde{P} \) to a multiple of \( R \) and hence a non-torsion point \( P \).

As \( l \) is prime and \( \tilde{P} \not\equiv \tilde{O} \), we know \( \text{ord}_{E_t(\mathbb{F}_p)}(P) = l \). (Further, note as \( p > 23 \), \( l \) is greater than 2 and hence odd by the Hasse bound.) Denote \( \text{ord}_{E_{\sigma(\tilde{P})}}(P^*) = r \), which we know by assumption is odd. As \( I \) is a non-empty interval, we know by Proposition 4.2.7 that \( m_{E_t}(I) > 0 \). Now, by Proposition 4.2.8 there must exist infinitely many \( n \) in the arithmetic progression \( 1 + lN \) and, for each \( n \), infinitely many \( m \) in the progression \( 1 + rN \) such that \( \tau((m(nP)^*)^*) \in I \). (Otherwise, the double limit in Proposition 4.2.8 would be zero.) By Definition 1.3.4, as we have assumed that \( E_t \) is a non-exceptional fiber, for all but finitely many \( n \), only finitely many points on \( E_{\sigma(nP)}^*(\mathbb{Q}) \) convert to torsion points under \( \Phi^* \). Thus, we can choose \( n \) and \( m \) such that \( (m(nP)^*)^* \) is a non-torsion point on its fiber and \( t_{n,m} = \tau((m(nP)^*)^*) \in I \).

Recall that we commented in Section 4.1 that, for any (pre-)crossfibered surface, the transition map \( \Phi \) commutes with reduction modulo a prime. This resulted from the fact that \( \Phi \) is (locally) defined by rational maps \( \nu(x,y,t) \), \( \nu(x,y,t) \), and \( \sigma(x,y,t) \). Then, for a point \( (x,y) \in E_t(\mathbb{Q}) \), reducing mod \( p \) and applying these rational maps is the same as applying the maps before reduction.

Then,

\[ nP \equiv P \mod p \]

because \( n \in 1 + lN \). As the transformation \( \Phi \) commutes with reduction mod \( p \),

\[ (nP)^* \equiv P^* \mod p, \]

and

\[ \sigma(nP) \equiv \sigma(P) \mod p. \]

Similarly, the map \( \Phi^* \) also commutes with reduction mod \( p \). Then,

\[ m(nP)^* \equiv (nP)^* \equiv P^* \mod p \]

because \( m \in 1 + rN \). Converting back, we find

\[ (m(nP)^*)^* \equiv (P^*)^* = P \mod p, \]
and 
\[ t_{n,m} = \tau((m(nP)^*)^*) \equiv \tau((P^*)^*) = \tau(P) = t \mod p. \]

In particular, \((m(nP)^*)^*\) does not reduce to zero \mod \(p\) because \(P\) does not.

Thus, we have produce a non-torsion, non-trivially reducing point on a fiber \(E_{t_{n,m}}\) that is isomorphic to \(E_t\) and hence \(\tilde{E}\) over \(\mathbb{F}_p\) such that \(t_{n,m} \in I\). The property that there exist a non-zero point \(\tilde{P} \in E_{t_{n,m}}(\mathbb{F}_p)\) such that \(\tilde{P}^*\) is a non-zero point of odd order on \(E_{\sigma(P)}^*(\mathbb{F}_p)\) is a purely \(\mathbb{F}_p\) property and thus is also preserved as \(E_{t_{n,m}} \cong E_t\) over \(\mathbb{F}_p\).

In the above argument we chose \(m\) and \(n\) in such a way that we “move around” the surface over \(\mathbb{Q}\) to achieve our desired real topological properties; however, nothing happens at all in the mod \(p\) picture. We will continue to look at how properties of fibers over \(\mathbb{Q}\), over \(\mathbb{R}\), and over \(\mathbb{F}_p\) will interact and, in certain cases, “mix well.”

The condition that there exist \(\tilde{P} \in E_t(\mathbb{F}_p)\) such that \(\tilde{P}^*\) is a non-zero point of odd order on \(E_{\sigma(P)}^*(\mathbb{F}_p)\) is somewhat clunky, and one might prefer to ask whether the property of being a candidate lift is (by itself) diffusive.

However, without this assumption, we could have a scenario where \((nP)^*\) is on the non-identity component of a cross-fiber \(E^*_s\) with two components, \((nP)^*\) has even order over \(\mathbb{F}_p\), \(rk(E^*_s) = 1\), and \(E^*_s(\mathbb{Q}) = <(nP)^*>\). Then every point that is in the same class as \((nP)^*\) must be an even multiple of it, and hence all of these points are on the non-identity component. Namely, there are classes in \(E^*_s(\mathbb{F}_p)\) that lift only to one of the two components, representing a failure for \(\mathbb{F}_p\) and \(\mathbb{R}\) properties to mix well. We might reasonably hope that some other multiple of \((nP)^*\) transforms onto a lift of the starting fiber, but this would be more subtle. We will consider certain cases where such behavior occurs in the next section.

Note that situation shows us that the addition of a condition can make it either easier for a property to be diffusive.

Proposition 4.3.1 has the following interesting corollary, which we saw stated slightly differently in the Introduction as Corollary 1.3.7:

**Corollary 4.3.2.** Let \(\tilde{E}\) be an elliptic curve over a finite field \(\mathbb{F}_p\) (with \(p > 23\)) such that \#\(\tilde{E}(\mathbb{F}_p)\) is prime. Suppose there exists a cross-fibered surface \(E\) for which

- \(R2MC\) does not hold for \(E\) in the main fibration \(\{E_t\}\)
- the number of fibers \(E_t\) which are candidate lifts and on which \(\exists\) a non-zero point \(\tilde{P} \in E_t(\mathbb{F}_p)\) such that \(\tilde{P}^*\) is a non-zero point of odd order on \(E_{\sigma(\tilde{P})}^*(\mathbb{F}_p)\) exceeds the sum of the bounds of Propositions 4.1.9 and 4.1.10.
Then there exists a lift satisfying the requirements of Problem 1.1.9.

Suppose we could find a surface where we knew R2MC was not true, i.e. such that there exists an interval $I \subset \mathbb{R}$ for which all $E_t$ for $t \in I$ had rank zero or one, and we were given enough fibers with the diffusive property of Proposition 4.3.1 for that property to be dense. Then, there would have to be a fiber $E_t$ with the property of Proposition 4.3.1 such that $t \in I$. This fiber would satisfy all the properties of Conjecture 1.1.10. Thus, Corollary 4.3.2 tells us that any cross-fibered surface on which there are infinitely many fibers with the diffusive property of Proposition 4.3.1 must either satisfy the R2MC or it can be used as a tool to solve instances of the R1LH.

Furthermore, the proof of Proposition 4.3.1 is algorithmic in nature. See Algorithm 4.

```
function FIND_CAND_LIFT_IN_I_SLOW($\mathcal{E}, E_{t_0}, P, \mathbb{F}_p, I$) = $(E_{t_{output}}, W)$

$(x, y) \leftarrow P$
$l \leftarrow \text{ord}_{E_{t_0}(\mathbb{F}_p)}(P)$
$s \leftarrow \sigma(x, y, t)$
$r \leftarrow \text{ord}_{E^*_z(\mathbb{F}_p)(P^*)}$
$N \leftarrow N_0(\mathcal{E}, E_{t_0}, P, \mathbb{F}_p, 1, 1, 1, r, z)$ by Algorithm 2
$t_{output} \leftarrow t_0$
$W \leftarrow P$

while $t_{output} \notin I$ do
    $k_1 \leftarrow \text{random integer in } [1, \frac{N-1}{l}]$
    $k_2 \leftarrow \text{random integer in } [1, \frac{N-1}{r}]$
    $n \leftarrow 1 + lk_1$
    $m \leftarrow 1 + rk_2$
    $(x_n, y_n) \leftarrow nP$
    $(u_{n,m}, v_{n,m}) \leftarrow m(nP)^*$
    $t_{output} = \tau(u_{n,m}, v_{n,m}, \sigma(x_n, y_n, t_0))$
    $W \leftarrow (m(nP)^*)^*$
end while

return $E_{t_{output}}$ and $W$
end function
```

Algorithm 4: Algorithm to find candidate lift in a fixed interval $I$ given a candidate lift a priori outside $I$ corresponding to Proposition 4.3.1 and Corollary 4.3.2

For $z$ and $N_0(P, I, z)$ computed by Algorithm 2, Algorithm 4 takes, on average, $\frac{1}{z}$ applications of the while loop. We compute the largest possible height of $W$ that this process uses:

$$\hat{h}(W) = \hat{h}((m(nP)^*)^*)$$
$$\leq \text{poly} \left(N_0(\mathcal{E}, E_t, P, I, 1, \text{ord}_{E_{t_0}(\mathbb{F}_p)}(P), 1, \text{ord}_{E^*_z(\mathbb{F}_p)(P^*)}, z), \hat{h}(P), ht(t)\right).$$
This computation is similar to our analysis of the running time of Algorithm 3 in the preceding section. Again, the polynomial here depends only on the coefficient polynomials that define \( E \). Thus, the average running time of this procedure is bounded by

\[
\frac{1}{z} \poly \left( N_0 \left( E, E_t, P, I, 1, \text{ord}_{E_{t_0}(F_p)}(P), 1, \text{ord}_{E^*_t(F_p)}(P^*), z \right), \hat{h}(P), ht(t) \right).
\]

If we can access \( m_{E_t}(I) \) and \( N \left( E, E_t, P, I, 1, \text{ord}_{E_{t_0}(F_p)}(P), 1, \text{ord}_{E^*_t(F_p)}(P^*), \frac{m_{E_t}(I)}{2} \right) \), then we have the bound:

\[
\frac{1}{m_{E_t}(I)} \poly \left( N \left( E, E_t, P, I, 1, \text{ord}_{E_{t_0}(F_p)}(P), 1, \text{ord}_{E^*_t(F_p)}(P^*), \frac{m_{E_t}(I)}{2} \right), \hat{h}(P), ht(t) \right).
\]

One might ask how \( N \left( E, E_t, P, I, 1, \text{ord}_{E_{t_0}(F_p)}(P), 1, \text{ord}_{E^*_t(F_p)}(P^*), \frac{m_{E_t}(I)}{2} \right) \) compares to \( N \left( E, E_t, P, I, 1, 1, 1, 1, \frac{m_{E_t}(I)}{2} \right) \) and hence how the running time of Algorithm 4 compares to that of Algorithm 3. Finding an explicit relationship between these quantities seems subtle because they depend on the rate of convergence of the limit in the Ergodic Theorem for irrational circle rotations that we considered in equation (4.5) in Section 4.2. As we commented above, this depends on how well the irrational number inducing the rotation can be approximated by rationals. In Proposition 4.2.8 we applied equation (4.5) twice: once corresponding to multiplication of the point \( P \) on \( E_t^0 \) and once corresponding to the multiplication of \( (nP)^* \) on its cross-fiber for each \( n \leq N \). By choosing \( n \) in different arithmetic progressions in our two algorithms, the \( (nP)^* \)'s will be different points on different curves which correspond to different irrational rotations, and it is not clear that their rates of convergence will be well related.

However, as \( p \) grows, we do not particularly expect the number of terms we need to take in equation (4.5) to grow. Some choices of \( p \) will lead to slower convergences than others, but the size of \( p \) does not seem to play a role. The number of terms in our two applications of equation (4.5) correspond to \( N/2b_1 \) and \( M/2b_2 \), where we want to choose \( N \) and \( M \) sufficiently large such that

\[
\left| \frac{\# \left\{ (n, m) : n \equiv a_1 \mod b_1, m \equiv a_2 \mod b_2, n \leq N, m \leq M, n, m \text{ even}, \tau(m(nP)^*) \in I \right\} - m_{E_t}(I)}{(N/2b_1)(M/2b_2)} \right| < \frac{1}{2}.
\]

Then, heuristically, for most inputs of \( E, E_t, P, \) and \( I \), we expect that the \( N \) and \( M \) we
need to take will roughly scale with $b_1$ and $b_2$ respectively. In Algorithm 4, our $n$ and $m$ are being drawn from the arithmetic progressions $1 + k_1 \text{ord}_{E_t(F_p)}(P)$ and $1 + k_2 \text{ord}_{E^*_t(F_p)}(P^*)$ whose constant differences $\text{ord}_{E_t(F_p)}(P)$ and $\text{ord}_{E^*_t(F_p)}(P^*)$ are $O(p)$; thus, we expect

$$N \left( E, E_t, P, I, 1, \text{ord}_{E_0(F_p)}(P), 1, \text{ord}_{E^*_0(F_p)}(P^*), \frac{1}{2} \right) \approx O \left( pN \left( E, E_t, P, I, 1, 1, 1, 1, \frac{1}{2} \right) \right).$$

Similarly, we heuristically expect

$$N_0 \left( E, E_t, P, I, 1, \text{ord}_{E_0(F_p)}(P), 1, \text{ord}_{E^*_0(F_p)}(P^*), z \right) \approx O \left( pN_0 \left( E, E_t, P, I, 1, 1, 1, 1, z \right) \right).$$

Suppose we had an example of a cross-fibered surface $\mathcal{E}$ that did not satisfy R2MC and we wanted to use it as a tool in Algorithm 4 to solve instances of the R1LH, as we remarked after Corollary 4.3.2 (where the instances of the R1LH accessible by this tool would be those where the elliptic curve $\tilde{E}$ occur as a mod $p$ reduction of some fiber of $\mathcal{E}$). Then, we saw the average running time of Algorithm 4 is bounded by

$$\frac{1}{z} \text{poly} \left( N_0 \left( E, E_t, P, I, 1, \text{ord}_{E_0(F_p)}(P), 1, \text{ord}_{E^*_0(F_p)}(P^*), z \right), \hat{h}(P), ht(t) \right),$$

and by our heuristic this should be roughly

$$\frac{1}{z} \text{poly} \left( pN_0 \left( E, E_t, P, I, 1, 1, 1, 1, z \right), \hat{h}(P), ht(t) \right).$$

Then, we think of $N_0 (E, E_t, P, I, 1, 1, 1, 1, z), \text{poly}, z, \hat{h}(P),$ and $ht(t)$ as corresponding to the effect on the running time of the $\mathcal{E}$, the starting fiber $E_t$, the starting point $P$, and $I$, and $p$ as corresponding to the effect on the running time of the instance of the R1LH that we chose. Thus, if our heuristic reasoning above is correct, Algorithm 4 should have an exponential running time in $\ln p$. As $p$ corresponds to the notion of size coming from the ECDLP, this is obviously too slow to have cryptographic applications.

However, one might think that we chose $n$ and $m$ unnecessarily large in order to guarantee that nothing happens in the mod $p$ picture during this process. Thus, we might ask if there is a better way to chose $n$ and $m$, and specifically, if we can find an appropriate candidate lift in reasonable time just by choosing random $n$ and $m$. We present such a procedure in Algorithm 5.

Note that, in Algorithm 5, in order to make the test for the while loop run quickly, we can replace the condition $E_{t_{\text{output}}} \neq E_{t_0}$ over $\mathbb{F}_p$ with $t_{\text{output}} \neq t_0 \text{ mod } p$ at the expense of possibly missing an acceptable lift.
function FIND_CAND_LIFT_IN_I_RAND(\(\mathcal{E}, E_{t_0}, P, \mathbb{F}_p, I\)) = \( (E_{\text{output}}, W) \)

\[
(x, y) \leftarrow P
\]
\[
s \leftarrow \sigma(x, y, t_0)
\]
\[
N \leftarrow N_0 (\mathcal{E}, E_{t_0}, P, 1, 1, 1, 1, z) \text{ by Algorithm 2}
\]
\[
t_{\text{output}} \leftarrow t_0
\]
\[
W \leftarrow P
\]
\[
\text{while } t_{\text{output}} \notin I \text{ or } E_{t_{\text{output}}} \not\cong E_{t_0} \text{ over } \mathbb{F}_p \text{ or } W \text{ has trivial reduction mod } p \text{ do}
\]
\[
n \leftarrow \text{random even integer in } [1, N]
\]
\[
m \leftarrow \text{random even integer in } [1, N]
\]
\[
(x_n, y_n) \leftarrow nP
\]
\[
(u_{n,m}, v_{n,m}) \leftarrow m(nP)^*
\]
\[
t_{\text{output}} = \tau(u_{n,m}, v_{n,m}, \sigma(x_n, y_n, t_0))
\]
\[
W \leftarrow (m(nP)^*)^*
\]
\[
\text{end while}
\]
\[
\text{return } E_{t_{\text{output}}} \text{ and } W
\]
end function

Algorithm 5: Proposed Algorithm to find candidate lift in a fixed interval \(I\) given a candidate lift a priori outside \(I\) by choosing random \(n\) and \(m\)

As Algorithm 5 is the same as Algorithm 3 with extra conditions on the while loop, we have already computed a bound on the largest possible height of \(W\) that this process uses:

\[
\hat{h}(W) \leq \text{poly}(N_0(P, I, z), \hat{h}(P), ht(t)),
\]

where the polynomial only depends on \(\mathcal{E}\). Then the maximum size of the intermediate values we are doing computations with is bounded by \(\text{poly}(\ln p, N_0(P, I, z), \hat{h}(P))\).

Every \(\frac{4}{7}\) attempts at the while loop, we expect to find \(t_{\text{output}} \in I\). However, for a general surface, we would roughly expect to have \(t_{\text{output}} \equiv t_0 \mod p\) only once in every \(p\) attempts. Thus, for such surfaces, Algorithm 5 is again a (randomize) exponential algorithm in \(\ln p\). Accordingly, we will mostly consider what happens when we perform Algorithm 5 on surfaces with an unusually low number of distinct fibers (and hence an elevated probability that any two fibers be isomorphic) \(\mod p\). For example, we will consider isotrivial surfaces on which there are only a small number of non-isomorphic fibers \(\mod \mathbb{F}_p\). In doing this, we will have to consider the degree to which the two conditions \(t_{\text{output}} \in I\) or \(E_{t_{\text{output}}} \cong E_{t_0} \text{ over } \mathbb{F}_p\) are independent, namely whether properties that belong to different perspectives of the surface (over \(\mathbb{R}\) and over \(\mathbb{F}_p\)) mix well. This will be further examined in Section 4.4.

