To the Graduate Council:
I am submitting herewith a dissertation written by William Coleman Bitting IV entitled "Explicit Constructions of Canonical and Absolute Minimal Degree Liftings of Twisted Edwards Curves." I have examined the final paper copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Luis Finotti, Major Professor

We have read this dissertation
and recommend its acceptance:

Marie Jameson

Shashikant Mulay

Michael Berry

Accepted for the Council:

Dixie Thompson

Vice Provost and Dean of the Graduate School

To the Graduate Council:
I am submitting herewith a dissertation written by William Coleman Bitting IV entitled "Explicit Constructions of Canonical and Absolute Minimal Degree Liftings of Twisted Edwards Curves." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Luis Finotti, Major Professor

We have read this dissertation
and recommend its acceptance:

Marie Jameson

Shashikant Mulay

Michael Berry

Accepted for the Council:

Dixie Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Explicit Constructions of Canonical and Absolute Minimal Degree Liftings of Twisted Edwards Curves

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

William Coleman Bitting IV

May 2023

Acknowledgements

I would like to thank my advisor Dr. Luis Finotti for his advice and support, as well as the love and understanding of my close friends and family. I also acknowledge the use of Magma for the computation in the dissertation.

Why, sometimes I've believed as many as six impossible things before breakfast.

-Lewis Carroll, Alice in Wonderland

Abstract

Twisted Edwards Curves are a representation of Elliptic Curves given by the solutions of $bx^2 + y^2 = 1 + ax^2y^2$. Due to their simple and unified formulas for adding distinct points and doubling, Twisted Edwards Curves have found extensive applications in fields such as cryptography. In this thesis, we study the Canonical Liftings of Twisted Edwards Curves and the associated lift of points Elliptic Teichmüller Lift. The coordinate functions of the latter are proved to be polynomials, and their degrees and derivatives are computed. Moreover, an algorithm is described for explicit computations, and some properties of the general formulas are given.

Additionally, we define a notion of Minimal and Absolute Minimal Degree Liftings modulo p^n and an associated lift of points we call an Edwards Lift. We show how the Canonical Lift may be used to find examples of Absolute Minimal Degree Liftings, at least modulo p^3.

Table of Contents

Chapter 1

Introduction

Let k be a field of characteristic $p > 2$. An **elliptic curve** E over k is said to be **ordinary** if $E[p^i] \cong \mathbb{Z}/p^i\mathbb{Z}$ for some (equivalently all) $i \geq 1$. [15, V.3.1] When E is given by

$$E/k : \qquad y^2 = f(x)$$

for a cubic polynomial f, we define the **Hasse Invariant** of E, denoted A_E, to be the coefficient of x^{p-1} in $f^{\frac{p-1}{2}}(x)$. Of note is that our elliptic curve E is ordinary if and only if $A_E \neq 0$. [15, V.4.1] It is worth noting that the given definition for the Hasse Invariant differs slightly from Silverman's as he defines the Hasse Invariant of an ordinary curve to be exactly 1. Such modifications allow us to explicitly use A_E in computations, even if its numerical value is changed by way of a birational equivalence of our elliptic curve.

Associated to an ordinary elliptic E/k, is a *unique* (up to canonical isomorphism) elliptic curve $\mathbf{E}$ over the ring of Witt Vectors over k, denoted $\mathbf{W}(k)$, whose reduction modulo p is E and for which we can lift the Frobenius map between rational points on our elliptic curves. We call $\mathbf{E}$ the **Canonical Lift of** E

Additionally, between E and $\mathbf{E}$ is a map $\tau : E(k) \to \mathbf{E}(\mathbf{W}(k))$ called the **Elliptic Teichmüller Lift** satisfying the following properties:

1) $\pi(\mathbf{E}) = E$ and $\pi \circ \tau = 1_E$.

2) If σ denotes the Frobenius map of k and $\mathbf{W}(k)$, then the canonical lift of E^σ is $\mathbf{E}^\sigma$.

3) The map τ is an injective group homomorphism.

4) Given $\phi : E \to E^\sigma$ the $p-$th power Frobenius, there exists a *Lifting of the Frobenius* $\boldsymbol{\phi} : \mathbf{E} \to \mathbf{E}^\sigma$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbf{E}(\mathbf{W}(k)) & \xrightarrow{\boldsymbol{\phi}} & \mathbf{E}^\sigma(\mathbf{W}(k)) \\ {\scriptstyle\tau}\uparrow \downarrow{\scriptstyle\pi} & & {\scriptstyle\tau}\uparrow \downarrow{\scriptstyle\pi} \\ E(k) & \xrightarrow[\phi]{} & E^\sigma(k) \end{array}$$

Thus our map is given by

$$\tau((x,y)) = (\mathbf{x},\mathbf{y}) := (x_0, y_0, x_1, y_1, ...).$$

for $x_0, x_1, ..., y_0, y_1, , ...$ entirely determined by the base point (x, y). Additionally, we can identify our curve $\mathbf{E}/\mathbf{W}(k)$ with its **Greenberg Transform**, denoted $\mathcal{G}(\mathbf{E})$, an infinite dimensional scheme over k given by the simultaneous solutions to the polynomials in the coordinates of $\mathbf{E}$. Under this identification, the Elliptic Teichmüller becomes

$$\tau((x,y)) = ((x, x_1, x_2, ...), (y, y_1, y_2, ...)).$$

In Chapter 2 we introduce the **Twisted Edwards Form** of an elliptic curve and establish properties of these curves by their relation to the **Montgomery Form**.

Importantly, we introduce an analog of the Hasse Invariant for the Twisted Edwards Form. In the process of doing so, we will demonstrate a birational equivalence between these curves and explore their underlying rings of rational functions.

In Chapters $3, 4$ we establish theoretical properties of $\mathbf{E}$ and τ, using these properties to develop an algorithm for directly computing the Canonical Lifts. Additionally, we show the developed algorithm allows for the construction of a representation of the Canonical Lift that produces modular coordinate functions that are well-defined for all pairs (a, b) yielding an ordinary elliptic curve.

Lastly, in Chapter 5, we explore an analog for **Minimal Degree Lifts** as presented in [9] for the Twisted Edwards Form and demonstrate the existence of a Minimal Degree Lift for the Twisted Edwards Form modulo p^3.

Chapter 2

A Review of Edwards Curves

2.1 General Overview

In [6], H. M. Edwards introduced a new normal form for elliptic curves over fields of characteristic different from 2 that results in simple and explicit expressions for the group law. In [2], Bernstein and Lange analyzed the efficiency of using Edwards curves on cryptographic applications, concluding that this form most often yields better results than the more usual Weierstrass equation. We summarize the main result of these two papers below and introduce yet-to-be-mentioned properties of Twisted Edwards Curves that will be important to our work

Let k be a perfect field of characteristic ≥ 3. We define the *Twisted Edwards Form* on an Elliptic Curve as follows:

Definition 2.1. For $a, b \in k^\times$ with $ab(a-b) \neq 0$ the Twisted Edwards Form of an elliptic curve is given by the solutions to the quartic equation

$$\mathcal{E}_{a,b}/k: \qquad bx^2 + y^2 = 1 + ax^2y^2.$$

As we will often need a square root for our coefficient b, rather than adopting a new symbol to express such a square root, we instead elect to use

$$E_{a,b}/k: \qquad b^2x^2 + y^2 = 1 + ax^2y^2 \tag{2.1.1}$$

though such a value for b may only exist in a quadratic extension of k.