Remark 4.3.3. While we do not know of any examples of surfaces for which R2MC is not true, considering the work of [30] showing that root number is not diffusive, it is perhaps
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

not implausible that such surfaces could exist.

Remark 4.3.4. Note that Algorithm 5 will run quickly (at least relative to the size of \( p \)) on any cross-fibered surface whose fibers are all isomorphic over \( \mathbb{F}_p \), e.g. a surface of the form (4.2)

\[
E_t : y^2 = x^3 + (a + pC_1(t))x + (b + pC_2(t))
\]

where \( C_1 \) and \( C_2 \) are cubics.

Somewhat less evidently, this is also the case for any surface of the form (4.3)

\[
E_t : y^2 = x^3 + bC(t)^2
\]

for \( p \equiv 2 \mod 3 \). In this case, by cubic reciprocity, \( C(t) \) is a cube mod \( p \) for any value of \( t \), so every fiber is isomorphic to \( E_t : y^2 = x^3 + b \).

In these cases, the expected number of attempts at the while loop necessary is \( \frac{4}{z} \); hence, Algorithm 5 is a randomized algorithm with average running time bounded by

\[
\frac{1}{z} \text{poly} (\ln p, N_0(P,I,z), \hat{h}(P)).
\]

If one has access to \( m_{E_t}(I) \) and \( N(P,I,m_{E_t}(I)/2) \), then the average running time is bounded by

\[
\frac{1}{m_{E_t}(I)} \text{poly} (\ln p, N(P,I,m_{E_t}(I)/2), \hat{h}(P)).
\]

4.4 Special cases where candidate lifts diffuse quickly

Most of this section will be dedicated to proving Theorem 1.3.8. First, we state a slightly more precise version of this theorem in which we make the choice of \( N_0 \) more explicit.

Theorem 4.4.1. Let \( \tilde{E} \) be an elliptic curve over a finite field \( \mathbb{F}_p \) (\( p > 23 \)). Let \( \{E_t\} \) be the main fibration of a cross-fibered elliptic surface \( \mathcal{E} \) which has non-trivial reduction (as a cross-fibered surface) mod \( p \). Further, assume that \( \{E_t\} \) has constant \( j \)-invariant mod \( p \) (and that \( j \not\equiv 1728 \mod p \) if \( p \equiv 1 \mod 4 \)).

Assume that there exists a rational curve \( C \) on \( \mathcal{E} \) over \( \mathbb{Q} \); \( \Psi : \mathbb{P}^1(\mathbb{Q}) \rightarrow C \). For \( k \in \mathbb{P}^1(\mathbb{Q}) \) at which \( \Psi \) is defined, we denote by \( P(k) \) the point on \( C \) that is the image of \( k \) under \( \Psi \). Suppose that

- the degree of \( C \) is such that \( p > 112 \deg(C)L(\mathcal{E})^36^{142L(\mathcal{E})} \)
- \( C \) contains at least one non-torsion point (on some non-singular fiber)
• $C$ contains at least one point of order greater than $r \mod p$ on its fiber

• for each $n$ and $m$, the rational curve $(m(nC)^*)^*$ contains points on exactly $\rho$ many non-isomorphic fibers over $\mathbb{F}_p$, and one of these fibers is isomorphic to $\tilde{E}$ over $\mathbb{F}_p$.

Let $I \subset \mathbb{R}$ be an interval and let $\epsilon > 0$. Let $k_0 \in \mathbb{Q}$ avoiding at most

$$\deg(C) \left(17832L(\mathcal{E})^3 + 14830L(\mathcal{E})^2 + 5922L(\mathcal{E}) + 1481\right)$$

exceptions. Then there exists an $\epsilon_1 > 0$ depending only on $E, C, k_0, I$, and $\epsilon$ such that for $N, M \geq \max \{N(P(k_0), (1 - \epsilon_1)I, \epsilon), N(P(k_0), (1 + \epsilon_1)I, \epsilon)\}$ there exists an open set $U(k_0, N, M)$ (which depends on $N$ and $M$) around $k_0$ such that

$$\left| \text{Prob}_{n,m,k} \left( \begin{array}{l}
(m(nP(k))^*)^* \text{ is on a fiber} \\
E_{t_{n,m}(k)}, \text{ which is a candidate} \\
lift and \ t_{n,m}(k) \in I
\end{array} \middle| \begin{array}{l}
n \leq N \text{ and } m \leq M \\
\text{are even and} \\
k \in U(k_0, N, M)
\end{array} \right) - \frac{m_{E_1(k_0)}(I)}{\rho} \right|$$

$$< \frac{2\epsilon}{\rho} + C(\rho) \left( \frac{m_{E_1(k_0)}(I) + 2\epsilon}{p} \right)$$

$$+ 10^6 L(\mathcal{E})^3 \max \left\{ \frac{1}{N^{1/4}}, \frac{1}{M^{1/4}}, \frac{1}{r^{1/4}}, \left( \frac{\deg(C)}{p} \right)^{1/16}, \left( \ln \left( \frac{1}{112\deg(C)L(\mathcal{E})^{6142L(\mathcal{E})}} \right) \right)^{1/4} \right\},$$

where

$$C(\rho) = \begin{cases} 10^5 \deg(C) L(\mathcal{E})^5 (2\sqrt{2} + 3)^{N+M} \sqrt{p} & \text{if } \rho = 1, 2, \text{ or } 3 \\
\frac{p}{12} + 10^5 \deg(C) L(\mathcal{E})^5 (2\sqrt{2} + 3)^{N+M} \sqrt{p} & \text{if } \rho = 6 \end{cases}$$

(Note, under these assumptions, these are the only possible values of $\rho$ for which the error bound is non-trivial.)

Thus, we see that the $N_0$ in the statement of Theorem 1.3.8 is in fact of the form

$$\max \{N(P(k_0), (1 - \epsilon_1)I, \epsilon), N(P(k_0), (1 + \epsilon_1)I, \epsilon)\}$$

for some $\epsilon_1 > 0$. We will see below how this $\epsilon_1$ is chosen.
4.4.1 A rational curve on a cross-fibered surface

A key assumption of Theorem 4.4.1 is that our $E$ contains a rational curve $C$ over $\mathbb{Q}$. As $C$ is rational, there is some birational map

$$\Psi : \mathbb{P}^1 \rightarrow C.$$ 

As in the statement of Theorem 4.4.1 for $k \in \mathbb{P}^1(\mathbb{Q})$ (that is not in the Zariski closed subset, namely the finitely many points of $\mathbb{P}^1$, at which $\Psi$ is undefined), we denote by $P(k)$ the point on $C$ that is the image of $k$ under $\Psi$. Then, writing the rational points of $C$ in terms of the rational functions that define the curve (in a fixed affine open subset of $E$), we have:

$$C(\mathbb{Q}) = \{P(k) = (x(k), y(k)) \in E_{t(k)} : k \in \mathbb{Q}\}.$$

Note that in [42], examples of explicit rational curves are constructed on several of the kinds of surfaces that we saw to be cross-fibered in Section 4.1.2. We will make use of some of these in Section 4.4.5 to find examples to which Theorem 4.4.1 applies.

In the statement of the theorem, we assume that such a curve exists over $\mathbb{Q}$; from context, it will be clear whether we are considering these functions over $\mathbb{Q}$ or over some reduction mod $p$.

We will find candidate lift fibers by seeing which fiber $(m(nP(k))^*)^*$ lies on for well-chosen $k$, $n$, and $m$. As we noted in the Introduction (and will see in more detail below), $nC$, $(nC)^*$, $m(nC)^*$, and $(m(nC)^*)^*$ are also rational curves in $E$. We write

$$nP(k) = (x_n(k), y_n(k)) \in E_{t(k)};$$

$$(nP(k))^* = (u_n(k), v_n(k)) \in E^*_{t_n(k)};$$

$$m(nP(k))^* = (u_{n,m}(k), v_{n,m}(k)) \in E^*_{t_{n,m}(k)};$$

and

$$(m(nP(k))^*)^* = (x_{n,m}(k), y_{n,m}(k)) \in E_{t_{n,m}(k)};$$

which sets notation for the coordinate rational functions of each of our rational curves (again in some fixed affine open subset of $E$).

4.4.2 A polynomial test to determine if $E_t$ is a lift of $\tilde{E}$

As we saw in the preceding section, in order for Algorithm 5 to run quickly, the surface $E$ should have an unusually low number of distinct fibers mod $p$. In this section, we
consider a modified version of this algorithm on surfaces such that the main fibration:

\[ E_t : y^2 = x^3 + a(t)x + b(t) \]

has constant \( j \)-invariant \( j \mod p \).

Then if we fix a curve of \( j \)-invariant \( j \in \mathbb{F}_p \):

\[ \tilde{E} : y^2 = x^3 + \tilde{a}x + \tilde{b}, \]

we define:

\[ d(t) = \frac{a(t)\tilde{b}}{b(t)\tilde{a}} \text{ if } j \neq 0, 1728, \quad d(t) = \frac{a(t)}{\tilde{a}} \text{ if } j \equiv 1728, \quad \text{and } d(t) = \frac{b(t)}{\tilde{b}} \text{ if } j \equiv 0. \]

Lemma 4.4.2. Suppose \( \{E_t\}, \tilde{E}, \text{ and } d(t) \) are as above and \( p \geq 5 \). If \( j \) is not 0 or 1728 mod \( p \), then \( E_t \) is isomorphic to \( \tilde{E} \) over \( \mathbb{F}_p \) if and only if \( d(t) \) is a quadratic residue mod \( p \). If \( j \equiv 1728 \mod p \), then \( E_t \) is isomorphic to \( \tilde{E} \) over \( \mathbb{F}_p \) if and only if \( d(t) \) is a quartic residue mod \( p \). If \( j \equiv 0 \mod p \), then \( E_t \) is isomorphic to \( \tilde{E} \) over \( \mathbb{F}_p \) if and only if \( d(t) \) is a sextic residue mod \( p \).

Proof. See \([41]\). \( \square \)

On such surfaces there are only a few non-isomorphic fibers over \( \mathbb{F}_p \). Particularly, for \( j \not\equiv 0, 1728 \mod p \), there are at most two non-isomorphic fibers on a surface of constant \( j \)-invariant \( j \), depending on whether \( d(t) \) takes a quadratic residue or quadratic non-residue value (of course, these curves are isomorphic over \( \mathbb{F}_p \)). Hence, in our situation, where the output fiber of our algorithm is going to be of the form

\[ t_{\text{out}} = t_{n,m}(k); \]

namely, a rational function in some underlying variable \( k \) chosen as an input, \( E_{t_{\text{out}}} \) being a lift is equivalent to some rational function taking a quadratic (or quartic or sextic) residue value at a \( k \). As clearing the denominator of this rational function by multiplying by a square does not affect whether a given value is a quadratic residue, we can use Weil’s bound on character sums (Theorem 3.1.3) to control the number of values of a polynomial that are such residues and hence control the number of input \( k \)'s that result in lifts.
We now develop the tools necessary to further analyse $t_{out}$. As we arrive at our output fiber via the map $P \mapsto (m(nP)^*)^*$, and as this map is built out of the multiplication by $n$ map (as well as the conversions from one fibration to the other), it is useful to have an explicit formula for the effect of multiplication on the coordinates of a point.

**Lemma 4.4.3.** Suppose $(x_P,y_P)$ is a point on an elliptic curve $y^2 = x^3 + Ax + B$. We write

$$(x_i,y_Pu_i) = [i](x_P,y_P)$$

and suppose that $x_P$ is not a 2-torsion point. Then, we can find $l_i$ such that $x_i$ is a rational function in $x$, $A$, and $B$ of the form

$$\frac{\text{polynomial of degree } l_i + 1}{\text{polynomial of degree } l_i}$$

whose value at $x = 1$, $A = 0$, $B = 0$ is $\frac{1}{l_i}$.

Furthermore, we can find $r_i$ such that $u_i - 1$ is a rational function of the form

$$\frac{\text{polynomial of degree } r_i}{\text{polynomial of degree } r_i}$$

whose value at $x = 1$, $A = 0$, $B = 0$ is $\frac{1 - i^3}{i^3}$.

Here the relevant polynomials are homogeneous in $x$, $A$, and $B$ where (as before) $x$, $A$, and $B$ are weighted with multiplicity 1, 2, and 3 respectively, and for $i \geq 4$:

$$r_i \leq \left(1 + \frac{3}{2\sqrt{2} + 2}\right)(2\sqrt{2} + 3)^i - 1 \quad \text{and} \quad l_i \leq \frac{\sqrt{2}}{2}\left(1 + \frac{3}{2\sqrt{2} + 2}\right)(2\sqrt{2} + 3)^i - 1$$

Denoting the largest coefficient in $x_i$ (in either the numerator or the denominator when writing $x_i$ with integer coefficients in lowest terms) by $c_i$ and the largest coefficient of $u_i - 1$ by $d_i$, we have

$$c_i, d_i \leq 486(486 \cdot 18)^{7i - 2}$$

For the details of this see Appendix A. Note that we use tools drawn from [14].

Thus, we see:

**Proposition 4.4.4.** $x_n(k)$, $y_n(k)$, $u_n(k)$, $v_n(k)$, $s_n(k)$, $u_{n,m}(k)$, $v_{n,m}(k)$, $t_{n,m}(k)$, and $d_{n,m}(k) = d(t_{n,m}(k))$ are all rational functions in $k$.

**Proof.** Lemma 4.4.3 shows that the $x$-coordinate of the multiple of a point is a rational function in the $x$-coordinate of that point and in the coefficients of the curve over which
one works. Further, it shows that the $y$-coordinate of the multiple of a point is a rational function in the $x$-coordinate of that point and in the coefficients of the curve over which one works, multiplied by the $y$-coordinate of the point. As the transformation maps of the cross-fibration are, by assumption, rational functions and as $d_{n,m}$ is a rational function in $t_{n,m}$, these functions are all (compositions of) rational functions in $x(k)$, $y(k)$, and $t(k)$ and hence rational functions in $k$.

Recall in, Section 4.1, we defined $L(E)$, which was a measure of the size of a (pre)-cross-fibration in terms of the degrees of the polynomials that give the conversions. Similarly, the “size” of the rational curve $C$ is measured by $\text{deg}(C)$ as

$$\max \{\text{deg}_k(x), \text{deg}_k(y), \text{deg}_k(t)\} \leq \text{deg}(C).$$

Then, we can calculate how large the result of the process

$$P(k) \mapsto n(P(k)) \mapsto (nP(k))^* \mapsto m(nP(k))^* \mapsto (m(nP(k))^*)^*$$

is in terms of these measures.

**Proposition 4.4.5.**

- $\text{deg}_k x_n(k) \leq \text{deg}(C)(2L(E) + 1)(l_n + 1)$
- $\text{deg}_k y_n(k) \leq \text{deg}(C)((2L(E) + 1)r_n + 1)$
- $\text{deg}_k u_n(k) \leq \text{deg}(C)L(E) [(2L(E) + 1)(l_n + r_n + 1) + 2]$
- $\text{deg}_k v_n(k) \leq \text{deg}(C)L(E) [(2L(E) + 1)(l_n + r_n + 1) + 2]$
- $\text{deg}_k s_n(k) \leq \text{deg}(C)L(E) [(2L(E) + 1)(l_n + r_n + 1) + 2]$
- $\text{deg}_k u_{n,m}(k) \leq \text{deg}(C)\text{deg}_k L(E) (2L(E) + 1) [(2L(E) + 1)(l_n + r_n + 1) + 2] (l_m + 1)$
- $\text{deg}_k v_{n,m}(k) \leq \text{deg}(C)\text{deg}_k L(E) [(2L(E) + 1)(l_n + r_n + 1) + 2] (2L(E) + 1)r_m + 1$)
- $\text{deg}_k t_{n,m}(k) \leq \text{deg}(C)\text{deg}_k L(E)^2 [(2L(E) + 1)(l_n + r_n + 1) + 2] [(2L(E) + 1)(l_m + r_m + 1) + 2]$
- $\text{deg}_k d_{n,m}(k) \leq 5\text{deg}(C)\text{deg}_k L(E)^2 [(2L(E) + 1)(l_n + r_n + 1) + 2] [(2L(E) + 1)(l_m + r_m + 1) + 2]$
Proof. We compute up to \( \deg_k u_n(k) \). The rest is similar. As we saw in Lemma 4.4.3, \( x_n \) is of the form
\[
\begin{align*}
\text{polynomial of degree } l_n + 1 \\
\text{polynomial of degree } l_n
\end{align*}
\]
where the polynomials are homogeneous in \( x = x(k), A = a(t(k)) \), and \( B = b(t(k)) \) (with weights 1, 2, and 3 respectively); namely, \( \deg_x x_n \leq l_n + 1 \), \( \deg_a x_n \leq \frac{l_n + 1}{2} \), and \( \deg_b x_n \leq \frac{l_n + 1}{3} \). So,
\[
\deg_k x_n \leq (l_n + 1) \deg_k x + \frac{l_n + 1}{2} \deg_t a \cdot \deg_k t + \frac{l_n + 1}{3} \deg_t b \cdot \deg_k t
\]
\[
\leq \deg(C)(2L(\mathcal{E}) + 1)(l_n + 1).
\]
Similarly, \( y_n \) is of the form
\[
\begin{align*}
y(k) \text{ polynomial of degree } r_n \\
\text{polynomial of degree } r_n
\end{align*}
\]
So,
\[
\deg_k y_n \leq \deg_k y + r_n \deg_k x + \frac{r_n}{2} \deg_t a \cdot \deg_k t + \frac{r_n}{3} \deg_t b \cdot \deg_k t
\]
\[
\leq \deg(C) + \deg(C)(2L(\mathcal{E}) + 1)r_n.
\]
Then, \( u_n(k) \) is a rational function in \( x_n(k), y_n(k), \) and \( t(k) \), so
\[
\deg_k u_n(k) \leq \deg_x v \cdot \deg_k x_n + \deg_y v \cdot \deg_k y_n + \deg_t v \cdot \deg_k t
\]
\[
\leq L(\mathcal{E})(\deg(C)(2L(\mathcal{E}) + 1)(l_n + 1) + \deg(C)(r_n(2L(\mathcal{E}) + 1) + 1) + \deg(C))
\]
\[
\leq \deg(C)L(\mathcal{E})[(2L(\mathcal{E}) + 1)(l_n + r_n + 1) + 2].
\]

Similarly, it will be useful to keep track of the largest coefficient that appears in each function as we go through this process. For a rational function \( f \) in \( k \) with integer coefficients written in lowest terms, we write \( \text{coeff}_k(f) \) to indicate its largest coefficient.

Define
\[
K(\mathcal{E}) = \max \left\{ \text{coeff}_x v, \text{coeff}_y v, \text{coeff}_z v, \text{coeff}_x v, \text{coeff}_y v, \text{coeff}_z v, \text{coeff}_x \sigma, \text{coeff}_y \sigma, \text{coeff}_z \sigma, \text{coeff}_u \xi, \text{coeff}_v \xi, \text{coeff}_s \xi, \right. \\
\left. \text{coeff}_u \iota, \text{coeff}_v \iota, \text{coeff}_s \iota, \text{coeff}_u \tau, \text{coeff}_v \tau, \text{coeff}_s \tau, \frac{\text{coeff}_a}{2}, \frac{\text{coeff}_b}{3}, \frac{\text{coeff}_c}{2}, \frac{\text{coeff}_d}{3} \right\}
\]
and similarly, again, for \( P(k) = (x(k), y(k)) \in E_t(k) \),
\[
\text{coeff}(C) = \max \{ \text{coeff}_k x, \text{coeff}_k y, \text{coeff}_k t \}. 
\]
Recalling the equivalent of Proposition \ref{prop:coeff_sum} for largest coefficients:

**Proposition 4.4.6.** Let $f$ and $g$ be rational functions.

- $\text{coeff}(f + g) \leq 2\text{coeff}(f) \cdot \text{coeff}(g) \cdot \min(\deg(f), \deg(g))$
- $\text{coeff}(fg) \leq \text{coeff}(f) \cdot \text{coeff}(g) \cdot \min(\deg(f), \deg(g))$
- Suppose $f$ is a rational function in $n$ variables and $g_1, \ldots, g_n$ are rational functions, then

$$\text{coeff}(f(g_1, \ldots, g_n)) \leq$$

$$2^n \text{coeff}(f) \cdot \max_i \left[ (\deg_{g_i}(f) \cdot \deg(g_i))^{n-1} \cdot (\deg_{g_i}(f) \cdot \text{coeff}(g_i))^{\deg_{g_i}(f)} \right].$$

Following an argument similar to that of Proposition \ref{prop:coeff_product}, one can show:

**Proposition 4.4.7.** Denote $T_i = \max\{l_i + 1, r_i\}$ and $S_i = \max\{c_i, d_i\}$. Then

$$\text{coeff}(t_{n,m}) \leq$$

$$3^{50L(\mathcal{E})^4 T_n T_m} L(\mathcal{E})^{38L(\mathcal{E})^3 T_n T_m} K(\mathcal{E})^{5L(\mathcal{E})^2 T_m} \deg(C)^{20L(\mathcal{E})^3 T_m}$$

$$\cdot \text{coeff}(C)^{6L(\mathcal{E})^4 T_n T_m} T_n^{108L(\mathcal{E})^2 T_m} T_m^{5L(\mathcal{E}) T_m} S_n^9 L(\mathcal{E})^3 T_n T_m S_m^L(\mathcal{E}).$$

### 4.4.3 Bounding the number of $k$, $n$, and $m$ with exceptional behaviors

We bound the number of points on such a curve that have certain exceptional properties.

**Lemma 4.4.8.** Let $\mathcal{E}$ be a cross-fibered elliptic surface on which there is a rational curve $C \subset \mathcal{E}$, on which there exists at least one point that is non-torsion (on some non-singular fiber of $\mathcal{E}$). Then, there are at most

$$\deg(C)(2L(\mathcal{E}) + 1) \sum_{m=2}^{16} (m^2 - 1) + \deg(C)$$

points $P(k)$ on $C$ that are torsion on their respective fibers.

**Proof.** For $m \geq 2$, the division polynomials we discussed in Section \ref{sec:division_polynomials} control whether $P(k)$ is $m$-torsion. We plug $x = x(k)$, $A = a(t(k))$, and $B = b(t(k))$ into their formulas;
as the degree of $\psi_m$ is at most $m^2 - 1$ in $x$, $\frac{m^2-1}{2}$ in $a$, and $\frac{m^2-1}{3}$ in $b$, by homogeneity, for each $m = 1, .., 16$, this results in a division polynomial $\psi_m(k)$ of degree at most:

$$(m^2 - 1) \deg_k x + \frac{m^2 - 1}{2} \deg_k a(t(k)) + \frac{m^2 - 1}{3} \deg_k b(t(k))$$

$$\leq (m^2 - 1) \deg(C) + \frac{m^2 - 1}{2} \deg_a t \cdot \deg_k t + \frac{m^2 - 1}{3} \deg_b t \cdot \deg_k t$$

$$\leq (m^2 - 1) \deg(C) + \frac{m^2 - 1}{2} 2L(E) \cdot \deg(C) + \frac{m^2 - 1}{3} 3L(E) \cdot \deg(C).$$

As there exists by assumption a point $P(k)$ that is non-torsion on its fiber, none of the $\psi_m(k)$ can be the zero polynomial. Note that $P(k)$ is itself the zero point only if the denominator of $x(k)$ is zero, hence for at most $\deg(C)$ values of $k$.

\begin{proof}

Lemma 4.4.9. Let $p$ be a prime. Let $E$ be a cross-fibered elliptic surface on which there is a rational curve $C \subset E$, on which there exists at least one point that is on a fiber of good reduction of $E \mod p$. Then, there are at most

$$12 \deg(C)L(E)$$

classes of $k$ such that $P(k)$ is on a fiber of bad reduction $mod\ p$.

\begin{proof}

The discriminant of $E_{t(k)}$:

$$\Delta(E_{t(k)}) = -16 \left(4a(t(k))^3 + 27b(t(k))^2\right)$$

is non-zero as a function of $k$ (over $\mathbb{F}_p$) by the assumption that there exist at least one point that is on a fiber of good reduction of $E \mod p$. Hence, the number of classes of $k$ that result in bad reduction $mod\ p$ is bounded by its degree, and

$$\deg(\Delta(E_{t(k)})) \leq 3 \deg_a t \cdot \deg_k t + 2 \deg_b t \cdot \deg_k t \leq 12 \deg(C)L(E).$$

\end{proof}

Lemma 4.4.10. Let $p$ be a prime and let $l \in \mathbb{N}$, $l \geq 2$. Let $E$ be a cross-fibered elliptic surface on which there is a rational curve $C \subset E$, on which there exists at least one point
that has order at least \( l \mod p \) on its fiber. Then, there are at most

\[
\text{deg}(C)(2L(\mathcal{E}) + 1) \sum_{m=2}^{l-1} (m^2 - 1) + \text{deg}(C)
\]

classes \( k \) in \( \mathbb{F}_p \) such that \( P(k) \) has order less than \( l \mod p \) on \( E_{t(k)} \).

**Proof.** This is essentially the same argument as that of Lemma 4.4.8. The point \( P(k) \) is itself zero mod \( p \) only if the denominator of \( x(k) \) is zero. As we have a point of order at least \( l \), this is not the zero polynomial, hence it can be zero for at most deg\((C)\) values of \( k \). Whereas the division polynomials over \( \mathbb{Q} \) control whether a point is torsion, looked at over \( \mathbb{F}_p \), they control the order of the point mod \( p \). We saw that for each \( m \geq 2 \), after we plug in \( x = x(k), A = a(t(k)), \) and \( B = b(t(k)) \), the \( m \)-division polynomial had degree in \( k \) at most

\[
\text{deg}(C)(2L(\mathcal{E}) + 1)(m^2 - 1).
\]

As there exists a point of order at least \( l \mod p \), none of these \( \psi_m(k) \) can be the zero polynomial (over \( \mathbb{F}_p \)).

\[\square\]

**Lemma 4.4.11.** Let \( p \) be a prime and let \( w \) and \( l \) be natural numbers that are both greater than 1. Let \( \mathcal{E} \) be a cross-fibered elliptic surface which has non-trivial reduction (as a cross-fibered surface) mod \( p \) on which there is a rational curve \( C \subset \mathcal{E} \) such that

- there exists at least one point that has order at least

\[
\max\left\{ l, \frac{w^2(w - 1)^2}{4} + 130L(\mathcal{E}) + 13 \right\}
\]

\( \mod p \) on its fiber (which has good reduction mod \( p \))

- \( C \) contains points on at least two distinct fibers over \( \mathbb{F}_p \).

Further, assume

\[
p > \text{deg}(C) \left( \frac{w^2(w - 1)^2}{4} + 1 \right) \left( L(\mathcal{E}) \left( \frac{w^2(w - 1)^2}{4} + 130L(\mathcal{E}) + 13 \right) + 117L(\mathcal{E}) \right)^3
\]

Then for all but
\[
\deg(C)(2L(E) + 1) \sum_{i=2}^{l-1} (i^2 - 1) + 72 \deg(C)L(E)^3 + 30 \deg(C)L(E)^2 + 14 \deg(C)L(E) + \deg(C) \\
+20 \deg(C)L(E)^3 \left( \frac{lw_2(w-1)^2}{4} + 130L(E) + 13 \right) \sum_{i=2}^{w-1} (i^2 - 1) \\
\]

many classes of \( k \mod p \) (where \( l_i \) and \( r_i \) are as in Lemma 4.4.3), \( P(k) \) is on a fiber of good reduction mod \( p \) and has order at least \( l \) on \( E_t(k) \), and there are at most

\[
6L(E)(2L(E) + 1) \sum_{i=1}^{w-1} (i^2 - 1) + 131L(E) + 10 
\]

many \( n \leq l \) such that

- \( P(k) \) is on a fiber of bad reduction mod \( p \)
- \( nP(k) \) is zero mod \( p \)
- \( (nP(k))^* \) is undefined or
- \( (nP(k))^* \) has order less than \( w \) mod \( p \) on \( E_{s_n(k)}^* \).

Furthermore, for \( k \) and \( n \) outside of the exclusions above, there are at most

\[
130L(E) + 13 
\]

many \( m \leq w \) such that

- \( m(nP(k))^* \) is zero mod \( p \)
- \( (m(nP(k))^*)^* \) is undefined or
- \( (m(nP(k))^*)^* \) zero on its fiber.

**Proof.** We begin by showing that under these assumptions the order of \( (nP(k))^* \mod p \) cannot be less than \( w \) for all choices of \( n \) and \( k \).

We note that as we have at least one point of order \( \frac{w^2(w-1)^2}{4} + 130L(E) + 13 \) on a fiber of good reduction, by Lemma 4.4.9 that there are at most \( 12 \deg(C)L(E) \) values of \( k \) at which \( E_{t(k)} \) has bad reduction mod \( p \). Furthermore, there are at most \( \deg(x(k)) \leq \deg(C) \) values of \( k \) at which \( P(k) \) is zero mod \( p \).
Note that as $E$ has non-trivial reduction as a cross-fibered surface mod $p$, none of $\Delta^*(x,y,t)$, $\text{den}(v(x,y,t))$, and $\text{den}(\sigma(x,y,t))$ are the zero function mod $p$. Hence by Propositions 4.1.9 and 4.1.10, there are at most

$$72L(E)^3 + 30L(E)^2 + 2L(E)$$

values of $t$ for which $\ast$ is undefined at all points on $E_t$, at which all points of $E_t$ are taken to points on fibers of bad reduction mod $p$ under $\ast$, or at which all points on $E_t$ are sent to zero under $\ast$. For any given $t_0$, the equation

$$t(k) = t_0$$

cannot hold for all $k$ because we have assumed that $C$ has points on multiple different fibers. Thus, this equation has at most $\deg(C)$ solutions; hence, there are at most

$$72 \deg(C)L(E)^3 + 30 \deg(C)L(E)^2 + 2\deg(C)L(E)$$

values of $k$ for which $t(k)$ has one of these degenerate properties. Again, by Propositions 4.1.9 and 4.1.10, for any other value of $k$, there are at most $130L(E) + 12$ many points on $E_{t(k)}$ that are sent to singular fibers, sent to zero, or on which $\ast$ is undefined.

We can plug in $p$ different values of $k$ into $P(k)$. We produce at least

$$p - \left( \deg(C)L(E) \sum_{i=1}^{w^2(w-1)^2+130L(E)+12} (i^2 - 1) + 117 \deg(C)L(E)^3 \right)$$

$$\geq p - \deg(C) \left( L(E) \left( \frac{w^2(w-1)^2}{4} + 130L(E) + 13 \right)^3 + 117L(E)^3 \right)$$

points $P(k)$ of order at least $\frac{w^2(w-1)^2}{4} + 130L(E) + 13$ on their respective fibers (and these fibers each have at least one point, $P(k)$, which is converted to a non-zero point on a fiber of good reduction under $\ast$). Hence, we produce at least

$$\left( p - \deg(C) \left( L(E) \left( \frac{w^2(w-1)^2}{4} + 130L(E) + 13 \right)^3 + 117L(E)^3 \right) \right) \left( \frac{w^2(w-1)^2}{4} + 130L(E) + 13 - (130L(E) + 12) \right)$$
distinct triples \((x, y, t)\) that are of the form \((x, y) = nP(k) \in E_t\) for some \(k\) and
\[
n \leq \frac{w^2(w-1)^2}{4} + 130L(\mathcal{E}) + 13
\]
and which are sent to a non-zero point on a good reduction fiber mod \(p\) under \(*\).

However, it is well known that the \(\mathbb{F}_p\) points of an elliptic curve have a group structure of the form \(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mj\mathbb{Z}\) for some \(m\) and \(j\). (See, for example, [13].) Thus, the number of small points any given cross-fiber has is limited. Specifically, the number of elements in \(\mathbb{Z}/N\) with order \(i\) is at most \(i\). Then the number of elements with order smaller than \(w\) is at most \(w-1\). Then, for a point in \(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mj\mathbb{Z}\) to have order less than \(w\) requires taking a pair both of whose coordinates have order less than \(w\) in its respective \(\mathbb{Z}/N\). So, there are at most \(w^2(w-1)^2/4\) points on any given \(E^*_s(\mathbb{F}_p)\) with order less than \(w\).

As there are \(p\) different values of \(s\), there are at most \(w^2(w-1)^2/4p\) distinct \((u, v, s)\) such that \((u, v)\) is a point of order less than \(w\) in \(E^*_s(\mathbb{F}_p)\). As the conversion between fibrations is bijective on the points where it is defined, there are then at most this many \((x, y, t)\) such that \((x, y)^*\) is a point of order less than \(w\). However, this is strictly less than the number of points we produced of the form \((x, y) = nP(k)\) by our assumptions on \(p\).

Now, fix some \(n_0 \leq \frac{w^2(w-1)^2}{4} + 130L(\mathcal{E}) + 13\) and \(k_0\) such that \((n_0P(k_0))^*\) has order at least \(w\). Whether \((n_0P(k))^*\) is zero or not for some \(k\) is determined by whether the denominator of \(u_{n_0}(k)\) is zero. There is at least one value of \(k\) such that this polynomial is non-zero \((k_0)\), so its number of zeros is bounded by its degree which, by Proposition 4.4.5 is at most
\[
\deg(C)L(\mathcal{E}) \left[(2L(\mathcal{E}) + 1) \left(l \frac{w^2(w-1)^2}{4} + 130L(\mathcal{E}) + 13 + r \frac{w^2(w-1)^2}{4} + 130L(\mathcal{E}) + 13 + 1\right) + 2\right].
\]

Then, for each \(i \leq w - 1\) and any \(k\) such that \((n_0P(k))^*\) is non-zero, the division polynomial:
\[
\psi^*_i(u_{n_0}(k), c(s_{n_0}(k)), d(s_{n_0}(k))
\]
that controls whether \((n_0P(k))^*\) has order \(i\) takes a non-zero value on \(k_0\), and hence is a non-zero polynomial of degree at most
\[
\deg_u \psi^*_i \cdot \deg_k u_{n_0} + \deg_c \psi^*_i \cdot \deg_k c \cdot \deg_k s_{n_0} + \deg_d \psi^*_i \cdot \deg_k d \cdot \deg_k s_{n_0}
\]
\[ \leq (i^2 - 1)(\deg_k u n_0 + 2L(E) \deg_k s n_0) \]
\[ \leq (i^2 - 1) \deg(C)L(E)(2L(E) + 1)(2L(E) + 1)(l n_0 + r n_0 + 1) + 2 \]
\[ \leq 15(i^2 - 1) \deg(C)L(E)^3 \left( l \frac{w^2(w-1)^2}{4} + 130L(E) + 13 + r \frac{w^2(w-1)^2}{4} + 130L(E) + 1 \right), \]
where we use Proposition 4.4.5 for the second inequality.