To achieve a smooth projective model we embed $E_{a,b}$ into $\mathbb{P}_3$ via the map

$$(x, y) \mapsto [1 : x : y : xy] \tag{2.1.2}$$

and see $E_{a,b}$ as the simultaneous zeros of the projective quadratic surfaces

$$b^2X^2 + Y^2 = T^2 + aZ^2 \qquad XY = TZ.$$

The proof this yields a smooth model is A.1 in the appendix. This embedding yields four points at infinity

$$\mathcal{O}^{\pm} = (0 : 0 : \pm\sqrt{a} : 1) \qquad \mathcal{Q}^{\pm} = \left(0 : \pm\frac{\sqrt{a}}{b} : 0 : 1\right). \tag{2.1.3}$$

The order of the poles of our coordinate function at the four points at infinity on $E_{a,b}$ will be an important value for our algorithm. To compute these orders, we observe that on the curve

$$\tilde{E}_{a,b}/k \qquad b^2t^2 + u^2 = t^2u^2 + a$$

$\mathcal{O}^{\pm}$ corresponds to the point $(0, \pm\sqrt{a})$ and $\mathcal{Q}^{\pm}$ to the point $\left(\frac{\sqrt{a}}{b}, 0\right)$, where the map between the affine part of $E_{a,b}$ and this curve is given by

$$(x, y) \mapsto \left(\frac{1}{u}, \frac{1}{t}\right).$$

Note at $\mathcal{O}^+$ we have the maximal ideal is given by $M_{\mathcal{O}^+} = (t, u - \sqrt{a}.)$ Observe

$$u - \sqrt{a} = \frac{t^2(u^2 - b^2)}{u + \sqrt{a}} \implies ord_{\mathcal{O}^+}(u - \sqrt{a}) = 2ord_{\mathcal{O}^+}(t)$$

Thus

$$ord_{\mathcal{O}^+}(u - \sqrt{a}) = 2, \qquad ord_{\mathcal{O}^+}(t) = 1.$$

Similarly $ord_{\mathcal{O}^-}(u + \sqrt{a}) = 2$ and $ord_{\mathcal{O}^-}(t) = 1$. This yields

$$ord_{\mathcal{O}^+}(y) = -1 \qquad ord_{\mathcal{O}^+}(\sqrt{a}x - 1) = 2 \qquad ord_{\mathcal{O}^+}(\sqrt{a}x + 1) = 0$$

$$ord_{\mathcal{O}^-}(y) = -1 \qquad ord_{\mathcal{O}^-}(\sqrt{a}x - 1) = 0 \qquad ord_{\mathcal{O}^-}(\sqrt{a}x + 1) = 2$$

motivating the shorthand notation

$$\mathcal{O}^{\pm} = \left(\pm\frac{1}{\sqrt{a}}, \infty\right)$$

highlighting the fact $ax^2 - 1$ has a root at $\mathcal{O}^{\pm}$. Similar analysis at $\mathcal{Q}^{\pm}$ gives

$$ord_{\mathcal{Q}^+}(\sqrt{a}y - b) = 2 \qquad ord_{\mathcal{Q}^+}(\sqrt{a}y + b) = 0 \qquad ord_{\mathcal{Q}^+}(x) = -1.$$

$$ord_{\mathcal{Q}^-}(\sqrt{a}y - b) = 0 \qquad ord_{\mathcal{Q}^-}(\sqrt{a}y + b) = 2 \qquad ord_{\mathcal{Q}^-}(x) = -1$$

with analogous shorthand notation

$$\mathcal{Q}^{\pm} = \left(\infty, \pm\frac{b}{\sqrt{a}}\right)$$

highlighting that $ay^2 - b^2$ has a root at $\mathcal{Q}^{\pm}$. Details regarding uniformizers on the affine points can be found in A.2 in the appendix.

The group law associated with $E_{a,b}$ boasts the ability to add distinct points and double a general point using the same addition formula

$$x_3 = \frac{x_1y_2 + x_2y_1}{1 + ax_1x_2y_1y_2} \qquad y_3 = \frac{y_1y_2 - b^2x_1x_2}{1 - ax_1x_2y_1y_2}. \tag{2.1.4}$$

[2, 3] The identity is the affine point $(0, 1)$ and the inverse of an affine point (x, y) is $(-x, y)$. Extending to projective coordinates yields

$$(T_1, X_1, Y_1, Z_1) + (T_2, X_2, Y_2, Z_2) = (T_3, X_3, Y_3, Z_3)$$

where

$$T_3 = (T_1T_2 + aZ_1Z_2)(T_1T_2 - aZ_1Z_2) \qquad X_3 = (X_1Y_2 + X_2Y_1)(T_1T_2 - aZ_1Z_2)$$

$$Y_3 = (Y_1Y_2 - b^2X_1X_2)(T_1T_2 + aZ_1Z_2) \qquad Z_3 = (X_1Y_2 + X_2Y_1)(Y_1Y_2 - b^2X_1X_2)$$

with identity $(1, 0, 1, 0)$ and $-(T, X, Y, Z) = (T, -X, Y, -Z)$. When a is not a square in our field k, then the group law is always defined [2]. Should we prefer to use an algebraically closed field, we may resolve ill-defined additions by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{b^2x_1x_2 + y_1y_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - x_1y_1}\right) \tag{2.1.5}$$

which extends to

$$(T_1, X_1, Y_1, Z_1) + (T_2, X_2, Y_2, Z_2) = (T_3, X_3, Y_3, Z_3)$$

where

$$T_3 = \left(b^2X_1X_2 + Y_1Y_2\right)(X_1Y_2 - X_2Y_1) \qquad X_3 = (X_1Y_1 + X_2Y_2)(X_1Y_2 - X_2Y_1)$$

$$Y_3 = (X_1Y_1 - X_2Y_2)\left(b^2X_1X_2 + Y_1Y_2\right) \qquad Z_3 = (X_1Y_1 + X_2Y_2)(X_1Y_1 - X_2Y_2)$$

[3]. While this alternative addition law does allow us to resolve any affine additions the first cannot, it too has exceptional cases. Most notably, it cannot be used to double a point. That said, for all points P, Q, one of these group laws is well-defined and when both are defined, they are equal [3]

Geometrically, $P+Q$ is the inverse of the 8-th point of intersection of the conic meeting $E_{a,b}$ at $\mathcal{O}^{\pm}, \mathcal{Q}^{\pm}, P, Q, (0,-1)$, accounting for multiplicity if $P \in \{Q, (0,-1)\}$[1]. See the diagram at the end of the chapter.

We now introduce two notable affine points to which we will make frequent reference:

$$\mathcal{K}_1 = (0,-1) \qquad \mathcal{K}_2 = \left(\frac{1}{b}, 0\right).$$

From a group theoretic point-of-view, we see the involutions of affine points

$$(x,y) \mapsto (x,-y) \qquad (x,y) \mapsto \left(\frac{y}{b}, bx\right)$$

as the maps

$$P \mapsto \mathcal{K}_1 - P \qquad P \mapsto \mathcal{K}_2 - P \tag{2.1.6}$$

respectively. We give these involutions the names κ_1, κ_2, extending to the points at infinity via

$$\kappa_1(P) = \mathcal{K}_1 - P \qquad \kappa_2(P) = \mathcal{K}_2 - P.$$

This yields

$$\kappa_1((x,y)) = (x,-y) \qquad \kappa_2((x,y)) = \left(\frac{y}{b}, bx\right). \tag{2.1.7}$$

for affine points, and the extension yields

$$\kappa_1(\mathcal{O}^{\pm}) = \mathcal{O}^{\mp} \qquad \kappa_1(\mathcal{Q}^{\pm}) = \mathcal{Q}^{\mp} \qquad \kappa_2\left(\mathcal{O}^{\pm}\right) = \mathcal{Q}^{\pm} \qquad \kappa_2\left(\mathcal{Q}^{\pm}\right) = \mathcal{O}^{\pm} \tag{2.1.8}$$

for the points at infinity. We conclude the section by detailing the properties and relations of our notable points, namely

$$|\mathcal{K}_1| = 2 \qquad |\mathcal{K}_2| = 4 \qquad \left|\mathcal{O}^{\pm}\right| = 4 \qquad \left|\mathcal{Q}^{\pm}\right| = 2 \tag{2.1.9}$$

$$2\mathcal{O}^{\pm} = \mathcal{K}_1 \qquad 2\mathcal{K}_2 = \mathcal{K}_1 \qquad \mathcal{O}^{\pm} + \mathcal{O}^{\mp} \qquad \mathcal{O}^{+} + \mathcal{Q}^{\pm} = \mathcal{K}_2 \tag{2.1.10}$$

2.2 Equivalence to Montgomery Form: Computing the j and Hasse Invariants

Recall the *Montgomery Form* on an elliptic curve is given by

$$M_{A,B}/k: \qquad Bu^2 = t^3 + At^2 + t. \tag{2.1.11}$$

with $B(A^2-4) \neq 0$ [4]. Every Twisted Edwards Curve is birationally equivalent to an elliptic curve in Montgomery Form. Specifically, taking $A = 2\frac{b^2+a}{b^2-a}$ and $B = \frac{4}{b^2-a}$ then there is a birational equivalence between $E_{a,b}$ and $M_{A,B}$ given by

$$(x,y) \mapsto \left(\frac{1+y}{1-y}, \frac{1+y}{x(1-y)}\right)$$

with inverse

$$(t,u) \mapsto \left(\frac{t}{u}, \frac{t-1}{t+1}\right).$$

The details of this equivalence are found in A.3 in the appendix. It is known the $j-$invariant of $M_{A,B}$ is given by

$$j(M_{A,B}) = \frac{256(A^2-3)^3}{A^2-4} \tag{2.1.12}$$

[4, 2.1] thus evaluting $A = 2\frac{b^2+a}{b^2-a}$, we find the j-invariant of $E_{a,b}$ is

$$j(E_{a,b}) = \frac{16(a^2+14ab^2+b^4)^3}{ab^2(a-b^2)^4}. \tag{2.1.13}$$

Since every elliptic curve over an algebraically closed field of characteristic not equal to $2,3$ is birationally equivalent to a curve in the Montgomery Form [4, Section 2.4], any elliptic curve over an algebraically closed field can be made into the Twisted Edwards Form.

To compute the analog of the Hasse Invariant for our curve, we let $\mathcal{C}$ be the Cartier Operator. For $M_{A,B}$

$$\mathcal{C}\left(\frac{dt}{u}\right) = A_M^{1/p}\frac{dt}{u}$$

where A_M is the Hasse Invariant of $M_{A,B}$. From our birational equivalence we find

$$\frac{dt(x,y)}{u(x,y)} = \frac{2xdy}{1-y^2}.$$

Thus we check for ordinariness of $E_{a,b}$ via

$$\begin{aligned} A_M^{1/p}\frac{2xdy}{1-y^2} = \mathcal{C}\left(\frac{2xdy}{1-y^2}\right) &= \frac{2x}{1-y^2}\cdot\mathcal{C}\left(\frac{(1-y^2)^{p-1}dy}{(x^2)^{\frac{p-1}{2}}}\right) \\ &= \frac{2x}{1-y^2}\cdot\mathcal{C}\left(\left((1-y^2)(b^2-ay^2)\right)^{\frac{p-1}{2}}dy\right). \end{aligned}$$

Since $(1-y^2)(b^2-ay^2)$ has degree 4, it follows

$$\mathcal{C}\left(\left((1-y^2)(b^2-ay^2)\right)^{\frac{p-1}{2}}dy\right) = A_E^{1/p}dy$$

where A_E is the coefficient of y^{p-1} in $\left((1-y^2)(b^2-ay^2)\right)^{\frac{p-1}{2}}$. This yields the equality

$$A_M^{1/p}\frac{2xdy}{1-y^2} = A_E^{1/p}\frac{2xdy}{1-y^2} \implies A_M = A_E,$$

showing our curve is ordinary if and only if $A_E \neq 0$. We will henceforth refer to A_E as the Hasse Invariant of $E_{a,b}$ (with the subscripts a, b assumed to be understood).

Continuing with our computations involving differentials, we find

$$2b^2x \cdot dx + 2y \cdot dy = 2ax^2y \cdot dy + 2axy^2 \cdot dx.$$

which can be rearranged as

$$2x\left(b^2-ay^2\right)\cdot dx = 2y\left(ax^2-1\right)\cdot dy.$$

Observe

$$b^2-ay^2 = \frac{1-y^2}{x^2}, \qquad ax^2-1 = \frac{b^2x^2-1}{y^2}.$$

Thus

$$\frac{2(1-y^2)dx}{x} = \frac{2(b^2x^2-1)dy}{y} \implies \frac{2ydx}{b^2x^2-1} = \frac{2xdy}{1-y^2}. \tag{2.1.14}$$

2.3 Properties of $k\left(E_{a,b}\right)$

We now explore properties of the function field of our Twisted Edwards Curve, beginning with its ring of regular functions.

Theorem 2.2. *Let $f \in k[E_{a,b}]$. There exist rational functions $\phi, \psi \in k(t)$ (for place-holder variable t) such that*

$$f = \phi(x) + y\psi(x).$$

Proof. Expand f as

$$\begin{aligned}\sum_{i=0}^{d}\sum_{j=0}^{e} a_{i,j}x^i y^j &= \sum_{i=0}^{d}\sum_{j=0}^{\lfloor \frac{e}{2} \rfloor} a_{i,j}x^i \left(y^{2j} + y^{2j+1}\right) \\ &= \sum_{i=0}^{d}\sum_{j=0}^{\lfloor \frac{e}{2} \rfloor} a_{i,j}x^i (1+y) \left(\frac{1-bx^2}{1-ax^2}\right)^j\end{aligned}$$

□

Corollary 2.3. *Let $f \in k[E_{a,b}]$. There exist rational functions $\phi, \psi \in k(t)$ such that*

$$f = \phi(y) + x\psi(y).$$

Proof. The argumentation is analogous to our previous theorem. □

Corollary 2.4. *Let $f/g \in k(E_{a,b})$. Then there exist rational functions $\phi, \psi \in k(t)$ such that*

$$f/g = \phi(x) + y\psi(x)$$

Proof. Write $f = \frac{\phi_1(x)}{\phi_2(x)} + y\frac{\psi_1(x)}{\psi_2(x)}$ and $g = \frac{\Phi_1(x)}{\Phi_2(x)} + y\frac{\Psi_1(x)}{\Psi_2(x)}$. Then we have