For any \( k \) (such that \( P(k) \) is a non-zero point on a fiber of good reduction mod \( p \) and \( E_{t(k)} \) does not have any of the degenerate properties of above with respect to \( * \)) at which these polynomials are non-zero and \( i \leq w - 1 \), there is at least one point (specifically \( n_0(P(k)) \)) on the curve \( E_{t(k)} \) that is not on the curve \( C_{i,k}^* : \psi^*_i(u(x,y,t(k)), c(\sigma(x,y,t(k))), d(\sigma(x,y,t(k)))) = 0 \)
whose degree is bounded by
\[ \deg_u \psi^*_i \cdot (\deg_x v + \deg_y v) + \deg_c \psi^*_i \cdot \deg_c c(\deg_x \sigma + \deg_y \sigma) + \deg_d \psi^*_i \cdot \deg_d d(\deg_x \sigma + \deg_y \sigma) \leq 2(i^2 - 1)L(E)(2L(E) + 1) \]
for \( i \geq 2 \), or on the curve \( C_{l,k}^* : \text{den}(v(x,y,t(k))) = 0 \),
which has degree at most \( \deg_x v + \deg_y y \leq 2L(E) \). So, \( E_{t(k)} \) is irreducible and does not share a component with any of the \( C_{i,k}^* \). Thus, by Bézout’s Theorem (using only the upper bound as \( C_{i,k}^* \) may have singularities or points of multiplicity), there are at most
\[ 6(i^2 - 1)L(E)(2L(E) + 1) \]
points on both \( E_{t(k)} \) and \( C_{i,k}^* \) for \( i \geq 2 \) and at most \( 6L(E) \) points on both \( E_{t(k)} \) and \( C_{1,k}^* \).

Further, again using Proposition 4.4.5, as we know by our choice of \( k \) that there is at least one point on \( E_{t(k)} \) on which \( * \) is defined and which is sent to a non-singular fiber, there are at most \( 125L(E) + 9 \) points on \( E_{t(k)} \) on which \( * \) is undefined or which are sent to singular fibers.

As we have a point on \( C \) with order at least \( l \) on a fiber of good reduction mod \( p \), we can use Lemmas 4.4.9 and 4.4.10 to guarantee that \( P(k) \) also has order at least \( l \) on a fiber of good reduction mod \( p \) (at the expense of excluding additional classes of \( k \) and noting that we have already excluded \( k \)'s such that \( P(k) \) is zero mod \( p \)). Hence, our bound on the number of points on \( E_{t(k)} \) at which \( * \) is undefined or that are also on some \( C_{i,k}^* \) for \( i < w \) converts into a bound on the number of \( n \leq l \) such that \( (nP(k))^* \) is
undefined or has order less than $w$ mod $p$ on $E^*_{s_n(k)}$. We also exclude the, at most, one additional $n \leq l$ at which $n(P(k))$ might be zero mod $p$.

For the final claim, note that there is a point on $E^*_{s_n(k)}$ (namely $(n(P(k)))^*$) which is sent by $*$ to a non-zero point on a fiber of good reduction mod $p$. So by Propositions 4.1.9 and 4.1.10, all but at most $130L(E) + 12$ points on $E^*_{s_n(k)}$ are sent to non-zero points on fibers of good reduction. As $(n(P(k)))^*$ has order $\geq w$, this translates into a bound on the number of $m \leq w$ such that $(m(n(P(k)))^*)$ is zero or undefined. Like above, we also exclude the, at most, one additional $m \leq w$ at which $m(n(P(k)))^*$ might be zero mod $p$.

### 4.4.4 Proof of Theorem 4.4.1

#### Proof of Theorem 4.4.1

Intuitively, based on Proposition 4.2.8, we expect that if we randomly choose $n$, $m$, and $k$, we have a probability of $m_{E_t(I)}$ that $t_{n,m}(k) \in I$, namely that $(m(n(P(k)))^*)$ be on a fiber in $I$. Similarly, we expect that we have a $\frac{1}{\rho}$ probability that $E_{t_{n,m}(k)}$ is a lift of $\tilde{E}$ (as by our assumptions about isotriviality, there are exactly $\rho$ non-isomorphic fibers over $\mathbb{F}_p$, which we might expect to occur with equal probability). Furthermore, the probabilities that $(m(n(P(k)))^*)$ reduces to zero mod $p$, that $(m(n(P(k)))^*)$ is torsion, or that one of the $*$'s used to compute $(m(n(P(k)))^*)$ is undefined should be quite small by Proposition 4.1.9, Proposition 4.1.10, and Lemma 4.4.11, which show that these phenomena only happen for a bounded number of exceptional $n$, $m$, and $k$. One then might hope that these properties are reasonably independent and that the probability that a given choice of $n$, $m$, and $k$ satisfy them all would be roughly $\frac{m_{E_t(I)}}{\rho}$. We will see that this is, in fact, the case.

**The $n$, $m$, and $k$ where $(m(n(P(k)))^*)$ reduces trivially or is torsion**

We begin by controlling the phenomena which we said to be exceptional and of small probability. Explicitly we will want to choose our $k$, $n$, and $m$ such that

- $P(k)$ is a non-torsion point
- $P(k)$ does not reduce to zero mod $p$
- $n(P(k))$ does not reduce to zero mod $p$
- $*$ is defined at $n(P(k))$ mod $p$
- $(n(P(k)))^*$ does not reduce to zero mod $p$
- $m(n(P(k)))^*$ does not reduce to zero mod $p$
• $\ast$ is defined at $m(n(P(k)))^\ast \mod p$

• $(m(n(P(k))))^\ast$ does not reduce to zero mod $p$

• $(m(n(P(k))))^\ast$ is a non-torsion point.

By assumption, $C$ contains at least one point of order at least $r$. Later, we will choose $l, w \in \mathbb{N}$ both greater than 1, such that

$$r \geq \max \left\{ l, \frac{w^2(w-1)^2}{4} + 130L(E) + 13 \right\}$$

and such that

$$p > \deg(C) \left( \frac{w^2(w-1)^2}{4} + 1 \right) \left( L(E) \left( \frac{w^2(w-1)^2}{4} + 130L(E) + 13 \right)^3 + 117L(E)^3 \right).$$

Note that $C$ satisfies the requirements of Lemma 4.4.11, as we have assumed that $C$ contains points on at least two distinct fibers over $\mathbb{F}_p$.

If we choose $k, n, \text{and } m$ avoiding the exceptions of Lemma 4.4.11, we have all the “mod $p$” properties listed above, namely all of the properties except $P(k)$ and $(m(n(P(k))))^\ast$ being non-torsion points. By Lemma 4.4.8, as we have assumed that there exists a non-torsion point on $C$, there are at most $\deg(C)(2L(E)+1) \sum_{i=2}^{16} (m^2 - 1) + \deg(C)$ values of $k$ (in $\mathbb{Q}$ so also in $\mathbb{F}_p$) such that $P(k)$ is torsion. Thus, the total number of classes of $k \mod p$ we must avoid is:

$$\# \text{ lost } k's = \deg(C)(2L(E) + 1) \left( \sum_{i=2}^{l-1} (i^2 - 1) + \sum_{m=2}^{16} (m^2 - 1) \right)$$

$$+ 20 \deg(C)L(E)^3 \left( l \frac{w^2(w-1)^2}{4} + 130L(E) + 13 + r \frac{w^2(w-1)^2}{4} + 130L(E) + 13 + 1 \right) \sum_{i=2}^{w-1} (i^2 - 1)$$

$$+ 72 \deg(C)L(E)^3 + 30 \deg(C)L(E)^2 + 14 \deg(C)L(E) + 2 \deg(C)$$

If $k$ is not one of the lost $k$’s, then as we choose $n \leq N$ and the order of $P(k)$ is at least $l$, we cycle through the various multiples of $P(k)$ at most $\left\lceil \frac{N}{l} \right\rceil$ times, hence the total number of $n$’s which are lost as exceptions to Lemma 4.4.11 is at most:

$$\# \text{ lost } n's = \left\lceil \frac{N}{l} \right\rceil \left( 6L(E)(2L(E) + 1) \sum_{i=1}^{w-1} (i^2 - 1) + 131L(E) + 10 \right).$$
Similarly, for \( k \) and \( n \) other than the exceptions, as we choose \( m \leq M \) and the order of \((n(P(k)))^*\) is at least \( w \), the total number of \( m \)'s which are lost as exceptions to Lemma 4.4.11 is at most \( \left\lceil \frac{M}{w} \right\rceil \left( 130L(E) + 13 \right) \). Note that the fiber \( E^*_s(k) \) contains at least one point that converts to a non-torsion point \((n(P(k)))^*\), hence none of the \( \psi_{i+2}(u, v, s_n(k)) \) can be zero as functions in two variables \((i = 1, ..., 16)\). Thus, by Proposition 4.1.10, there are at most \( 10 \left( 2L(E)^2 + L(E) \right) \sum_{m=2}^{16} (m^2 - 1) + 96 \) many points on \( E^*_s(n(k)) \) that convert to torsion points. As each of the \( m(n(P(k)))^* \) for \( m = 1, ..., w \) are distinct points over \( \mathbb{F}_p \) they are distinct over \( \mathbb{Q} \), thus the total number of \( m \) which we must exclude is at most:

\[
\# \text{ lost } m \text{'s} = \left\lceil \frac{M}{w} \right\rceil \left( 130L(E) + 109 + 10 \left( 2L(E)^2 + L(E) \right) \sum_{m=2}^{16} (m^2 - 1) \right).
\]

So, the total number of exceptional \((k, n, m)\) such that \( k \in \mathbb{F}_p, n \leq N \) is even, and \( m \leq M \) is even is at most

\[
\# \text{ lost triples } (k, n, m) = \frac{NM}{4} \# \text{ lost } k \text{'s} + (p - \# \text{ lost } k \text{'s}) \left[ \# \text{ lost } n \text{'s} \frac{M}{2} + \left( \frac{N}{2} - \# \text{ lost } n \text{'s} \right) \# \text{ lost } m \text{'s} \right].
\]

We choose \( l \) and \( w \) such that this is well controlled. For example, if we choose

\[
l = \left\lceil \frac{\min \left\{ N, M^4, r, \left( \frac{p}{\deg(C)} \right)^{1/4}, \ln \left( \frac{p}{112 \deg(C) L(E)^2 6^{142} L(E)} \right) \right\}}{10^6 L(E)^4} \right\rceil
\]

and

\[
w = \left\lceil \frac{\min \left\{ N^{1/4}, M^{1/4}, \left( \frac{p}{\deg(C)} \right)^{1/16}, \ln \left( \frac{p}{112 \deg(C) L(E)^2 6^{142} L(E)} \right) \right\}}{10L(E)} \right\rceil,
\]

then we can show (using the assumption that \( p > 112 \deg(C) L(E)^2 6^{142} L(E) \) and the upper bounds on \( l_i \) and \( r_i \) from Lemma 4.4.3):

\[
\frac{\# \text{ lost triples } (k, n, m)}{p^{N/2} M/2} \leq 10^8 L^3 \max \left\{ \frac{1}{N^{1/4}}, \frac{1}{M^{1/4}}, \left( \frac{\deg(C)}{p} \right)^{1/16}, \ln \left( \frac{1}{112 \deg(C) L(E)^2 6^{142} L(E)} \right) \right\}^{1/4}.
\]
Note that the $l$ and $w$ we choose will satisfy the inequalities relating $r$ and $p$ to $L(\mathcal{E})$ and $\deg(C)$ as long as this bound is $\leq 1$ (and otherwise this statement holds trivially, as the number of lost triples is less than the total number of triples).

Figure 4.4: For each non-exceptional choice of $k$, we have a grid of points over different choices of $n \leq N$ and $m \leq M$. If $n$ is one of the exceptional $n$’s that we exclude, we lose its entire row in the grid. For each of the rows of the non-exceptional $n$’s, we lose a certain number of exceptional $m$’s.

**Choices of $k$, $n$, and $m$ such that $t_{n,m}(k) \in I$**

Let $k_0 \in \mathbb{Q}$ be such that $P(k_0)$ is a non-torsion point and $E_{t_0}$ is a non-exceptional fiber. By Propositions 4.1.9 and 4.1.10 and Lemma 4.4.8 (and again using the fact that there are at most $\deg(C)$ values of $k$ that give any given fiber as $t(k)$ is non-constant), there are at most

$$\deg(C) \left(17832L(\mathcal{E})^3 + 14830L(\mathcal{E})^2 + 5922L(\mathcal{E}) + 1481\right)$$

many $k_0 \in \mathbb{Q}$ for which this is not the case.

As $m_{E_{t(k_0)}}$ is a measure by Proposition 4.2.6 there exists some $\epsilon_1 > 0$ such that

$$\left|m_{E_{t(k_0)}}(I) - m_{E_{t(k_0)}}((1 - \epsilon_1)I)\right| < \frac{\epsilon}{2} \quad \text{and} \quad \left|m_{E_{t(k_0)}}(I) - m_{E_{t(k_0)}}((1 + \epsilon_1)I)\right| < \frac{\epsilon}{2}.$$

We choose $N$ and $M$ to be larger than

$$\max \left\{ N(\mathcal{E}, E_{t(k_0)}, P(k_0), (1 - \epsilon_1)I, 0, 1, 0, 1, \epsilon), N(\mathcal{E}, E_{t(k_0)}, P(k_0), 1.1I, 0, 1, 0, 1, \epsilon) \right\}.$$ 

Then, applying Proposition 4.2.8 (with the trivial arithmetic progressions $a_1 = a_2 = 0,$
whether $E$ be the quadratic residue character. We saw in Lemma 4.4.2, that $\chi$ is a quadratic residue at each $k$ if $p \equiv 0$ or undefined mod $p$. So, as the constant must be a quadratic residue mod $p$.

Then, each of the $t_{n,m}$ is a continuous function at $k_0$ (except, possibly, when $n$ and $m$ are among the lost triples for all $k \in \mathbb{F}_p$). So, we take $U(k_0, N, M)$ to be an open set around $k_0$ such that

$$|t_{n,m}(k) - t_{n,m}(k_0)| < \epsilon$$

for all $k \in U(k_0, N, M)$, $n \leq N$, and $m \leq M$ (for which $t_{n,m}$ is continuous).

The percentage of $k$ such that $E_{t_{n,m}(k)}$ is a lift of $\tilde{E}$

We now investigate which choices of $k$, $n$, and $m$ are such that $E_{t_{n,m}(k)}$ is a lift of $\tilde{E}$. For the moment, we will assume that deg$(d_{n,m}) \leq \frac{3}{96} \sqrt{p}$. By Lemma 4.4.2, whether $E_{t_{n,m}(k)}$ is a lift will depend on whether $d_{n,m}(k)$ is some kind of residue mod $p$. As each $(m(nC))^*$ takes a point on a fiber isomorphic to $\tilde{E}$, we know, in particular, that $d_{n,m}$ is not identically zero (either in the numerator or in the denominator), so

$$\# \{k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \} \leq 2 \deg(d_{n,m}).$$

First, we consider the case where $\{E_k\}$ has $j$-invariant $j \neq 0, 1728$ mod $p$. Let $\chi_2$ be the quadratic residue character. We saw in Lemma 4.4.2, $E_{t_{n,m}(k_1)} \cong E_{t_{n,m}(k_2)}$ if and only if $\chi_2(d_{n,m}(k_1)) = \chi_2(d_{n,m}(k_2))$. In particular, $E_{t_{n,m}(k)} \cong \tilde{E}$ over $\mathbb{F}_p$ if and only if $d_{n,m}(k)$ is a quadratic residue mod $p$. However, as $d_{n,m}(k)$ is a rational function, whether it is a quadratic residue at $k$ is equivalent to whether some polynomial of degree at most $2 \deg_k d_{n,m}$ is a quadratic residue at $k$. By assumption, for each $n$ and $m$, the rational curve $(m(nC))^*$ contains points on exactly $\rho$ non-isomorphic fibers over $\mathbb{F}_p$. In this case, $\rho \leq 2$ because there are only two non-isomorphic curves of a fixed $j$-invariant over $\mathbb{F}_p$ for $j \neq 0, 1728$ mod $p$. Further, as one of these fibers is isomorphic to $\tilde{E}$, 1 must be in the image of $\chi_2(d_{n,m})$.

Suppose $d_{n,m}(k) = \text{constant} f(k)^2$ for some $f \in \mathbb{F}_p(k)$. As 1 is in the image of $\chi_2(d_{n,m})$, the constant must be a quadratic residue mod $p$. So

$$\# \{k \in \mathbb{F}_p : \chi_2(d_{n,m}(k)) = 1 \} - p = \# \{k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \}.$$
namely, all values of \( k, n, \) and \( m \) produce a lift except those where \( d_{n,m}(k) \equiv 0 \) or is undefined (and note that these cases are already included in the lost triples, as for these triples, \( E_{t_{n,m}(k)} \) has bad reduction mod \( p \)). In this case, \( \rho = 1 \).

Then, suppose \( d_{n,m}(k) \) is not of the form constant \( f(k)^2 \) over \( \mathbb{F}_p \) (and hence neither is the polynomial we get by multiplying together its numerator and denominator) or, equivalently, it is not of the form \( f(k)^2 \) over \( \overline{\mathbb{F}}_p \), as \( \mathbb{F}_p \) is perfect. Then, by Weil’s theorem on character sums of polynomials (Theorem 3.1.3) we have:

\[
\sum_{k \in \mathbb{F}_p} \chi_2(d_{n,m}(k)) \leq 2 \deg(d_{n,m}) \sqrt{p}.
\]

So,

\[
\left| \# \{ k \in \mathbb{F}_p : \chi_2(d_{n,m}(k)) = \pm 1 \} - \frac{p}{2} \right| \\
\leq 2 \deg(d_{n,m}) \sqrt{p} + \frac{\# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \}}{2}.
\]

In this case we must have \( \rho = 2 \) (as, by our assumptions about \( \deg(d_{n,m}) \), the error bound is non-trivial and there must be \( k \) such that \( \chi_2(d_{n,m}(k)) \) takes each of the two values 1 and \( -1 \)).