$$\begin{aligned}
\frac{f}{g} &= \frac{\frac{\phi_1(x)}{\phi_2(x)} + y\frac{\psi_1(x)}{\psi_2(x)}}{\frac{\Phi_1(x)}{\Phi_2(x)} + y\frac{\Psi_1(x)}{\Psi_2(x)}} \\
&= \frac{\left(\frac{\phi_1(x)}{\phi_2(x)} + y\frac{\psi_1(x)}{\psi_2(x)}\right)\left(\frac{\Phi_1(x)}{\Phi_2(x)} - y\frac{\Psi_1(x)}{\Psi_2(x)}\right)}{\frac{\Phi_1(x)^2}{\Phi_2(x)^2} - y^2\frac{\Psi_1(x)^2}{\Psi_2(x)^2}} \\
&= \frac{\frac{\phi_1(x)}{\phi_2(x)}\frac{\Phi_1(x)}{\Phi_2(x)} + y\left(\frac{\Phi_1(x)}{\Phi_2(x)}\frac{\psi_1(x)}{\psi_2(x)} - \frac{\phi_1(x)}{\phi_2(x)}\frac{\Psi_1(x)}{\Psi_2(x)}\right) - y^2\frac{\psi_1(x)}{\psi_2(x)}\frac{\Psi_1(x)}{\Psi_2(x)}}{\frac{\Phi_1(x)^2}{\Phi_2(x)^2} - y^2\frac{\Psi_1(x)^2}{\Psi_2(x)^2}} \\
&= \frac{\frac{\phi_1(x)}{\phi_2(x)}\frac{\Phi_1(x)}{\Phi_2(x)} + y\left(\frac{\Phi_1(x)}{\Phi_2(x)}\frac{\psi_1(x)}{\psi_2(x)} - \frac{\phi_1(x)}{\phi_2(x)}\frac{\Psi_1(x)}{\Psi_2(x)}\right) - \left(\frac{1-b^2x^2}{1-ax^2}\right)\frac{\psi_1(x)}{\psi_2(x)}\frac{\Psi_1(x)}{\Psi_2(x)}}{\frac{\Phi_1(x)^2}{\Phi_2(x)^2} - \left(\frac{1-b^2x^2}{1-ax^2}\right)\frac{\Psi_1(x)^2}{\Psi_2(x)^2}}
\end{aligned}$$

The desired result follows by clearing the nested denominators of the rational expressions in the numerator and denominator. □

Corollary 2.5. *Let $f/g \in k(E_{a,b})$ There exist rational functions $\phi, \psi \in k(t)$ such that*

$$f/g = \phi(y) + x\psi(y)$$

Proof. Argumentation is analogous to the above. □

Theorem 2.6. *Let $f \in k[E_{a,b}]$. There exist polynomials ϕ, ψ, Φ, Ψ such that*

$$f = \phi(x) + \psi(y) + y\Phi(x) + x\Psi(y).$$

Moreover, if one insists

$$\psi(0) = \Phi(0) = \Psi(0) = \Psi'(0) = 0$$

then this decomposition is unique.

Proof. Expand f as

$$f = \sum_{i=0}^{d}\sum_{j=0}^{e} a_{i,j}x^i y^j.$$

Define

$$\phi_0(x) := \sum_{i=0}^{d} a_{i,0}x^i \qquad \psi_0(y) := \sum_{j=0}^{e} a_{0,j}y^j - a_{0,0}.$$

Then

$$f = \phi_0(x) + \psi_0(y) + \sum_{i=1}^{d}\sum_{j=1}^{e} a_{i,j}x^i y^j.$$

Continuing like this, we define

$$\Phi_0 := \sum_{i=1}^{d} a_{i,1}x^i \qquad \Psi_0 := \sum_{j=1}^{e} a_{1,j}y^j - a_{1,1}y$$

and see

$$\begin{aligned} f &= \phi_0(x) + \psi_0(y) + y\Phi_0(x) + x\Psi_0(y) + \sum_{i=2}^{d}\sum_{j=2}^{e} a_{i,j}x^i y^j \\ &= \phi_0(x) + \psi_0(y) + y\Phi_0(x) + x\Psi_0(y) + x^2y^2\sum_{i=0}^{d-2}\sum_{j=0}^{e-2} a_{i+2,j+2}x^i y^j. \end{aligned}$$

from which we find

$$\begin{aligned} f &= \phi_0(x) + \psi_0(y) + y\Phi_0(x) + x\Psi_0(y) + \frac{b^2x^2 + y^2 - 1}{a}\sum_{i=0}^{d-2}\sum_{j=0}^{e-2} a_{i+2,j+2}x^i y^j \\ &= \phi_0(x) + \psi_0(y) + y\Phi_0(x) + x\Psi_0(y) + \frac{b^2}{a}\sum_{i=0}^{d}\sum_{j=0}^{e-2} a_{i,j+2}x^i y^j + \frac{1}{a}\sum_{i=0}^{d-2}\sum_{j=0}^{e} a_{i+2,j}x^i y^j \\ &\qquad + \frac{1}{a}\sum_{i=0}^{d-2}\sum_{j=0}^{e-2} a_{i+2,j+2}x^i y^j. \end{aligned}$$

Note the total degree on each of the summations has decreased. Thus after finitely many repetitions, we arrive at the desired result.

To see the added conditions give a unique decomposition, assume for a contradiction we have two distinct representations. Subtracting one representation from the other,

we find their difference must be of the form

$$\begin{aligned}\phi(x) + \psi(y) + y\Phi(x) + x\Psi(y) &= (b^2x^2 + y^2 - 1 - ax^2y^2) \cdot h \\ &= y^2(1 - ax^2)h + (b^2x^2 - 1)h,\end{aligned}$$

for some $h \in k[x, y]$. If $h \neq 0$, let $cx^k y^l$ be a monomial of h with maximal degree on y. Then, we would necessarily have the term on $acx^{k+2}y^{l+2}$ on the left side of the equation, which contradicts the fact that the left-hand side has no monomial with both $x-$degree and $y-$degree greater than 1. □

While this third decomposition is the least used of the three, it has the distinguishing trait of preserving polynomials and thus is how computer algebra systems perform the arithmetic associated with $E_{a,b}$.

2.4 Decomposing Even Functions

Consider the ring $R_{\alpha,\beta} := k[t, s]/(\beta t + s - 1 - \alpha ts)$ where $\alpha, \beta \in k$ are such that $\alpha\beta(\alpha - \beta) \neq 0$. We dedicate this section to the proof of the following theorem.

Theorem 2.7. *$R_{\alpha,\beta}$ is the k vector space generated by $\{1, t, s, t^2, s^2, ...\}$.*

To prove this, we show the following:

Proposition 2.8. *Let $P, Q \in k[z]$. Then there exist polynomials $F, G \in k[z]$ with $\deg(F) \leq \deg(P)$ and $\deg(G) \leq \deg(Q)$ such that*

$$P(t)Q(s) = F(t) + G(s).$$

Proof. We prove this by induction on n, the sum of the degrees of P and Q, seeing it is clearly true for $n = 0$ as the product of constant functions can clearly be written as the sum of constant functions. Further, if one of $\deg(P), \deg(Q) = 0$, then the result follows as the scaling a polynomial by a constant can be written as the sum of

a polynomial and a constant. Thus we assume both $\deg(P), \deg(Q)$ are positive. Let $\ell + m = n + 1$ with $\deg(P) = \ell > 0, \deg(Q) = m > 0$. Write

$$\begin{aligned}
P(t)Q(s) &= \sum_{i=0}^{\ell}\sum_{j=0}^{m} \delta_i \epsilon_j t^i s^j \\
&= \delta_0\epsilon_0 + \delta_1\epsilon_0 t + \delta_0\epsilon_1 s + ts\sum_{i=1}^{\ell}\sum_{j=1}^{m} \delta_i \epsilon_j t^{i-1} s^{j-1} \\
&= \delta_0\epsilon_0 + \delta_1\epsilon_0 t + \delta_0\epsilon_1 s + \frac{1}{\alpha}\sum_{i=1}^{\ell}\sum_{j=1}^{m} \delta_i \epsilon_j \left(\beta^2 t^i s^{j-1} + t^{i-1}s^j - t^{i-1}s^{j-1}\right) \\
&= \delta_0\epsilon_0 + \delta_1\epsilon_0 t + \delta_0\epsilon_1 s + P_1(t)Q_1(s) + P_2(t)Q_2(s) - P_3(t)Q_3(s) \\
&= \delta_0\epsilon_0 + \delta_1\epsilon_0 t + \delta_0\epsilon_1 s + (F_1(t) + F_2(t) - F_3(t)) + (G_1(s) + G_2(s) - G_3(s))
\end{aligned}$$

Observe by the induction hypothesis, $\deg(F_2), \deg(F_3) \leq \ell - 1$ and $\deg(F_1) \leq \ell$ and $\deg(G_2), \deg(G_3) \leq m-1$ and $\deg(G_1) \leq m$ thus we have written $P(t)Q(s)$ as the sum of polynomials $F(t) + G(s)$ with $\deg(F) \leq \ell = \deg(P)$ and $\deg(G) \leq m = \deg(Q)$, proving the desired result. □

Corollary 2.9. *Every element of $R_{\alpha,\beta}$ can be written as $F(t) + G(s)$.*

Note this implies the stated theorem. Appealing to the embedding $(t, s) \mapsto (x^2, y^2)$, we find an important result for $E_{a,b}$:

Corollary 2.10. *Any product $P(x^2)Q(y^2)$ in $k[E_{a,b}]$ can be written as a sum $F(x^2) + G(y^2)$ with $F, G \in k[t]$ and $\deg(F) \leq \deg(P)$ and $\deg(G) \leq \deg(Q)$.*

For $i, j \geq 1$, define $L(i, j) \subset R_{\alpha,\beta}$ to be the $k-$ vector space of generated by $\{1, t, ..., t^i, s, ..., s^j\}$.

Lemma 2.11. *$dim_k\left(L(i, j)\right) = i + j + 1$.*

Proof. Observe that any linear combination of powers of t, s can be written as

$$F(t) + G(s)$$

for polynomials F, G such that $G(0) = 0$. To see that the sum of these polynomials cannot be 0, observe this would mean that there exists $H(t, s) \in k[t, s]$ such that

$$F(t) + G(s) = (\beta t + s - 1 - \alpha ts)H(t, s)$$

But unless $H = 0$, there will be a term in ts on the right-hand side, but none on the left-hand side. This cannot be, so it must be the case that the set $\{1, t, ..., t^i, s, ..., s^j\}$ is linearly independent, and thus $dim_k\,(L(i, j)) = i + j + 1$. □

Theorem 2.12. *Let $A \in L(i, j)$, $B \in L(m, n)$ and $C \in L(d, e)$ be such that $1 \in (A, B)$. Define $r := \max\{d, m + i\}$ and $q := \max\{e, n + j\}$. There exists $u \in L(m, q - j)$ and $v \in L(r - m, j)$ such that*

$$Au + Bv = C.$$

Proof. Consider the $k-$linear map $\psi : L(m, q - j) \oplus L(r - m, j) \to L(r, q)$ by

$$\psi(u, v) = Au + Bv.$$

While $\gcd(A, B)$ need not be well defined *in general*, the condition that $1 \in (A, B)$ guarantees that $(A) \cap (B) = (AB)$, thus it follows

$$\psi(u, v) = 0$$

if and only if $u = Bz$ and $v = -Az$ for some $z \in V$. Write $-A = F(t) + G(s)$, $B = H(t) + I(s)$, and $z = P(t) + Q(s)$. This gives the equities

$$u = H(t)P(t) + P(t)I(s) + H(t)Q(s) + I(s)Q(s)$$

$$v = F(t)P(t) + F(t)Q(s) + P(t)G(s) + G(s)Q(s).$$

Then $m \geq \deg(H) + \deg(P) = m + \deg(P) \implies \deg(P) = 0$ and $j \geq \deg(G) + \deg(Q) = j + \deg(Q) \implies \deg(Q) = 0$. Thus z is a constant polynomial so

$\ker \psi = span\{(1,-1)\}$. Thus the image of ψ has dimension $q+r+1$, proving ψ is surjective as its image has the same dimension as the co-domain. $\square$

2.5 Edwards Isogenies

Assume we have two Twisted Edward Curves

$$b^2x^2 + y^2 = 1 + ax^2y^2 \qquad (b')^2(x')^2 + (y')^2 = 1 + (a')(x')^2(y')^2$$

We define a **Edwards Isogeny** to be an isogeny of elliptic curves $(x,y) \mapsto (x',y')$ that also fixes $\mathcal{O}^{\pm}, \mathcal{Q}^{\pm}$. This need not be all possible isogenies, as the map $(x,y) \mapsto (x,y^{-1})$ is an isogeny between $E_{a,b}$ and $E_{b^2,\sqrt{a}}$ not fixing the points at infinity. We now introduce the following theorem:

Theorem 2.13. *Let $\phi : E_{a,b} \to E_{a',b'}$ be an Edwards Isogeny. Then there exists some $\alpha \in k^{\times}$ such that*

$$\phi(x,y) = (\alpha x, y) \qquad a' = \frac{a}{\alpha^2} \qquad b' = \frac{b}{\alpha}.$$

Proof. Consider the divisors

$$D_1 := \mathcal{O}^+ + \mathcal{O}^- \qquad D_2 := \mathcal{Q}^+ + \mathcal{Q}^-. \tag{2.13.1}$$

By the Riemann-Roch Theorem, we have

$$\ell(D_1) = 2 \qquad \ell(D_2) = 2$$

so we acquire two bases for $\mathcal{L}(D_1), \mathcal{L}(D_2)$ given by

$$\{1, x\} \qquad \{1, x'\}$$

for $\mathcal{L}(D_1)$ and

$$\{1, y\} \qquad \{1y'\}$$

for $\mathcal{L}(D_2)$. Thus there must be scalars $\alpha_0, \alpha_1, \beta_0, \beta_1$ such that

$$x' = \alpha_0 + \alpha_1 x \qquad y' = \beta_0 + \beta_1 y.$$

from which we see

$$(b')^2(\alpha_0 + \alpha_1 x)^2 + (\beta_0 + \beta_1 y)^2 = 1 + a'(\alpha_0 + \alpha_1 x)^2(\beta_0 + \beta_1 y)^2.$$

Expanding our terms yields

$$\begin{aligned}
&(b')^2(\alpha_0^2 + 2\alpha_0\alpha_1 x + \alpha_1^2 x^2) + (\beta_0^2 + 2\beta_0\beta_1 y + \beta_1 y^2) \\
=&1 + a'(\alpha_1^2\beta_1^2 x^2 y^2 + 2\alpha_1^2\beta_0\beta_1 x^2 y + \alpha_1^2\beta_0^2 x^2 + 2\alpha_1\alpha_0\beta_1^2 xy^2 \\
&+4\alpha_1\alpha_0\beta_0\beta_1 xy + 2\alpha_1\alpha_0\beta_0^2 x + \alpha_0^2\beta_1^2 y^2 + 2\alpha_0^2\beta_0\beta_1 y + \alpha_0^2\beta_0^2).
\end{aligned}$$

The term x^2y^2 on the right-hand side can be resolved as

$$\frac{\alpha_1^2\beta_1^2}{a}(b^2x^2 + y^2 - 1)$$

so we may appropriately compare terms across the equal sign.