Now for \( j \equiv 0 \mod p \), we saw in Lemma 4.4.2 that \( E_{t_{n,m}(k)} \cong \tilde{E} \) if and only if \( d_{n,m}(k) \) is a sextic residue mod \( p \). If \( p \equiv 2 \mod 3 \), then every non-zero class is a cubic residue, and a class being a sextic residue is equivalent to it being a quadratic residue. Thus, we have the same bounds on \( \# \{ k \in \mathbb{F}_p : \chi_2(d_{n,m}(k)) = \pm 1 \} \) that we had in the \( j \not\equiv 0, 1728 \) case. If \( p \equiv 1 \mod 3 \), there exists a “rational cubic character” (see [43, Theorem 9]), namely a cubic character \( \chi_3 \) mod \( p \) such that \( \chi_3(c) = 1 \) if and only if \( c \) is a cubic residue mod \( p \). Consequently, there is a sextic character \( \chi_6 \) such that \( \chi_6(c) = 1 \) if and only if \( c \) is a sextic residue mod \( p \) given by \( \chi_6 = \chi_2 \cdot \chi_3 \).

Similarly to above, as there is a fiber isomorphic to \( \tilde{E} \) on each \( (m(nC))^* \), 1 must be in the range of \( \chi_6(d_{n,m}) \); hence, 1 must be in the range of each \( \chi_2(d_{n,m}) \) and \( \chi_3(d_{n,m}) \). Recall that \( \chi_2(d_{n,m}) \) takes values in \{1, \(-1\)\}, and \( \chi_3(d_{n,m}) \) takes values in \{1, \omega, \overline{\omega}\}, where \( \omega \) is a primitive cubic root of unity. Thus, the range of \( \chi_6(d_{n,m}) \) has at most six elements. As two fibers \( E_{t_{n,m}(k_1)} \) and \( E_{t_{n,m}(k_2)} \) are isomorphic if and only if \( \chi_6(d_{n,m}(k_1)) = \chi_6(d_{n,m}(k_2)) \), \( \rho \leq 6 \).

If \( d_{n,m} = f^6 \) over \( \overline{\mathbb{F}}_p \), then as \( \chi_6(d_{n,m}) \) takes the value 1, we have, similarly to above,

\[
\left| \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = 1 \} - p \right| = \# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \}.
\]

In this case \( \rho = 1 \).
Suppose \( d_{n,m}(k) \) is not of the form \( f(k)^2 \) over \( \mathbb{F}_p \) but is of the form \( f(k)^3 \). Then, \( \chi_3(d_{n,m}) \) is constant, implying that \( d_{n,m}(k) \) is a sextic residue if and only if \( \chi_2(d_{n,m}(k)) = 1 \). We are again in the same situation as we had for the \( j \neq 0, 1728 \) case, and hence we have the same bounds.

Next, suppose \( d_{n,m}(k) \) is not of the form \( f(k)^3 \) over \( \mathbb{F}_p \) but is of the form \( f(k)^2 \). So \( d_{n,m}(k) \) is a sextic residue if and only if it is a cubic residue, and again, using Theorem 3.1.3:

\[
\left| \sum_{k \in \mathbb{F}_p} \chi_3(d_{n,m}(k)) \right| \leq 2 \deg(d_{n,m}) \sqrt{p}.
\]

Suppose that the number of \( k \) such that \( \chi_3(d_{n,m}(k)) \) takes each of its three values \( \alpha_0, \alpha_1, \text{ and } \alpha_2 \) are \( M_0, M_0 + N_1 \), and \( M_0 + N_2 \) respectively such that \( N_2 \geq N_1 \). Then, as \( 1 + \omega + \overline{\omega} = 0 \),

\[
\sum_{k \in \mathbb{F}_p} \chi_3(d_{n,m}(k)) = N_1 \alpha_1 + N_2 \alpha_2 = N_1 (-\alpha_0) + (N_2 - N_1) \alpha_2
\]

For example, if \( \alpha_0 = \overline{\omega}, \alpha_1 = \omega, \text{ and } \alpha_2 = 1 \)

\[
\left| \sum_{k \in \mathbb{F}_p} \chi_3(d_{n,m}(k)) \right| \geq N_2 x \text{coord}(-\overline{\omega}) = \frac{N_2}{2}.
\]

By the symmetry of the situation, this bound holds generally.

Then,

\[
\# \{ k : \chi_3(d_{n,m}(k)) = \alpha_2 \} \leq \# \{ k : \chi_3(d_{n,m}(k)) = \alpha_0 \} + N_2
\]

and

\[
\# \{ k : \chi_3(d_{n,m}(k)) = \alpha_2 \} \leq \# \{ k : \chi_3(d_{n,m}(k)) = \alpha_1 \} + N_2,
\]

but

\[
\# \{ k : \chi_3(d_{n,m}(k)) = \alpha_2 \}
\]

\[
= p - \# \{ k : \chi_3(d_{n,m}(k)) = \alpha_0 \} - \# \{ k : \chi_3(d_{n,m}(k)) = \alpha_1 \} - \# \{ k : d_{n,m}(k) \equiv 0 \text{ or is undefined} \},
\]

so

\[
\# \{ k : \chi_3(d_{n,m}(k)) = \alpha_2 \} - \frac{p}{3} \leq \frac{2N_2 - \# \{ k : d_{n,m}(k) \equiv 0 \text{ or is undefined} \}}{3}.
\]

Note that we took \( \alpha_2 \) to be the value of \( \chi_3(d_{n,m}(k)) \) that occurred for the most \( k \). Proving a similar lower bound and applying our bound for \( N_2 \) above, we have for each
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

α_i

\[ \left| \# \{ k \in \mathbb{F}_p : \chi_3(d_{n,m}(k)) = \alpha_i \} - \frac{p}{3} \right| \leq \frac{8}{3} \deg(d_{n,m}) \sqrt{p} + \frac{\# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or is undefined mod } p \}}{3}. \]

Here \( \rho = 3 \) (as again, by our assumptions on \( \deg(d_{n,m}) \), the error bound is non-trivial).

Now suppose \( d_{n,m}(k) \) is not of the form \( f(k)^2 \) or \( f(k)^3 \) and hence also not \( f(k)^6 \) over \( \mathbb{F}_p \). Then, we can again apply Theorem 3.1.3 to \( \chi_6 \) to obtain:

\[ \left| \sum_{k \in \mathbb{F}_p} \chi_6(d_{n,m}(k)) \right| \leq 2 \deg(d_{n,m}) \sqrt{p}. \]

We will see that if \( \alpha_i \) is a sixth root of unity,

\[ \left| \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = \alpha_i, -\omega \alpha_i, \text{ or } -\overline{\omega} \alpha_i \} - \frac{p}{2} \right| \leq \frac{p}{6} + \frac{4}{3} \deg(d_{n,m}) \sqrt{p} + \frac{2}{3} \# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \}. \]

As

\[ \left| \sum_{k \in \mathbb{F}_p} x_{\text{coord}}(\chi_6(d_{n,m}(k))) \right| \leq \left| \sum_{k \in \mathbb{F}_p} \chi_6(d_{n,m}(k)) \right|, \]

and the smallest \( x \)-coordinate of \( 1, -\omega, \text{ or } -\overline{\omega} \) is \( \frac{1}{2} \) (and the \( x \)-coordinates of \( -1, \omega, \text{ or } \overline{\omega} \) all have absolute value at most 1), we have

\[ \frac{1}{2} \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = 1, -\omega, \text{ or } -\overline{\omega} \} \]

\[ \leq \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = -1, \omega, \text{ or } \overline{\omega} \} + \sum_{k \in \mathbb{F}_p} \chi_6(d_{n,m}(k)) \].

However, we also have

\[ \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = -1, \omega, \text{ or } \overline{\omega} \} = p - \# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \} - \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = 1, -\omega, \text{ or } -\overline{\omega} \} \]

from which we deduce the above claim when \( \alpha_i = 1 \). However, by symmetry, the same argument holds for any \( \alpha_i \).

Furthermore, as \( \alpha_i \) and \( -\alpha_i \) are the two values of \( \chi_6(d_{n,m}) \) that correspond to a shared
value of $\chi_2(d_{n,m})$, we have from the $d_{n,m} \neq f^3$ case that

$$\left| \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = \alpha_i \text{ or } -\alpha_i \} - \frac{p}{3} \right| \leq \frac{8}{3} \deg(d_{n,m}) \sqrt{p} + \frac{\# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \} }{3}.$$

Similarly, $-\alpha_i, -\omega\alpha_i,$ and $-\overline{\omega}\alpha_i$ are values of $\chi_6(d_{n,m})$ that correspond to a shared value of $\chi_3(d_{n,m})$, so from the $d_{n,m} \neq f^2$ case

$$\left| \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = -\alpha_i, -\omega\alpha_i, \text{ or } -\overline{\omega}\alpha_i \} - \frac{p}{2} \right| \leq 2 \deg(d_{n,m}) \sqrt{p} + \frac{\# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \} }{2}.$$

Putting these inequalities together and using:

$$\# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = \alpha_i \} = \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = \alpha_i, -\omega\alpha_i, \text{ or } -\overline{\omega}\alpha_i \} - \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = -\alpha_i, -\omega\alpha_i, \text{ or } -\overline{\omega}\alpha_i \} + \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = -\alpha_i \},$$

we get:

$$\left| \# \{ k \in \mathbb{F}_p : \chi_6(d_{n,m}(k)) = \alpha_i \} - \frac{p}{6} \right| \leq \frac{p}{12} + 3 \deg(d_{n,m}) \sqrt{p} + \frac{3}{4} \# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \}.$$

Here $\rho = 6$ by similar reasoning to above.

Finally, if $j \equiv 1728 \mod p$ then, by Lemma 4.4.2, $E_{t_{n,m}(k)} \cong \tilde{E}$ if and only if $d_{n,m}(k)$ is a quartic residue mod $p$. If $p \equiv 3 \mod p$, then a value is a quartic residue if and only if it is a quadratic residue. So, we have the same bounds as in the $j \neq 0, 1728$ case. We have excluded the $p \equiv 1 \mod p$ case, as we do not know of a “rational quartic character” that can play the role of $\chi_3$.

In any case

$$\left| \# \{ k \in \mathbb{F}_p : E_{t_{n,m}(k)} \cong \tilde{E} \text{ over } \mathbb{F}_p \} - \frac{p}{\rho} \right| \leq C_0(\rho),$$

\[\text{We expect that it might be possible to remove or at least improve the } \frac{p}{\rho} \text{ term. We used the property that the sum of the roots of unity is zero in a rather crude way. Indeed, consider an extreme case where asymptotically (considering only the terms proportional to } p) \chi_6(d_{n,m}(k)) \text{ takes values } 1, -\omega, -\overline{\omega}, -1, \omega, \text{ and } \overline{\omega} \text{ at } \frac{p}{12}, \frac{3p}{12}, \frac{3p}{12}, \frac{p}{12}, \frac{p}{12}, \text{ and } \frac{p}{12} \text{ many values of } k \text{ respectively. This satisfies all of the bounds that we used, but one can see that the sum of these values, namely } \sum_{k \in \mathbb{F}_p} \chi_6(d_{n,m}(k)), \text{ is not zero.} \]
where \( C_0(\rho) = \begin{cases} \# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \} & \text{if } \rho = 1 \\ 2 \deg(d_{n,m})\sqrt{p} + \frac{\# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \}}{2} & \text{if } \rho = 2 \\ \frac{8}{3} \deg(d_{n,m})\sqrt{p} + \frac{\# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \}}{3} & \text{if } \rho = 3 \\ \frac{p}{12} + 3 \deg(d_{n,m})\sqrt{p} + \frac{3\# \{ k \in \mathbb{F}_p : d_{n,m}(k) \equiv 0 \text{ or undefined mod } p \}}{4} & \text{if } \rho = 6. \end{cases} \)

**Conclusion of proof**

We take a set \( S \) of \( k \)'s in \( U(k_0, N, M) \) consisting of one element in each class mod \( p \).

Being a candidate lift consists in being a lift and in having a list of properties that we saw hold for all triples \((k, n, m)\) except the lost triples. Thus, we have

\[
\# \left\{ (n, m, k) : n \leq N, m \leq M, n, m \text{ even, } k \in S \right\} \\
\geq \# \left\{ (n, m, k) : n \leq N, m \leq M, n, m \text{ even, } k \in S \\
\quad \text{or } t_{n,m}(k) \in I \right\} - \# \text{lost triples}(k, n, m) \\
\geq \# \left\{ (n, m, k) : n \leq N, m \leq M, n, m \text{ even, } k \in S \\
\quad \text{or } t_{n,m}(k) \in (1 - \epsilon_1)I \right\} - \# \text{lost triples}(k, n, m) \\
\geq \# \left\{ (n, m) : n, m \text{ even, } \\
\quad t_{n,m}(k_0) \in (1 - \epsilon_1)I \right\} \min_{n,m} \# \left\{ k \in S : E_{t_{n,m}(k)} \equiv \tilde{E} \text{ mod } p \right\} - \# \text{lost triples}(k, n, m)
\]

So,

\[
\# \left\{ (n, m, k) : n \leq N, m \leq M, n, m \text{ even, } k \in S \\
\quad \text{or } t_{n,m}(k) \in I \right\} \geq \frac{p^{N M}}{2} \\
\geq (m_{E_t(k_0)}(I) - 2\epsilon) \left( \frac{1}{p} \frac{C_0(\rho)}{p} \right) - \frac{\# \text{lost triples}(k, n, m)}{p^{N M}}.
\]

Proving a similar upper bound and using Proposition 4.4.5 for a bound on \( \deg d_{n,m} \), we see:
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

\[ \# \left\{ (n, m, k) : n \leq N, m \leq M, n, m \text{ even}, k \in S \right\} \]
\[ \frac{m_{E_t(k_0)}(I)}{\rho} \leq 0 \]
\[ \frac{2\epsilon + C_1(\rho)}{\rho} \left( \frac{m_{E_t(k_0)}(I) + 2\epsilon}{p} \right) \]
\[ + 10^8 L(\mathcal{E})^3 \max \left\{ \frac{1}{N^{1/4}}, \frac{1}{M}, \frac{1}{p^{1/4}} \left( \frac{\deg(C)}{p} \right)^{1/16}, \left( \frac{1}{\ln(p \cdot L(\mathcal{E})^{1/12} L_E)} \right)^{1/4} \right\} , \]

where
\[ C_1(\rho) = \begin{cases} 
10^3 \deg(C) L(\mathcal{E})^5 (2\sqrt{2} + 3)^{N+M} \sqrt{p} & \text{if } \rho = 1, 2, \text{ or } 3 \\
\frac{p}{12} + 10^3 \deg(C) L(\mathcal{E})^5 (2\sqrt{2} + 3)^{N+M} \sqrt{p} & \text{if } \rho = 6 \end{cases} \]

Returning to the assumption that \( \deg(d_{n,m}) \leq \frac{3}{96} \sqrt{p} \), by Proposition 4.4.5, it is sufficient to have \( \sqrt{p} \geq 10^5 \deg(C) L(\mathcal{E})^5 (2\sqrt{2} + 3)^{N+M} \). However if this is not the case, then \( \frac{C(\rho)}{p} > 1 \) where
\[ C(\rho) = \begin{cases} 
10^5 \deg(C) L(\mathcal{E})^5 (2\sqrt{2} + 3)^{N+M} \sqrt{p} & \text{if } \rho = 1, 2, \text{ or } 3 \\
\frac{p}{12} + 10^5 \deg(C) L(\mathcal{E})^5 (2\sqrt{2} + 3)^{N+M} \sqrt{p} & \text{if } \rho = 6 \end{cases} \]

Then, the above bound is trivial for with \( C_1(\rho) \) replaced by \( C(\rho) \), as it can be reduced to:
\[ 0 \leq \frac{\# \left\{ (n, m, k) : n \leq N, m \leq M, n, m \text{ even}, k \in S \right\}}{p^{N+M}} \leq m_{E_t(k_0)}(I) + 2\epsilon , \]
which we know by above.

As \( S \) is any set of \( k \) in \( U(k_0, N, M) \) that contains one element of each class of \( \mathbb{F}_p \), this concludes the proof.

Note that if we weaken the assumptions on the number of non-isomorphic fibers on which \( (m(nC)^*)^* \) has points and only want the lower bound in the above argument, we
have seen:

**Theorem 4.4.12.** Consider $\tilde{E}$, $p$, $\{E_t\}$, and $C$ that satisfy the hypotheses of Theorem 4.4.1 except that for each $n$ and $m$ we only assume the rational curve $(m(nC)^*)^*$ contains points on at most $\rho$ many non-isomorphic fibers over $\mathbb{F}_p$, and that one of these fibers is isomorphic to $\tilde{E}$ over $\mathbb{F}_p$.