The left-hand side has no term in x^2y, xy, or xy^2 thus

$$2\alpha_1^2\beta_0\beta_1 = 2\alpha_1\alpha_0\beta_1^2 = 4\alpha_1\alpha_0\beta_1\beta_0 = 0.$$

Since x', y' are not constant functions we see $\alpha_1, \beta_1 \neq 0$, and since our field does not have characteristic 2 we find $\alpha_0 = \beta_0 = 0$. Thus

$$x' = \alpha_1 x \qquad y' = \beta_1 y.$$

Since our map is an isogeny, we require $(0,1) \mapsto (0,1)$, so $\beta_1 = 1$. The map $(x,y) \mapsto (\alpha x, y)$ clearly preserves the Twisted Edward form, we find all Edwards Isogenies must be given

$$(x,y) \mapsto (\alpha x, y) \tag{2.13.2}$$

with an associated change in coefficients

$$(a,b) \mapsto \left(\frac{a}{\alpha^2}, \frac{b}{\alpha}\right). \tag{2.13.3}$$

□

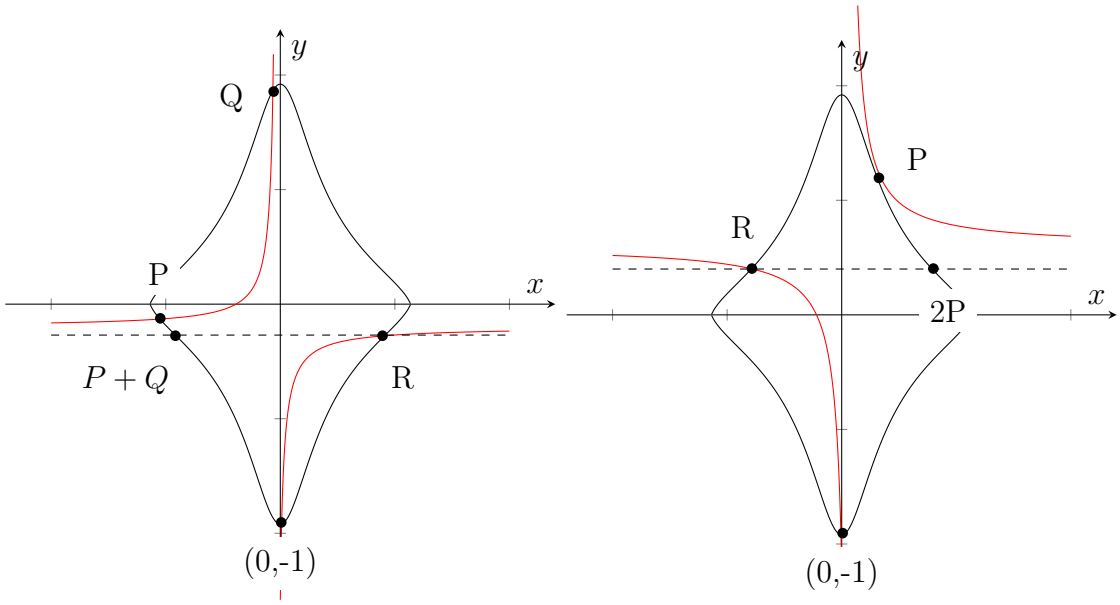

Figure 2.13.1: Addition and Doubling

Chapter 3

Witt Vectors and The Greenberg Transform

3.1 Witt Vectors

Let p be an odd prime and k a field of characteristic p. We begin our introduction to the ring of Witt vectors with three infinite sequences of polynomials.

Definition 3.1. Let $n \in \mathbb{N}$. Then we define *the n-th Witt Polynomial*

$$W_n(x_0, x_1, ..., x_n) := \sum_{i=0}^{n} p^i x_i^{p^{n-i}}.$$

Additionally, for each n, there exists $S_n, P_n \in \mathbb{Z}[x_0, y_0, x_1, y_1, ..., x_n, y_n]$, respectively called the *Summation Polynomials* and *Product Polynomials* such that

$$W_n(S_0(x_0, y_0), ..., S_n(x_0, y_0, .., x_n, y_n)) = W_n(x_0, .., x_n) + W_n(y_0, .., y_n)$$

$$W_n(P_0(x_0, y_0), ..., P_n(x_0, y_0, .., x_n, y_n)) = W_n(x_0, .., x_n) \cdot W_n(y_0, .., y_n).$$

More explicitly, we may write

$$S_n = x_n + y_n + \sum_{i=1}^{n} \frac{1}{p^i} \left(x_{n-i}^{p^i} + y_{n-i}^{p^i} - S_{n-i}^{p^i} \right)$$

and

$$\begin{aligned} P_n &= \frac{1}{p^n} \left(\sum_{i=0}^{n} \sum_{\ell=0}^{n} p^{i+\ell} x_i^{p^{n-i}} y_\ell^{p^{n-\ell}} - \sum_{m=0}^{n-1} p^m P_m^{p^{n-m}} \right) \\ &= \sum_{i=0}^{n} \sum_{\ell=0}^{n-i} \frac{1}{p^i} \left(x_\ell^{p^{n-\ell}} y_{n-i-\ell}^{p^{i+\ell}} \right) - \sum_{i=0}^{n-1} \frac{1}{p^i} P_i^{p^{n-i}} + p\,(...) \end{aligned}$$

Clearly, $S_n, P_n \in \mathbb{Q}[x_0, y_0, ..., x_n, y_n]$, but enough cancellation occurs so $S_n, P_n \in \mathbb{Z}[x_0, y_0, ..., x_n, y_n]$ (see [14] or [13]). To minimize the number of variables we need to express, we introduce the following shorthand:

Let $\mathbf{a} = (a_0, a_1, ...)$ and $\mathbf{b} = (b_0, b_1, ...)$. Then we say

$$S_n(\mathbf{a}, \mathbf{b}) := S_n(a_0, b_0, ..., a_n, b_n) \qquad P_n(\mathbf{a}, \mathbf{b}) := P_n(a_0, b_0, ..., a_n, b_n).$$

Definition 3.2. We define the ring of Witt Vectors over k to be the countable product

$$\mathbf{W}(k) := \prod_{n=0}^{\infty} k$$

with addition and multiplication to be defined by

$$\mathbf{a} + \mathbf{b} = (S_0(\mathbf{a}, \mathbf{b}), S_1(\mathbf{a}, \mathbf{b}), ...) \qquad \mathbf{a} \cdot \mathbf{b} = (P_0(a_0, b_0), P_1(\mathbf{a}, \mathbf{b}), ...)\,. \tag{3.2.1}$$

This yields a ring of charecteristic 0 with additiive identity $(0, 0, ...)$ and multiplicative identity $(1, 0, ...)$.

Note since each coordinate of the Witt Vector exists in characteristic p, we

may use the reductions modulo p of S_n, P_n to compute the coordinates. Denote these reductions as $\bar{S}_n, \bar{P}_n$ respectively with similar shorthand to the above for $\bar{S}_n(\mathbf{a}, \mathbf{b}), \bar{P}_n(\mathbf{a}, \mathbf{b})$.

Example: Let $k = \mathbb{F}_7$, $\mathbf{x} = (3, 1, ...)$, and $\mathbf{y} = (2, 5, ...)$. Through computation, we see that we have

$$S_0 = X_0 + Y_0 \qquad P_0 = X_0 Y_0$$

$$S_1 = X_1 + Y_1 - \sum_{n=1}^{6} \frac{6!}{n!(7-n)!} X_0^n Y_0^{7-n}$$

$$P_1 = X_0^7 Y_1 + X_1 Y_0^7 + 7X_1 Y_1$$

Thus

$$\mathbf{x} + \mathbf{y} = (5, 0, ...)$$

$$\mathbf{xy} = (6, 3, ...).$$

3.2 The Greenberg Transform

Definition 3.3. Consider a curve given by

$$\mathbf{C}/\mathbf{W}(k): \quad \mathbf{f}(\mathbf{x}, \mathbf{y}) = \mathbf{0}.$$

Associated to $\mathbf{C}$ is an equality of Witt Vectors

$$\mathbf{f}((x_0, x_1, ...), (y_0, y_1, ...)) = (0, 0, ...)$$

found by the evaluation map $\mathbf{x} = (x_0, x_1, ...), \mathbf{y} = (y_0, y_1, ...)$. We call the simultaneous solutions to this equality *The Greenberg Transform of* $\mathbf{C}$ and denote it $\mathcal{G}(\mathbf{C})$

Example: We may see the curve $(2,1,...)\mathbf{x}^2+(1,3,...)\mathbf{y}^2-\mathbf{1}=\mathbf{0}$ as the simultaneous solutions to

$$(2x_0^2+y_0^2, x_0^6+2x_0^4y_0^2+x_0^3x_1+x_0^2y_0^4+2y_0^3y_1,...)-(1,0,....)=(0,0,...)$$

Lemma 3.4. *For* $\mathbf{g}\in\mathbf{W}(k)[\mathbf{x},\mathbf{y}]$ *having Greenberg Transform*

$$\mathcal{G}(\mathbf{g})=(g_0,g_1,....)$$

the $n+1st$ *entry of* $\mathcal{G}(\mathbf{g})$ *is given by*

$$g_n=x_n\left(\frac{\partial g_0}{dx_0}\right)^{p^n}+y_n\left(\frac{\partial g_0}{dx_0}\right)^{p^n}+... \tag{3.4.1}$$

where omitted terms are polynomials in $k[x_0,..,x_{n-1},y_0,..,y_{n-1}]$.

This is Lemma 7.4 in [7]

3.3 The Canonical Lift

Recall an elliptic curve E/k over a field of characteristic $p\neq 0$ is called *ordinary* if the following equivalent conditions hold:

i) $A_E\neq 0$, where A_E is the Hasse Invariant of E/k.

ii) $E[p^r]\cong\mathbb{Z}/p^r\mathbb{Z}$ for some (all) $r\geq 1$.

[15, V.3.1] Associated with an ordinary elliptic curve E, is a unique (up to isomorphism) elliptic curve $\mathbf{E}/\mathbf{W}(k)$ called the *Canonical Lift of* E and a map $\tau: E(\bar{k})\to\mathbf{E}\left(\mathbf{W}(\bar{k})\right)$ called the *Elliptic Teichmüller lift*, characterized by the following properties:

1) $\pi(\mathbf{E})=E$ and $\pi\circ\tau=1_E$.

2) If σ denotes the Frobenius map of k and $\mathbf{W}(k)$, then the canonical lift of E^σ is $\mathbf{E}^\sigma$.

3) The map τ is an injective group homomorphism.

4) Given $\phi : E \to E^\sigma$ the $p-$th power Frobenius, there exists a *Lifting of the Frobenius* $\boldsymbol{\phi} : \mathbf{E} \to \mathbf{E}^\sigma$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbf{E}\left(\mathbf{W}(k)\right) & \xrightarrow{\boldsymbol{\phi}} & \mathbf{E}^\sigma\left(\mathbf{W}(k)\right) \\ {\scriptstyle\tau}\uparrow \downarrow{\scriptstyle\pi} & & {\scriptstyle\tau}\uparrow \downarrow{\scriptstyle\pi} \\ E(k) & \xrightarrow[\phi]{} & E^\sigma(k) \end{array}$$

We will frequently identify $\mathbf{E}/\mathbf{W}(k)$ with its Greenberg transform $\mathcal{G}(\mathbf{E})/k$, viewing τ as a morphism of schemes over k

$$\tau((x_0, y_0)) = (\mathbf{x}, \mathbf{y}) = ((x_0, x_1, x_2, ...), (y_0, y_1, y_2, ...)) \tag{3.4.2}$$

where, in general, $x_n, y_n \in k(x_0, y_0)$. [5][11]

Chapter 4

The Canonical Lift of Twisted Edwards Curves

4.1 Properties of x_n, y_n

Our goal throughout this section is to establish the basic properties of the coordinates of τ. Doing so will inform us of what requirements we will need to insist our algorithm meets, and thus provide guidance on how to create such an algorithm. We begin with the following theorem:

Theorem 4.1. *Fix a Twisted Edwards Curve E_{a_0,b_0} and its Canonical Lift $\mathbf{E_{a,b}}$ given by*

$$\mathbf{E_{a,b}}/\mathbf{W}(k): \qquad \mathbf{b}^2\mathbf{x}^2 + \mathbf{y}^2 = \mathbf{1} + \mathbf{a}\mathbf{x}^2\mathbf{y}^2$$

where $\mathbf{a} = (a_0, a_1, ...), \mathbf{b} = (b_0, b_1, ...)$. Let τ be the Teichmüller Lift sending a point $P = (x_0, y_0)$ to a point $\mathbf{P} = (\mathbf{x}, \mathbf{y}) = ((x_0, x_1, ...), (y_0, y_1, ...))$. Then for all n

$$x_n \in k[x_0] \qquad y_n \in k[y_0]$$

and are odd functions.

Proof. To begin by decomposing y_n as

$$y_n = \frac{f_1(y_0)}{f_2(y_0)} + x_0 \cdot \frac{g_1(y_0)}{g_2(y_0)}$$

using Corollary (2.5). Since $\tau(-P) = -\tau(P)$ it follows

$$\begin{aligned}
\tau((-x_0, y_0)) &= -\tau((x_0, y_0)) \\
&= -((x_0, x_1, ...), (y_0, y_1, ...)) \\
&= (-(x_0, x_1, ...), (y_0, y_1, ...)) \\
&= ((-x_0, -x_1, ...), (y_0, y_1, ...))
\end{aligned}$$

where we have used the fact that for $p \geq 3$, the negation of a Witt Vector is the Witt Vector of the negations of each component. Thus

$$y_n(x_0, y_0) = y_n(-x_0, y_0)$$

for all x_0, which yields

$$\frac{g_1(y_0)}{g_2(y_0)} = 0.$$

As such, y_n is a rational expression purely in y_0.

Since y_n is regular away from the points $\mathcal{O}^{\pm}$, it follows that the denominator can only have roots at $\mathcal{O}^{\pm}$. But any non-constant polynomial in y_0 has poles at $\mathcal{O}^{\pm}$, thus it must be the case that $g_2(y_0) \in k^{\times}$, so $y_n \in k[y_0]$.

To see the analog result for x_n, recall that the involution $(x_0, y_0) \mapsto (x_0, -y_0)$ can be given group-theoretically as

$$P \mapsto (0, -1) - P.$$

Since τ is an injective group homomorphism and a section of the reduction modulo p map, it follows that

$$\tau(0,-1) = (\mathbf{0},-\mathbf{1})$$

as both are the sole affine point of order 2 in their respective groups. Thus we can see that

$$\begin{aligned}
\tau((x_0,-y_0)) &= \tau((0,-1)-(x_0,y_0)) \\
&= \tau((0,-1)) - \tau((x_0,y_0)) \\
&= (\mathbf{0},-\mathbf{1}) - ((x_0,x_1,...),(y_0,y_1,...)) \\
&= ((x_0,x_1,...),-(y_0,y_1,...)) \\
&= ((x_0,x_1,...),(-y_0,-y_1,...)).
\end{aligned}$$

But we must have

$$x_n(x_0,y_0) = x_n(x_0,-y_0)$$

for all y_0, after which point our previous argumentation gives the analogous result for x_n. We complete the proof by observing that, once we know x_n, y_n are polynomials in a single variable,

$$\tau((-x_0,y_0)) = ((-x_0,-x_1,...),(y_0,y_1,...))$$

$$\tau((x_0,-y_0)) = ((x_0,x_1,...),(-y_0,-y_1,...))$$

shows x_n, y_n are odd functions. □

Recall the involution κ_2, is given by

$$\kappa_2(P) = \mathcal{K}_2 - P \qquad \kappa_2((x_0,y_0)) = \left(\frac{y_0}{b_0}, b_0 x_0\right)$$

where $\mathcal{K}_2 = \left(\frac{1}{b_0}, 0\right)$ has order 4. Since $\tau(\mathcal{K}_2)$ must be an affine point of order 4 whose reduction modulo p is $\mathcal{K}_2$, we see

$$\tau(\mathcal{K}_2) = \left(\frac{\mathbf{1}}{\mathbf{b}}, \mathbf{0}\right).$$