Then, let $I \subset \mathbb{R}$ be an interval and let $\epsilon > 0$. Let $k_0 \in \mathbb{Q}$, avoiding at most

$$\deg(C) \left(17832L(E)^3 + 14830L(E)^2 + 5922L(E) + 1481\right)$$

exceptions. Then, there exists an $\epsilon_1 > 0$ depending only on $E$, $C$, $k_0$, $I$, and $\epsilon$ such that for $N, M \geq N_0(P(k_0), (1 - \epsilon_1)I, \epsilon)$, there exists an open set $U(k_0, N, M)$ (which depends on $N$ and $M$) around $k_0$ such that

$$\frac{m_{E_t(k_0)}(I)}{\rho} - \frac{2\epsilon}{\rho} - C(\rho) \left(\frac{m_{E_t(k_0)}(I) + 2\epsilon}{p}\right)$$

$$- 10^8L(E)^3 \max \left\{ \frac{1}{N^{1/4}}, \frac{1}{M^{1/4}} \{ \frac{\deg(C)}{p} \}^{1/16}, \left(\frac{1}{\ln \left(\frac{p}{112 \deg(C)L(E)^{6\log_{10}L(E)}}\right)}\right)^{1/4} \right\}$$

where

$$C(\rho) = \begin{cases} 10^5 \deg(C)L(E)^5(2\sqrt{2} + 3)^{N+M}\sqrt{p} & \text{if } \rho = 1, 2, \text{ or } 3 \\ \frac{p}{12} + 10^5 \deg(C)L(E)^5(2\sqrt{2} + 3)^{N+M}\sqrt{p} & \text{if } \rho = 6 \end{cases}$$

Furthermore, we have:

**Theorem 4.4.13.** Let $\tilde{E}$ be an elliptic curve over a finite field $\mathbb{F}_p$ ($p > 23$), and let $E$ and $C$ be as in Theorem 4.4.12. Then, let $I \subset \mathbb{R}$ be an interval such that there exists $k_0 \in \mathbb{Q}$, $\epsilon_1 > 0$, $z > 0$, and $N, M \geq N_0(P(k_0), (1 - \epsilon_1)I, z)$ such that

$$\delta := \frac{z}{\rho} - C(\rho)\frac{z}{p}$$
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

\[-\max \left\{ \frac{1}{N^{1/4}}, \frac{1}{M^{1/4}}, \frac{1}{r^{1/4}}, \left( \frac{\deg(C)}{p} \right)^{1/16}, \left( \frac{1}{\ln \left( \frac{p}{112 \deg(C) L(E)^3 + 142 L(E)^2} \right)^{1/4}} \right)^{1/4} \right\} > 0,
\]

where \( r \) and \( C(\rho) \) are as in Theorem 4.4.12. Then, there is a candidate lift \( E_{t_{\text{out}}} \) of \( \tilde{E} \) such that \( t_{\text{out}} \in I \), \( \text{ht}(t_{\text{out}}) \leq \text{poly}(\ln(p)) \), and this \( t_{\text{out}} \) can be found in randomized \( \text{poly}(\ln(p)) \) time, where the coefficients of these polynomials depend on \( L(E), K(E), \deg(C), \text{coeff}(C) \), and \( N_0(P(k_0), (1 - \epsilon_1) I, z) \) (but not on \( p \)).

We will see that for \( p \) sufficiently large (relative to fixed \( E \) and \( C \)), such choices of \( \epsilon_1, N, \) and \( M \) will exist.

**Proof.** First, we choose a random \( k_0 \) rational by choosing its numerator and denominator both in

\[
[1, ..., 2 \deg(C) \left( 17832 L(E)^3 + 14830 L(E)^2 + 5922 L(E) + 1481 \right)].
\]

There are at least enough distinct rational numbers represented here so we have at least a \( 1/2 \) chance of choosing \( k_0 \) such that \( P(k_0) \) is a non-torsion point on a non-exceptional fiber. For each \( k_0 \) we choose, we can check these conditions by evaluating whether any of the division polynomials for \( m = 2, ..., 16 \), \( \text{den}(x(k)) \), or \( \Delta(t(k)) \) are zero. Note that these polynomials, as well as the bound on the height of \( k_0 \), depend only on \( L(E) \) and \( \deg(C) \), and are, in particular, independent of \( p \).

We assumed there exist \( \epsilon_1, z, N, \) and \( M \) such that \( \delta > 0 \). Suppose we have these values available to us. See the following remark for what one can do at this point to try to find working \( \epsilon_1, N, \) and \( M \) if they are unknown.

In the proof of Theorem 4.4.1, we said that \( U(k_0, N, M) \) could be found as the intersections of the delta neighborhoods of \( t_{n,m} \)'s, which are continuous. Specifically, suppose the \( k_0 \) we choose is such that we can write it as a ratio of two integers less than \( h \). We write

\[ f(w) = t_{n,m}(w + k_0) - t_{n,m}(k_0), \]

and writing \( f \) as a single rational function with integer coefficients, we note

\[ \deg(f) \leq \deg(t_{n,m}) \quad \text{and} \quad \text{coeff}(f) \leq 4 h^2 \deg(t_{n,m}) \cdot \deg(t_{n,m})^{\deg(t_{n,m})+1} \cdot \text{coeff}(t_{n,m})^2. \]

Note that the \( t_{n,m}(w + k_0) \) evaluated at \( w = 0 \) gives \( t_{n,m}(w + k_0) \), which is a non-zero rational number. Hence \( t_{n,m}(w + k_0) \) has non-zero constant term in its denominator. Thus, the denominator of \( f \), which is the denominator of \( t_{n,m}(w + k_0) \) multiplied by the denominator of \( t_{n,m}(k_0) \), also has non-zero constant term, which is at least of absolute value 1, as the coefficients of \( f \) are integers. On the other hand, \( f(0) = 0 \), so the
constant term of the numerator of $f$ is zero. Hence $|\text{den}(f)| \geq 1 - \deg(f) \cdot \text{coeff}(f)|w|$ and $|\text{num}(f)| \leq \deg(f) \cdot \text{coeff}(f)|w|$. Then, we see that if
\[
|k - k_0| = |w| \leq \min \left\{ \epsilon_1, 1 \right\} \frac{8h^2 \deg(t_{n,m}) \cdot \deg(t_{n,m})^{\deg(t_{n,m})+2} \cdot \text{coeff}(t_{n,m})^2}{\deg(C)L(E)^9(N+M)^{9N+M}K(E)^{10}L(E)^{2gM} \text{deg}(C)^{73}L(E)^{9N+M} \text{coeff}(C)^{12}L(E)^{9N+M}}.
\]
we have $|t_{n,m}(k) - t_{n,m}(k_0)| = |f(w)| \leq \epsilon_1$.

Then, using the bounds of Propositions \ref{prop:4.4.5} and \ref{prop:4.4.7} and Lemma \ref{lem:4.4.3} it is sufficient that $|k - k_0| \leq \delta_1$ where $\delta_1 = \min \left\{ \epsilon_1, 1 \right\}$.

Then, we can pick a finite subset of $\mathcal{U}(k_0, N, M)$ that is uniform in the classes mod $p$ as follows: take $R = 1 + \left\lceil \frac{1}{\delta} \right\rceil p$, then the finite subset $\mathcal{S} = \left\{ k_0 + \frac{i}{R} : i = 1, ..., p \right\}$ is uniform in the residue classes mod $p$ and $|k_0 + \frac{i}{R} - k_0| = \left| \frac{i}{R} \right| \leq \frac{p}{R} < \delta_1$, so all of the elements in $\mathcal{S}$ are in $\mathcal{U}(k_0, N, M)$.

Now we simply make random choices $n \leq N$, $m \leq M$ and $k \in \mathcal{S}$, compute $W = (m(nP(k))^*)$ and $t_{\text{out}} = \tau(m(nP(k))^*)$, and check whether $t_{\text{out}} \in I$ and whether $W$ is non-torsion and non-zero mod $p$. By Theorem \ref{thm:4.4.12}, we have at least a $\delta$ chance of success for each such random triple. The bounds $N$ and $M$ do not depend on $p$, and elements of $\mathcal{S}$ have bit size that is polynomial in $\ln p$ (but exponential in $L(E)$, $K(E)$, $\deg(C)$, $\text{coeff}(C)$, $N$, and $M$); thus, for each trial of $n$, $m$, and $k$, our computations run in poly($\ln p$) time (where, again, this polynomial depends on $L(E)$, $K(E)$, $\deg(C)$, $\text{coeff}(C)$, $N$, and $M$).

\[ \square \]

Remark 4.4.14. Suppose we do not have values given to us a priori for $\epsilon_1$, $z$, $N$, and $M$ and we want to search for working values. We can do the following: We find $\epsilon_1$ by repeatedly applying Algorithm \ref{alg:2} to the interval $(1 - \epsilon_1)I$ for decreasing values of $\epsilon_1$ until the algorithm produces some $z > 0$ and $N_0(P(k_0), (1 - \epsilon_1)I, z)$. By Proposition \ref{prop:4.2.7}, for any $\epsilon_1 \in (0, 1)$, we have $m_{E_{t(k_0)}}((1 - \epsilon_1)I) > 0$; so, for any $\epsilon_1$, we know Algorithm \ref{alg:2} will halt with probability 1. However, if $\epsilon_1$ is such that $m_{E_{t(k_0)}}((1 - \epsilon_1)I)$ is very small, one may want to choose a smaller $\epsilon_1$ so that Algorithm \ref{alg:2} runs more quickly. How small $\epsilon_1$ must be to guarantee $m_{E_{t(k_0)}}((1 - \epsilon_1)I)$ is of a certain size relative to $m_{E_{t(k_0)}}(I)$ depends on how clumped the measure of $I$ is under $m_{E_{t(k_0)}}$ relative to Lesbesque measure. Note that the running time of this process is constant with respect to $p$.

Now we try to bound each of the error terms used in the computation of $\delta$ by $\frac{z}{3p}$. Then, we need to choose $N$ and $M$ larger than $N_0(P(k_0), (1 - \epsilon_1)I, z)$ and also larger...
than $\frac{10^{34}L(\mathcal{E})^{12}p^4}{z^4}$ so that $10^{34}L(\mathcal{E})^3 \max \left\{ \frac{1}{N^{1/4}}, \frac{1}{M^{1/4}} \right\} \leq \frac{z}{3p}$. So, we take $N$ and $M$ to be the maximum of these quantities. Now we have made all the choices necessary to compute $\delta$. If we arrive at a positive $\delta$, we can continue. Otherwise, we halt the algorithm as $p$ is not large enough relative to $\mathcal{E}$, $C$, $I$ and the choices we made for $k_0$, $\epsilon_1$, $N$, and $M$. Note that this process is not perfectly optimized, so we might fail to find acceptable $\epsilon_1$, $N$, and $M$ even if they exist. However, our choices are probably relatively close to optimal, considering the exponential dependence of the error bound on $N$ and $M$, as we have chosen $\epsilon_1$ to be relatively large which allows $N$ and $M$ to be relatively small. Note that for any fixed choices of $z$, $N$, and $M$, if $p$ and $r$ are sufficiently large then we will, in fact, have $\delta > 0$.

We summarize this process in Algorithm $[\ref{alg:diffusion}]$.

In the setting where we view values of $m_{E_t}(I)$ and $N(P, I, \epsilon)$ as being computationally accessible, we have:

**Theorem 4.4.15.** Let $\tilde{E}$ be an elliptic curve over a finite field $\mathbb{F}_p$ ($p > 23$) and let $\mathcal{E}$, $C$, $I$, $k_0$, $\epsilon > 0$ and $\epsilon_1$ be as in Theorem $[\ref{thm:diffusion}]$. Then if there exists

$$N, M \geq N(P(k_0), (1 - \epsilon_1)I, \epsilon)$$

such that

$$\delta = \frac{m_{E_t(k_0)}(I)}{\rho} - \text{the error bound of Theorem } [\ref{thm:diffusion}] > 0,$$

there is a candidate lift $E_{\text{out}}$ of $\tilde{E}$ such that $t_{\text{out}} \in I$, $ht(t_{\text{out}}) \leq \text{poly}(\ln(p))$. Furthermore, if one can efficiently compute values $m_{E_t}(I)$ and $N(P, I, \epsilon)$, then this $t_{\text{out}}$ can be found in randomized $\text{poly}(\ln(p), \frac{1}{\delta})$ time where the coefficients of these polynomials depend on quantities associated with $\mathcal{E}$, $C$, $I$, and $\epsilon$.

**Proof.** Note that

$$N_0 \left( P(k_0), (1 - \epsilon_1)I, m_{E_t(k_0)}(I) - \epsilon \right) \leq N \left( P(k_0), (1 - \epsilon_1)I, \epsilon \right).$$

Thus, we can take $z = m_{E_t(k_0)}(I) - \epsilon$, and the $\delta$ we compute is exactly the same value of $\delta$ as in Theorem $[\ref{thm:diffusion}]$. Then, as we assume that we can compute the necessary values of $m_{E_t}(I)$ and $N(P, I, \epsilon)$, we proceed exactly as in the proof of Theorem $[\ref{thm:diffusion}]$.

From this we conclude Theorem $[\ref{thm:main}]$ from the Introduction. Note that we could also use Theorem $[\ref{thm:diffusion}]$ to prove an analog of Corollary $[\ref{cor:main}]$. 


Algorithm 6: Algorithm to find a candidate lift in fixed interval $I$ following Theorem 4.4.13
4.4.5 Examples of surfaces to which Theorems 4.4.1 and 4.4.12 apply

Examples of the form (4.3)

Let $e \neq 0$. Then, it is shown in the proof of Theorem 3.1 of [42] that the surface

$$E_t : y^2 = x^3 + (t^3 + e)^2$$

contains the rational curve $C : (x(k), y(k), t(k))$ where

$$x(k) = \frac{k^2}{3} - \left( \frac{-432e^4 + 1440e^2k^6 + 16k^{12}}{1728e^3k^2 + 576ek^8} \right)^2,$$

$$y(k) = \frac{-2187e^8 - 19440e^6k^6 + 2754e^4k^{12} - 72e^2k^{18} + k^{24}}{1296e^2k^3(3e^2 + k^6)^2},$$

and

$$t(k) = \frac{27e^4 - 90e^2k^6 - k^{12}}{36ek^2(3e^2 + k^6)}.$$

Further, Ulas notes in [42] that if one views $(x(k), y(k))$ as a section on the surface

$$y^2 = x^3 + \left( \frac{27e^4 - 90e^2k^6 - k^{12}}{36ek^2(3e^2 + k^6)} \right)^3 + e \right)^2,$$

then this section is non-torsion. Hence, by the Silverman Specialization Theorem (Theorem 3.4.1), there can only be finitely many values of $k$ such that the point $(x(k), y(k))$ is torsion on $E_t(k)$. So, in particular, $C$ contains at least one non-torsion point (on some non-singular fiber).

We have seen in Section 4.1.2 that surfaces of this form are cross-fibered (as they are of the form (4.3)) with a correspondence to:

$$E^*_s : v^2 = u^3 + (es^3 + 1).$$

We compute in this case $L(\mathcal{E}) = 3$ and $\deg(C) = 24$. Further, we note that this surface has constant $j$-invariant 0.

We saw in the proof of Theorem 4.4.1 that if the bound in the statement is non-trivial, $j = 0$, and $p \equiv 1 \mod 3$, then the property that the rational curve $(m(nC))^*$ contain points on exactly three non-isomorphic fibers over $\mathbb{F}_p$ is equivalent to $d_{n,m}(k)$ being a square but not a cube as a rational function over $\mathbb{F}_p$ (for this surface, the case
where \( p \equiv 2 \mod 3 \) was considered in Remark 4.3.4. Of course \( d_{n,m}(k) = \frac{(t_{n,m}(k)^3 + e)^2}{b} \) is obviously a square over \( \mathbb{F}_p \), and we prove the following proposition:

**Proposition 4.4.16.** Let \( e \) be a non-zero element of \( \mathbb{F}_p \) and \( g(k) \) be a rational function over \( \mathbb{F}_p \). Then, there does not exist any rational function \( h(k) \) and \( d \in \mathbb{F}_p \) such that \( g(k)^3 + e = dh(k)^3 \).

The major tool that we will use to prove this is the abc conjecture for polynomials, which is a theorem due to Mason:

**Theorem 4.4.17** (Mason, see [20]). Let \( a(x), b(x), \) and \( c(x) \) be three polynomials with no common factors such that \( a(x) + b(x) = c(x) \), then

\[
\max \{ \deg a, \deg b, \deg c \} \leq n_0(abc) - 1,
\]

where \( n_0(f) \) denotes the number of distinct roots of \( f \).

**Proof of Proposition 4.4.16.** Express \( g(k) = \frac{g_1(k)}{g_2(k)} \) and \( h(k) = \frac{h_1(k)}{h_2(k)} \) as quotients of relatively prime polynomials. Then,

\[
t^3 + e = dh(k)^3 \Rightarrow g_1(k)^3 + eg_2(k)^3 = dh_1(k)^3g_2(k)^3.
\]

As the left hand side is a polynomial,

\[
h_2(k)^3|h_1(k)^3g_2(k)^3,
\]

and as \( h_1 \) and \( h_2 \) are relatively prime,

\[
h_2(k)^3|g_2(k)^3.
\]

If \( h_2(k)^3 \neq g_2(k)^3 \), then there is a polynomial \( a(k) \) that is a factor of \( g_2 \) that also factors \( g_1(k)^3 + eg_2(k)^3 \) and hence \( g_1 \), which would be contradictory. Hence, we have:

\[
g_1(k)^3 + eg_2(k)^3 = dh_1(k)^3,
\]

where the three polynomials \( g_1, g_2, \) and \( h_1 \) are relatively prime. Then, by Theorem 4.4.17 we see:

\[
\max (3 \deg(g_1), 3 \deg(g_2), 3 \deg(h_1)) \leq \deg(g_1) + \deg(g_2) + \deg(h_1) - 1.
\]
Thus,

- \[ 2 \deg(g_1) \leq \deg(g_2) + \deg(h_1) - 1 \]
- \[ 2 \deg(g_2) \leq \deg(g_1) + \deg(h_1) - 1 \]
- \[ 2 \deg(h_1) \leq \deg(g_1) + \deg(g_2) - 1 \]

Combining inequalities 1 and 3 gives us \( \deg(g_1) \leq \deg(g_2) - \frac{1}{3} \), while combining inequalities 2 and 3 \( \deg(g_2) \leq \deg(g_1) - \frac{1}{3} \), which is contradictory.

Hence, \( d_{n,m}(k) \) is not a cube over \( \mathbb{F}_p \) for any \( n \) and \( m \). Following the analysis in Section 4.4.2, one of the three non-isomorphic fibers in each \( (m(nC)^*)^* \) is clearly isomorphic to \( \tilde{E} \), as all of the values of \( d_{n,m}(k) \) are quadratic residues mod \( p \).

We see explicitly that this surface has non-trivial reduction as a cross-fibered surface for \( p > 3 \) as we compute:

\[
\Delta^*(x, y, t) = -432 \left( e \left( \frac{x}{x+e} \right)^3 + 1 \right)^2 \quad \text{den}(v)(x, y, t) = t^3 + e \quad \text{den}(\sigma)(x, y, t) = t^3 + e
\]

\[
\Delta^{**}(u, v, s) = -432 \left( \left( \frac{u}{s} \right)^3 + e \right)^4 \quad \text{den}(\xi)(u, v, s) = s^2 \quad \text{den}(\tau)(x, y, t) = s
\]

Thus, we have shown:

**Example 4.4.18.** Let \( p > 6^{433} \) be a prime number congruent to 1 mod 3. Let \( E_t \) and \( C \) as above, and let \( \tilde{E} \) be the reduction of any fiber of \( E_t \) of good reduction. Let \( I \subset \mathbb{R} \) be an interval, and let \( \epsilon > 0 \). Take \( r_0 \) to be a lower bound on the largest order of \( P(k_0) \) on its fiber mod \( p \). Choose \( k_0 \in \mathbb{Q} \), avoiding at most \( 10^8 \) exceptions. Then, there exists an \( \epsilon_1 > 0 \) depending only on \( E, C, k_0, I, \) and \( \epsilon \) such that for \( N, M \geq \max \{ N(P(k_0), \epsilon), N(P(k_0), (1 + \epsilon_1)I, \epsilon) \} \) there exists an open set \( \mathcal{U}(k_0, N, M) \) (which depends on \( N \) and \( M \)) around \( k_0 \) such that

\[
\left| \text{Prob}_{n,m,k} \left( \begin{array}{c} (m(nP(k))^*)^* \text{ is on a fiber} \\ E_{t_{n,m}(k)} \text{ which is a candidate lift and } t_{n,m}(k) \in I \\ n \leq N \text{ and } m \leq M \\ \text{ are even and } k \in \mathcal{U}(k_0, N, M) \end{array} \right) - \frac{m_{E_t(k_0)}(I)}{3} \right| < 2 \epsilon + 10^9 \cdot \frac{2\sqrt{2} + 3)^{N+M}}{\sqrt{p}} \left( m_{E_t(k_0)}(I) + 2\epsilon \right)
\]

\[
+ 10^{10} \max \left\{ \frac{1}{N^{1/4}}, \frac{1}{M^{1/4}}, \frac{1}{r_0^{1/4}}, \left( \frac{24}{p} \right)^{1/16}, \left( \frac{1}{\ln \left( \frac{p}{r_0^{1/4}} \right)} \right)^{1/4} \right\}.
\]
Note that if we knew a priori that \( \tilde{E} \) had prime order over \( \mathbb{F}_p \), then \( r_0 \geq p + 1 - 2\sqrt{p} \), as \( \mathcal{E} \) has non-trivial reduction mod \( p \). Otherwise, for \( \frac{1}{\sqrt{r_0}} \) to be smaller than any given bound translates into another condition that \( p \) be sufficiently large, as there is a point on \( C \) that is non-torsion on its fiber, so none of the division polynomials \( \psi_m(C) \) can be identically zero over \( \mathbb{Q} \) and hence not identically zero over \( \mathbb{F}_p \) for sufficiently large \( p \).

Examples of the form (4.1)

Let \( \alpha \) and \( \beta \) be rational numbers such that

- \( 4 \left( \beta - \frac{\alpha^2}{3} \right)^3 + 27 \left( \frac{2}{27} \alpha^3 - \frac{\alpha \beta}{3} \right)^2 \neq 0 \)
- \( \beta - \frac{\alpha^2}{3} \neq 0 \)
- \( \frac{2}{27} \alpha^3 - \frac{\alpha \beta}{3} \neq 0 \)
- \( \frac{\beta - \alpha^2}{\frac{2}{27} \alpha^3 - \frac{\alpha \beta}{3}} \in \mathbb{Q}^2 \)

We will let \( \tilde{E} \) be the reduction of

\[
y^2 = x^3 + \frac{\beta - \frac{\alpha^2}{3}}{(\beta - \frac{\alpha^2}{3})^2} x + \frac{\frac{2}{27} \alpha^3 - \frac{\alpha \beta}{3}}{(\beta - \frac{\alpha^2}{3})^3}
\]

mod \( p \) where \( p \) will be a prime chosen later, subject to constraints.

Then, it is shown in Section 4.1.2 that the surface

\[
E_t: y^2 = x^3 + \frac{(\beta - \frac{\alpha^2}{3})}{(t^2 + \beta - \frac{\alpha^2}{4})^2} x + \frac{\frac{2}{27} \alpha^3 - \frac{\alpha \beta}{3}}{(t^2 + \beta - \frac{\alpha^2}{4})^3}
\]

is cross-fibered with a correspondence to

\[
E_s^*: v^2 = u^3 + \left( \beta - \frac{\alpha^2}{3} \right) u + \left( \frac{2}{27} \alpha^3 - \frac{\alpha \beta}{3} - \left( \beta - \frac{\alpha^2}{4} \right) s^2 \right)
\]

We compute the \( j \)-invariant of this surface to be

\[
\frac{-4 \left( \beta - \frac{\alpha^2}{3} \right)^3}{-4 \left( \beta - \frac{\alpha^2}{3} \right)^3 - 27 \left( \frac{2}{27} \alpha^3 - \frac{\alpha \beta}{3} \right)^2}
\]

which is clearly constant and is furthermore neither 0 nor 1728 by our assumptions on \( \alpha \) and \( \beta \).
This surface contains the rational curve \( C : (x(k), y(k), t(k)) \), where

\[
x(k) = \frac{k^2 + \frac{\alpha}{3}}{k^4 + \alpha k^2 + \beta}, \quad y(k) = \frac{k}{k^4 + \alpha k^2 + \beta}, \quad \text{and} \quad t(k) = k^2 + \frac{\alpha}{2}.
\]

We can view \((x(k), y(k))\) as a section on the surface

\[
y^2 = x^3 + \left(\frac{\beta - \frac{\alpha^2}{3}}{k^4 + \alpha k^2 + \beta}\right)^2 x + \frac{\left(\frac{27}{27} \alpha^3 - \frac{\alpha \beta}{3} \right)}{(k^4 + \alpha k^2 + \beta)^3},
\]

which also contains the 2-torsion section \((x, y) = \left(\frac{\alpha / 3}{k^4 + \alpha k^2 + \beta}, 0\right)\), and these two sections intersect at \( k = 0 \). (Note that the existence of this torsion section implies that fibers of \( E_t \) cannot be curves of cryptographic instances of the ECDLP). Then, the section induced by \( C \) must be non-torsion, as we have by [22, Lemma 1.1] that any two torsion sections would be disjoint. Hence, by the Silverman Specialization Theorem, \( C \) contains points that are non-torsion on their fibers.

We compute \( L(E) = 3 \) and \( \deg(C) = 4 \). This surface has non-trivial reduction as a cross-fibered surface for \( p > 3 \) as we compute:

\[
\Delta^*(x, y, t) = -16 \left[ 4 \left( \beta - \frac{\alpha^2}{3} \right)^3 + 27 \left( \frac{27}{27} \alpha^3 - \frac{\alpha \beta}{3} \right) y^2 \left( t^2 + \beta - \frac{\alpha^2}{4} \right)^4 \right]
\]

\[
\Delta^{**}(u, v, s) = \frac{-16 \left[ 4 \left( \beta - \frac{\alpha^2}{3} \right)^3 + 27 \left( \frac{27}{27} \alpha^3 - \frac{\alpha \beta}{3} \right) \right]}{\left( \frac{v}{s} \right)^2 + \beta - \frac{\alpha^2}{4}}^6
\]

\[
\text{den}(v)(x, y, t) = 1 \quad \text{den}(\sigma)(x, y, t) = 1
\]

\[
\text{den}(\xi)(u, v, s) = v^2 + \left( \beta - \frac{\alpha^2}{4} \right) s^2 \quad \text{den}(\tau)(x, y, t) = s
\]

Now we will study the number of non-isomorphic fibers over \( \mathbb{F}_p \) on which each \((m(nC)^*)^*\) has points. Note that in the Weierstrass model we have chosen, we have \( \deg(\text{numerator}(t(k))) > \deg(\text{denominator}(t(k))) \). Compute

\[
t_{m,n}(k) = \frac{v_{n,m}(k)}{y_n(k) \left( t(k)^2 + \beta - \frac{\alpha^2}{4} \right)}.
\]

Using Lemma \[4.4.3\] we see that

\[
\deg(\text{numerator}(y_n(k))) - \deg(\text{denominator}(y_n(k)))
\]
\[ = \deg(\text{numerator}(y(k))) - \deg(\text{denominator}(y(k))). \]

(Note this is well-defined as any common terms that we could multiply through would effect the numerator and denominator equally.) Similarly,

\[
\deg(\text{numerator}(v_{n,m}(k))) - \deg(\text{denominator}(v_{n,m}(k))) \\
= \deg(\text{numerator}(v_n(k))) - \deg(\text{denominator}(v_n(k))).
\]

But

\[ v_n(k) = y_n(k) \cdot t(k) \cdot \left( t(k)^2 + \beta - \frac{\alpha^2}{4} \right). \]

By what we know about \( t(k), \)

\[
\deg \left( \text{numerator} \left( t(k)^2 + \beta - \frac{\alpha^2}{4} \right) \right) - \deg \left( \text{denominator} \left( t(k)^2 + \beta - \frac{\alpha^2}{4} \right) \right) \\
= 2 \left[ \deg(\text{numerator}(t(k))) - \deg(\text{denominator}(t(k))) \right].
\]

Hence,

\[
\deg(\text{numerator}(v_n(k))) - \deg(\text{denominator}(v_n(k))) = \\
\deg(\text{numerator}(y_n(k))) - \deg(\text{denominator}(y_n(k))) \\
+ 3 \left[ \deg(\text{numerator}(t(k))) - \deg(\text{denominator}(t(k))) \right]
\]

Putting this together we get

\[
\deg(\text{numerator}(t_{n,m}(k))) - \deg(\text{denominator}(t_{n,m}(k))) \\
= \deg(\text{numerator}(t(k))) - \deg(\text{denominator}(t(k))) > 0.
\]

For any \( p, \)

\[ d_{n,m}(k) \equiv \left( t_{n,m}(k)^2 + \beta - \frac{\alpha^2}{4} \right) \cdot \frac{\beta - \frac{\alpha^2}{3}}{\frac{2}{27} \alpha^3 - \frac{\alpha \beta}{3}} \mod p. \]

If

\[ t_{n,m}(k)^2 + \beta - \frac{\alpha^2}{4} = d \cdot h(k)^2 \]
for some $d \in \mathbb{Q}$ and $h(k) \in \mathbb{Q}(t)$ then we have

$$\text{numerator}(t_{n,m}(k))^2 + \left( \beta - \frac{\alpha^2}{4} \right) \cdot \text{denominator}(t_{n,m}(k))^2 = d \cdot h_1(k)^2$$

for some $h_1(k) \in \mathbb{Q}[t]$. By what we know about the degrees of the numerator and denominator of $t_{n,m}$, the leading coefficient on the right hand side is the square of the leading coefficient of $t_{n,m}$. The leading coefficient on the left hand side is $d$ multiplied by a square. Hence $d \in \mathbb{Q}^2$.

So either

- \[ \left( t_{n,m}(k)^2 + \beta - \frac{\alpha^2}{4} \right) \cdot \frac{\beta - \frac{\alpha^2}{4}}{\frac{27}{\alpha^3 - \frac{\alpha^2}{3}}} = h(k)^2 \text{ for some } h(k) \in \mathbb{Q}(t) \text{ or} \]

- \[ \left( t_{n,m}(k)^2 + \beta - \frac{\alpha^2}{4} \right) \cdot \frac{\beta - \frac{\alpha^2}{4}}{\frac{27}{\alpha^3 - \frac{\alpha^2}{3}}} \neq h(k)^2 \text{ for any } h(k) \in \overline{\mathbb{Q}}(t) \]

Now we prove a proposition that will relate this to whether

$$\left( t_{n,m}(k)^2 + \beta - \frac{\alpha^2}{4} \right) \cdot \frac{\beta - \frac{\alpha^2}{3}}{\frac{27}{\alpha^3 - \frac{\alpha^2}{3}}}$$

is in $\mathbb{F}_p(x)^2$.

**Proposition 4.4.19.** For any polynomial $f \in \mathbb{Q}[x]$, denote by $\bar{f}_p$ the reduction of this polynomial mod $p$. Then, if $f$ is not of the form $d \cdot h(x)$ for some $d \in \mathbb{Q}$ and $h(x) \in \mathbb{Q}[x]$, then for all sufficiently large primes $p$, $f$ is not of the form $\bar{d} \cdot \bar{h}(x)^2$ for any $\bar{d} \in \mathbb{F}_p$ and $\bar{h} \in \mathbb{F}_p[x]$.

For this we use:

**Theorem 4.4.20** (Theorem 5.5.1 and Exercise 5.5.2 of [26]). Let $K$ be a number field, $p$ a (rational) prime, and $\theta \in \mathcal{O}_K$ be such that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Then, take $f$ the minimal polynomial of $\theta$ over $\mathbb{Z}[x]$. Suppose $f(x) \equiv f_1(x)^{e_1} f_2(x)^{e_2} \ldots f_g(x)^{e_g} \mod p$ where each $f_i$ is irreducible in $\mathbb{F}_p[x]$. Then $p\mathcal{O}_K = P_1^{e_1} \ldots P_g^{e_g}$, where $P_i = (p, f_i(\theta))$ are prime ideals.

**Proof of Proposition 4.4.19.** By the assumptions on $f$, there must be at least one irreducible factor of $f$ over $\mathbb{Q}$ that occurs to an odd power. Call this factor $h$ (and without loss of generality divide by the leading coefficient of this polynomial so that it can be assumed monic). Then take $\theta$ to be a root of $h$ over some splitting field. As $h$ is irreducible and monic, $h$ is then the minimal polynomial for this root. Thus, we have $f(x) = h(x)^tg(x)$, where $h$ is not a factor of $g$ (over $\mathbb{Q}$), $t$ is odd, and $g(\theta) \neq 0$ (because if $g(\theta) = 0$, by the properties of minimal polynomials, we would have $h|g$).
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

Take \( p \) a prime. Consider the factorization \( \tilde{h}(x) \equiv h_1(x)^{e_1}h_2(x)^{e_2}...h_g(x)^{e_g} \text{ mod } p \) such that each \( h_i \) is irreducible in \( \mathbb{F}_p \). If any of the \( e_i \) are even (in fact if any of the \( e_i \) bigger than one), then if \( p > [\mathcal{O}_K : \mathbb{Z}[\theta]] \), we have that \( p \) ramifies by Theorem 4.4.20 and hence \( p \mid d_K \). Thus, for sufficiently large \( p \), we have \( \tilde{h}(x)^t = h_1(x)h_2(x)...h_g(x) \text{ mod } p \), which consists of a product of irreducible factors to odd powers.

If \( \tilde{f}_p \) does not have at least one irreducible factor to an odd power, then all of the \( h_i \) must divide \( \tilde{g} \). Namely, we must have \( \tilde{g}(x) \equiv \tilde{g}(x)\tilde{h}(x) \text{ mod } p \). Then taking \( q \) a lift of \( \tilde{g} \) to \( \mathbb{Q} \), we have \( g(\theta) = q(\theta)h(\theta) + p\alpha \) where \( \alpha \in \mathbb{Z}[\theta] \). Note that we can take such \( \alpha \), as if we choose \( q \) the lift of \( \tilde{g} \) with smallest degree i.e. \( \text{deg}(q) = \text{deg}(\tilde{q}) \leq \text{deg}(g) \), then \( \text{deg}(q \cdot h) \leq \text{deg}(g) + \text{deg}(h) \leq \text{deg}(f) \), so we have \( r = g - q \cdot h \in \mathbb{Z}[x] \) of degree at most \( \text{deg}(f) \). We must have \( r(x) \equiv 0 \text{ mod } p \) for all \( x \in \mathbb{F}_p \) which, if \( p \geq \text{deg}(f) \), is impossible unless \( p \) divides all the coefficients of \( r \), thus making it the zero polynomial mod \( p \). Thus, \( r(x) = p \cdot r_0(x) \), where \( r_0(x) \) is again in \( \mathbb{Z}[x] \) and then \( \alpha = r_0(\theta) \).

Thus, \( g(\theta) \in (p, h(\theta)) = (p) \) (as \( h(\theta) = 0 \)). Namely, \( (p)|(g(\theta)) \), which only happens for finitely many primes as \( g(\theta) \neq 0 \) implies \( (g(\theta)) \neq (0) \). So, in summary, the statement of the proposition holds if

\[
p > \max\left([\mathcal{O}_K : \mathbb{Z}[\theta]], d_K, \max(\text{prime } p \text{ such that } (p)|(g(\theta)))\right). \text{deg}(f))
\]

\( \square \)

Consequently, for \( p \) sufficiently large (relative to the choice of \( \alpha \) and \( \beta \)) either

- \( d_{n,m}(k) \in \mathbb{F}_p(k)^2 \) or
- \( d_{n,m}(k) \notin \mathbb{F}_p(k)^2 \).

Following the analysis of Section 4.4.2 \( \rho \) is at most 2, and in either case \( d_{n,m}(k) \) takes quadratic residue values (as long as \( p \) is large enough so that the bound in the theorem is non-trivial), and there are points on each \( (m(nC)^*)^* \) that are fibers isomorphic to \( \tilde{E} \).

As a result, this situation satisfies the conditions of Theorem 4.4.12 so we have:

**Example 4.4.21.** Let \( \tilde{E}, E_1, \) and \( C \) as above and let \( p \) be a sufficiently large prime number. Let \( I \subset \mathbb{R} \) be an interval and let \( \epsilon > 0 \). Take \( r_0 \) to be a lower bound on the largest order of \( P(k_0) \) on its fiber mod \( p \). Choose \( k_0 \in \mathbb{Q} \) avoiding at most \( 10^7 \) exceptions. Then, there exists an \( \epsilon_1 > 0 \) depending only on \( E, C, k_0, I, \) and \( \epsilon \) such that for \( N, M \geq \max\{N(P(k_0), (1 - \epsilon_1)I, \epsilon), N(P(k_0), (1 + \epsilon_1)I, \epsilon)\} \) there exists an open set \( \mathcal{U}(k_0, N, M) \) (which depends on \( N \) and \( M \)) around \( k_0 \) such that
Chapter 4. Diffusion of candidate lifts on cross-fibered surfaces

\[
\begin{align*}
\text{Prob}_{n,m,k} & \left( (m(nP(k))^* \text{ is on a fiber } E_{t_{n,m}(k)} \ : \ n \leq N \text{ and } m \leq M \text{ are even and } k \in U(k_0, N, M) \right) > \\
& \geq \frac{m_{E(t_0)}(I)}{2} - \frac{10^8 \cdot (2\sqrt{2} + 3)^{N+M}}{\sqrt{p}} \left( m_{E(t_0)}(I) + 2\epsilon \right) \\
& \quad - 10^{10} \max \left\{ \frac{1}{N^{1/4}}, \frac{1}{M}, \frac{1}{r_0^{1/4}}, \left( \frac{4}{p} \right)^{1/16}, \left( \frac{1}{\ln \left( \frac{p}{6^{1/3}} \right) } \right)^{1/4} \right\}
\end{align*}
\]

Similar comments about \(r_0\) apply as in Example 4.4.18.
Chapter 5

Possibilities for future work

The most natural direction in which to continue these ideas would be to ask what other arithmetic properties of elliptic curves can be shown to be diffusive (on some class of elliptic fibrations). The diffusive properties that we considered in this work were motivated by lifting problems, but we could consider a wide range of other properties. For example, given an elliptic fibration $E_t$ and a prime $p$, are the sets

$$\{ t \in \mathbb{Q} : E_t \text{ is supersingular mod } p \}$$

and

$$\{ t \in \mathbb{Q} : \#E_t(\mathbb{F}_p) \text{ is composite} \}$$

either finite or dense in $\mathbb{R}$? This question is very rich because we would expect the arguments necessary to prove diffusion to vary significantly by property; yet we might still expect common elements in these proofs. For example, all of our arguments involving diffusion on cross-fibered surfaces involve, in some way or another, Diffusion Process 4.1.4 which gives a natural framework for arithmetic properties to interact with the real topology.

Moreover, it would be interesting to consider versions of Mazur’s Conjecture for elliptic surfaces (Conjecture 1.2.7) in which we have fibrations over some base other than the projective line. In general, for any curve $C$ and elliptic surface with projection $\pi : \mathcal{E} \to C$, we should be able to consider the set

$$\{ c \in C(\mathbb{Q}) : \pi^{-1}(c) = E_c, \ rk(E_c(\mathbb{Q})) \geq 1 \} .$$

Then, we can ask in what situations does one expect this set to be either finite or dense in $C(\mathbb{R})$. Specifically, we might study whether special cases, such as those studied in [24],
where one can prove such a dichotomy, exist for other choices of $C$ and whether we can reconstruct some of our diffusion results in this setting.

Finally, further study of the relationship between the ECDLP and Rank One Lifting Problem (and other related lifting problems) also has the potential to be fruitful. Improvements in our understanding of the distribution of ranks in families of elliptic curves (particularly if one could prove a sharper bound in Theorem 3.4.2) may someday be sufficient to find the lifts necessary to prove Conjecture 1.1.10. However, we might hope that some recharacterization of the properties that these lifts need to have may yet provide us with the insight necessary to find them via a more direct method.
Appendix A

Properties of the multiplication formulas on elliptic curves

We prove Lemma 4.4.3. For this we use:

Lemma A.0.1 (Lemma 2 of [14]). Let \((x_i, y_i, u_i) = [i](x_P, y_P)\), and suppose that \(x_P^3 + Ax_P + B \neq 0\). Then,

\[
x_{2i} = \frac{(3x_i^2 + A)^2}{4(x_i^3 + Ax_i + B)} - 2x_i, \quad u_{2i} = u_i \left( \frac{3x_i^2 + A}{2(x_i^3 + Ax_i + B)} (x_i - x_{2i}) - 1 \right).
\]

Furthermore, for \(x_i \neq x_P\):

\[
x_{i+1} = \frac{(x_P^3 + Ax_P + B)(u_i - 1)^2}{(x_i - x_P)^2} - x_i - x_P, \quad u_{i+1} = \frac{(u_i - 1)(x_P - x_{i+1})}{x_i - x_P} - 1.
\]

Proof of Lemma 4.4.3. We proceed by induction. For \(i = 2\): by [39] Ch. 3, Group Law Algorithm 2.3.d],

\[
x_2 = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)},
\]

which is a homogeneous polynomial of degree 4 over one of degree 3 such that the value at \(x = 1, A = 0, B = 0\) is \(\frac{1}{4} = \frac{1}{2^2}\). Further, we compute (noting that \(x_1 = x = \) and as \(y_1 = y, u_1 - 1 = 0\))

\[
u_2 - 1 = u_1 \left[ \frac{3x_1^2 + A}{2(x_1^3 + Ax_1 + B)} (x_1 - x_2) - 1 \right] - 1
\]
\[
\begin{align*}
&= \left[ \frac{3x^2 + A}{2(x^3 + Ax + B)} \left( x - \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} \right) - 1 \right] - 1 \\
&= \frac{(3x^2 + A)(3x^4 + 6Ax^2 - 4Bx + A^2) - 16(x^3 + Ax + B)^2}{8(x^3 + Ax + B)^2},
\end{align*}
\]

which is the quotient of two homogeneous polynomials of degree six and whose value at \( x = 1, A = 0, B = 0 \) is \( \frac{3 \cdot 3 - 16}{8} = \frac{1 - 2^3}{2^3} \). The largest coefficients of \( x_2 \) and \( u_2 - 1 \) are 8 and 18, respectively which are both within the stated bound.

Now we proceed with the induction step. As \( i > 2 \), we can now limit ourselves to only using the latter formula of Lemma A.0.1. Note that sum of homogeneous polynomials of the same degree is a homogeneous polynomial of that degree (or the zero polynomial), and that the product of homogeneous polynomials is a homogeneous polynomial whose degree is the product of the degrees of its factors. By keeping track of the value at \( x = 1, A = 0, B = 0 \), namely the coefficient of the \( x \) power, we will be able to avoid cases where the sum of two homogeneous polynomials is identically zero. To ease notation, when we write constant \cdot polynomial, the polynomial is homogeneous and takes the value 1 at \( x = 1, A = 0, B = 0 \). Then,

\[
x_{i+1} = \frac{(x^3 + Ax + B)(u_i - 1)^2}{(x_i - x)^2} - x_i - x
\]

\[
= \frac{(\text{degree 3 polynomial}) \left( \frac{1 - i^3}{i^2} \text{ degree } r_i \text{ polynomial} \right)^2}{\left( \frac{1}{i^2} \text{ degree } l_i \text{ polynomial} \right)^2} - \frac{1 \text{ degree } l_i + 1 \text{ polynomial}}{i^2} \text{ degree } l_i \text{ polynomial} - \text{ degree 1 poly.}
\]

\[
= \frac{(i^3 - 1)^2 \text{ degree } 2l_i + 2r_i + 3 \text{ polynomial}}{i^2(i^2 - 1)^2} - \frac{i^2 + 1 \text{ degree } l_i + 1 \text{ polynomial}}{i^2} \text{ degree } l_i \text{ polynomial}
\]

Hence the value at \( x = 1, A = 0, B = 0 \) is

\[
\frac{(i^3 - 1)^2 - (i^2 + 1)(i^2 - 1)^2}{i^2(i^2 - 1)^2} = \frac{(i - 1)^2(i^2 + i + 1)^2 - (i^2 + 1)(i - 1)^2(i + 1)}{i^2(i + 1)^2(i - 1)^2}
\]

\[
= \frac{1}{(i + 1)^2}.
\]
Appendix A. Properties of the multiplication formulas on elliptic curves

Tracking the largest coefficient at each stage and writing \(\text{coeff} \ K\) to indicate a polynomial of largest coefficient at most \(K\) (when the polynomial is written with integer coefficients in lowest terms), \(x_i\) is of the form

\[
\text{coeff} \ 1 \left( \frac{\text{coeff} \ d_i}{\text{coeff} \ c_i} \right)^2 \left( \frac{\text{coeff} \ c_i}{\text{coeff} \ c_i} \right) - \text{coeff} \ c_i - \text{coeff} \ 1 = \frac{\left( \text{coeff} \ d_i \right)^2}{\left( \text{coeff} \ c_i \right)^2} - \text{coeff} \ 2c_i
\]

\[
= \frac{\text{coeff} \ c_i^2 d_i^2}{\text{coeff} \ 4c_i^2 d_i^2} - \text{coeff} \ 2c_i
\]

\[
= \frac{\text{coeff} \ c_i^2 d_i^2 + 4c_i^3 d_i^2}{\text{coeff} \ 8c_i^3 d_i^2}.
\]

So \(c_{i+1} \leq 9c_i^3 d_i^2\).

Via a similar computation we see

\[
u_{i+1} - 1 = \frac{(u_i - 1)(x - x_{i+1})}{x_i - x} - 2
\]

\[
= \frac{1 - i^3 \text{ degree } \ell_i \text{ polynomial}}{i^3 \text{ degree } \ell_i \text{ polynomial}} \left( \text{degree 1 polynomial} - \frac{1}{(i+1)^2} \text{ degree } \ell_{i+1} \text{ polynomial} \right) - 2
\]

\[
= \frac{1 - i^3 \text{ degree } \ell_i \text{ polynomial}}{i^3 \text{ degree } \ell_i \text{ polynomial}} \left( \frac{(i+1)^2 - 1 \text{ degree } \ell_{i+1} \text{ polynomial}}{(i+1)^2} \text{ degree } \ell_{i+1} \text{ polynomial} \right) - 2
\]

\[
= \frac{(-i^3 + 1)((i + 1)^2 - 1) - 2i(i + 1)^2(1 - i^2)}{i(i + 1)^2(1 - i^2)} \text{ degree } \ell_{i+1} + \ell_i + r_i + 1 \text{ polynomial}
\]

Then,

\[
\frac{(-i^3 + 1)((i + 1)^2 - 1) - 2i(i + 1)^2(1 - i^2)}{i(i + 1)^2(1 - i^2)} = \frac{-i(i - 1)(i^2 + i + 1)(i + 2) + 2i(i + 1)^3(i - 1)}{-i(i + 1)^3(i - 1)}
\]

\[
= -i^3 - 3i^2 - 3i
\]

\[
= \frac{1 - (i + 1)^3}{(i + 1)^3},
\]

and \(u_{i+1} - 1\) is of the form

\[
\frac{\text{coeff} \ d_i}{\text{coeff} \ d_i} \left( \frac{\text{coeff} \ 1 - \text{coeff} \ c_{i+1}}{\text{coeff} \ c_i} \right) - 2 = \frac{\text{coeff} \ d_i}{\text{coeff} \ d_i} \left( \frac{\text{coeff} \ 2c_{i+1}}{\text{coeff} \ c_i} \right) - 2
\]
Appendix A. Properties of the multiplication formulas on elliptic curves

\[ \frac{\text{coeff } 2c_i c_{i+1} d_i}{\text{coeff } 2c_i c_{i+1} d_i} - 2 = \frac{\text{coeff } 2c_i c_{i+1} d_i + 4(2c_i c_{i+1} d_i)}{\text{coeff } 2c_i c_{i+1} d_i}. \]

So \( d_{i+1} \leq 6c_i c_{i+1} d_i \).

Thus, we have \( t_{i+1} \leq 3l_i + 2r_i + 2 \) and \( t_{i+1} \leq l_{i+1} + l_i + r_i + 1 \leq 4l_i + 3r_i + 3 \). (We have an inequality here because it is possible that there will be common terms in the denominator and numerator of \( x_i \) or \( r_i \) resulting in a reduction of degree.)

We consider the recursive sequences \( L_i \) and \( R_i \) satisfying

\[
L_1 = 1, \quad T_1 = 1, \quad L_{i+1} = 3L_i + 2R_i + 2 \quad \text{and} \quad T_{i+1} = 4L_i + 3R_i + 3.
\]

Upper bounds for \( L_i \) and \( R_i \) will translate into bounds for \( l_i \) and \( r_i \).

First, we show \( L_i \leq \sqrt{2}^i R_i \) and \( L_i \leq \frac{\sqrt{2} - 1}{\sqrt{2} + 2} (L_i + R_i + 1) \) for \( i > 1 \). For \( L_2 = 7 \), \( T_2 = 10 \) and these statements are true. Then for \( i > 2 \):

\[
\frac{T_{i+1} - L_{i+1}}{T_i + L_i} = \frac{L_i + R_i + 1}{4L_i + 3R_i + 3} = \frac{L_i + R_i + 1}{3(L_i + R_i + 1) + L_i} \geq \frac{L_i + R_i + 1}{(\sqrt{2} + 2)(L_i + R_i + 1)} = \frac{1}{\sqrt{2} + 2}.
\]

\[
\Rightarrow (\sqrt{2} + 2)(T_{i+1} - L_{i+1}) \geq T_{i+1} \Rightarrow L_{i+1} \leq \frac{\sqrt{2} + 1}{\sqrt{2} + 2} T_{i+1} = \frac{\sqrt{2}}{2} T_{i+1}.
\]

Then,

\[
L_{i+1} + T_{i+1} + 1 \geq L_{i+1} + \frac{1}{\sqrt{2}/2} L_{i+1} + 1 > (\sqrt{2} + 1) L_{i+1}.
\]

So

\[
L_{i+1} \leq (\sqrt{2} - 1)(L_{i+1} + T_{i+1} + 1).
\]

completing the induction.

Further, we show by induction that

\[
R_i \leq (2\sqrt{2} + 3)^{i-1} + 3 \sum_{j=0}^{i-2} (2\sqrt{2} + 3)^j
\]

for \( i \geq 4 \) For the base case, note that \( T_4 = 318 \), whereas the sum on the right hand side is about 319 for \( i = 4 \).

Then, for \( i > 4 \),

\[
T_{i+1} = 4L_i + 3R_i + 3 \leq (2\sqrt{2} + 3)R_i + 3 \quad \text{(using the inequality of above as } i > 1)\]


\[
\leq (2\sqrt{2} + 3) \left[ (2\sqrt{2} + 3)^{i-1} + 3 \sum_{j=0}^{i-2} (2\sqrt{2} + 3)^j \right] + 3 \\
= (2\sqrt{2} + 3)^i + 3 \left( \sum_{j=0}^{i-1} (2\sqrt{2} + 3)^j \right).
\]

Then, evaluating the geometric series,
\[R_i \leq (2\sqrt{2} + 3)^{i-1} + 3 \frac{(2\sqrt{2} + 3)^{i-1} - 1}{2\sqrt{2} + 2} \leq \left( 1 + \frac{3}{2\sqrt{2} + 2} \right) (2\sqrt{2} + 3)^{i-1}\]

Consequently (for \(i > 4\)),
\[L_i \leq \frac{\sqrt{2}}{2} \left( 1 + \frac{3}{2\sqrt{2} + 2} \right) (2\sqrt{2} + 3)^{i-1}.
\]

We proceed similarly for the bounds on the largest coefficient. We take the recursive sequences defined by
\[
C_2 = 8, \ D_2 = 18, \ C_{i+1} = 9C_i^3D_i^2, \ D_{i+1} = 6C_{i+1}D_i.
\]
Then \(C_i\) is then clearly an upper bound for \(c_i\), and as \(C_i \leq C_{i+1}\), \(D_i\) is an upper bound for \(d_i\). Furthermore,
\[
D_{i+1} = 6(9C_i^3D_i)^2D_i = 486C_i^6D_i^3.
\]
Note then that \(C_i \leq D_i^{2/3}\) for \(i \geq 3\) (note the bound in the statement already holds for \(i \leq 3\)) and hence \(D_{i+1} \leq 486D_i^7\).

Then, we will see by induction
\[
D_i \leq 486^{\sum_{j=0}^{i-2} 7^j} 18^{7^{i-2}}.
\]
In the base case, we have \(D_2 = 18\), so the claim holds. Using the induction hypothesis,
\[
D_{i+1} \leq 486 \left( 486^{\sum_{j=0}^{i-2} 7^j} 18^{7^{i-2}} \right)^7 = 486 \cdot 486^{\sum_{j=1}^{i-1} 7^j} 18^{7^{i-1}} = 486^{\sum_{j=0}^{i-1} 7^j} 18^{7^{i-1}}.
\]
However, \(\sum_{j=1}^{i-2} 7^j \leq 7^i\), so
\[
D_i \leq 486(486 \cdot 18)^{7^{i-2}}
\]
and
\[
C_i \leq D_i \leq 486(486 \cdot 18)^{7^{i-2}}.
\]
\[\square\]
Bibliography