Since τ commutes with the group operations, we see

$$\begin{aligned}\left(\frac{\mathbf{y}}{\mathbf{b}}, \mathbf{bx}\right) + (\mathbf{x}, \mathbf{y}) &= \left(\frac{\mathbf{1}}{\mathbf{b}}, \mathbf{0}\right) \\ &= \tau\left(\left(\frac{1}{b_0}, 0\right)\right) \\ &= \tau((x_0, y_0) + \kappa_2((x_0, y_0)) \\ &= (\mathbf{x}, \mathbf{y}) + \tau\left(\left(\frac{y_0}{b_0}, b_0 x_0\right)\right).\end{aligned}$$

Thus

$$\tau\left(\left(\frac{y_0}{b_0}, b_0 x_0\right)\right) = \left(\frac{\mathbf{y}}{\mathbf{b}}, \mathbf{bx}\right). \tag{4.1.1}$$

Writing $\tau\left(\left(\frac{y_0}{b_0}, b_0 x_0\right)\right)$ as

$$\tau\left(\left(\frac{y_0}{b_0}, b_0 x_0\right)\right) = \left(\left(\frac{y_0}{b_0}, x_1\left(\frac{y_0}{b_0}\right), x_2\left(\frac{y_0}{b_0}\right), ...\right), (b_0 x_0, y_1(b_0 x_0), y_2(b_0 x_0), ...)\right)$$

and $\left(\frac{\mathbf{y}}{\mathbf{b}}, \mathbf{bx}\right)$ as

$$\left(\frac{(y_0, y_1(y_0), y_2(y_0), ...)}{(b_0, b_1, ...)}, (b_0, b_1, b_2, ...)(x_0, x_1(x_0), x_2(x_0), ...)\right)$$

we see Equation (4.1.1) defines the system of equations

$$(b_0, b_1, b_2, ...)\left(\frac{y_0}{b_0}, x_1\left(\frac{y_0}{b_0}\right), x_2\left(\frac{y_0}{b_0}\right), ...\right) = (y_0, y_1(y_0), y_2(y_0), ...) \tag{4.1.2}$$

Given we usually denote $y_n(y_0)$ as just y_n, we re-notate as

$$(b_0, b_1, b_2, ...)\left(\frac{y_0}{b_0}, x_1\left(\frac{y_0}{b_0}\right), x_2\left(\frac{y_0}{b_0}\right), ...\right) = (y_0, y_1, y_2, ...)$$

and derive the equality

$$y_n = b_0^{p^n} x_n\left(\frac{y_0}{b_0}\right) + b_n y_0^{p^n} + ... \tag{4.1.3}$$

where all omitted terms are elements of $k[y_0, ..., y_{n-1}, b_0, ..., b_{n-1}]$. In particular, we observe that if/when $\mathbf{b} = (b_0, 0, ...)$ then

$$x_n = \sum \alpha_i x_0^i \implies y_n = \sum b_0^{p^n - i}\alpha_i y_0^i.$$

Next, by Theorem 3.1 and Corollary 4.5 of [8] and the fact that $\binom{-1}{n} = (-1)^n$ for all $n \in \mathbb{N}$, we get the following results:

$$ord_{\mathcal{O}^\pm}(y_n) = -(n+1)p^n + np^{n-1} \qquad ord_{\mathcal{Q}^\pm}(x_n) = -(n+1)p^n + np^{n-1}.$$

Since $ord_{\mathcal{O}^\pm}(y_0) = -1$ and $ord_{\mathcal{Q}^\pm}(x_0) = -1$, we obtain the degrees of x_n, y_n as polynomials in x_0, y_0 respectively.

Theorem 4.2. *For all $n \geq 1$,*

$$\deg(x_n) = (n+1)p^n - np^{n-1} \qquad \deg(y_n) = (n+1)p^n - np^{n-1}$$

as polynomials in x_0, y_0 respectively.

We next compute the derivatives of x_n, y_n. Let ϕ denote the p-th power Frobenius on $\mathbf{W}(k)$. We introduce the following propositions, stated and proven as Proposition 4.4 and Corollary 4.2 in [9].

Proposition 4.3. *Let C be a curve and $\mathbf{C}$ a lift of C. Let $\nu(x_0, y_0) = ((x_0, x_1, ...), (y_0, y_1, ...))$ be a lift between the affine parts of the curves and assume there exists a lifting of the Frobenius between the affine parts, say ϕ. Then modulo p^{n+1}, ϕ^n is given by*

$$(\mathbf{x}^{p^n} + p\mathbf{x_1}p^{n-1} + ... + p^n\mathbf{x_n}, \mathbf{y}^{p^n} + p\mathbf{y_1}p^{n-1} + ... + p^n\mathbf{y_n})$$

where $\mathbf{x_k}, \mathbf{y_k} \in \mathbf{W}(k)(\mathbf{x}, \mathbf{y})$ are lifts of x_k, y_k respectively.

Proposition 4.4. *Let k be a perfect field of characteristic $p \geq 3$ and*

$$U/k : \qquad g(x_0, y_0) = 0$$

an affine curve in $\mathbb{A}^2$. Let

$$\mathbf{U}/\mathbf{W}_{n+1}(k) : \qquad \mathbf{g}(\mathbf{x}, \mathbf{y}) = 0$$

be an affine curve with reduction U, i.e., g reduces to g modulo p. If we have a lift of points $\nu : U(k) \to \mathbf{U}(\mathbf{W}_{n+1}(k))$ given by

$$\nu(x_0, y_0) = ((x_0, x_1, ..., x_n), (y_0, y_1, ..., y_n)),$$

with $x_i, y_i \in k[x_0, y_0]$, then the reduction modulo p of $\left(\frac{1}{p^n}\phi^n\right)^* d\mathbf{x}$ is

$$dx_n + x_{n-1}^{p-1}dx_{n-1} + ... + x_1^{p^{n-1}-1}dx_1 + x_0^{p^n-1}dx_0$$

and the reduction modulo p of $\left(\frac{1}{p^n}\phi^n\right)^* d\mathbf{y}$ is

$$dy_n + y_{n-1}^{p-1}dy_{n-1} + ... + y_1^{p^{n-1}-1}dy_1 + y_0^{p^n-1}dy_0.$$

With these two propositions, we prove the following theorem:

Theorem 4.5. *Let E_{a_0,b_0} be an ordinary elliptic curve in Twisted Edwards Form and $\mathbf{E_{a,b}}$ its canonical lift. Let $\tau : E(k) \to \mathbf{E}(\mathbf{W}(k))$ be the elliptic Teichmüller lift*

$$\tau(x_0, y_0) = ((x_0, x_1, ...), (y_0, y_1, ...)).$$

Then, for $n \geq 1$,

$$\frac{dx_n}{dx_0} = A_E^{-(p^n-1)/(p-1)}(b_0^2x_0^2 - 1)^{\frac{p^n-1}{2}}(a_0x_0^2 - 1)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} x_k^{p^{n-k}-1}\frac{dx_k}{dx_0} \tag{4.5.1}$$

$$\frac{dy_n}{dy_0} = A_E^{-(p^n-1)/(p-1)}(b_0^2 - a_0y_0^2)^{\frac{p^n-1}{2}}(1 - y_0^2)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} y_k^{p^{n-k}-1}\frac{dy_k}{dy_0}. \tag{4.5.2}$$

where A_E is the Hasse invariant of E_{a_0,b_0}.

Proof. Let ω denote the reduction modulo p of

$$\left(\frac{1}{p^n}\phi^n\right)^* \left(\frac{2\mathbf{x}d\mathbf{y}}{\mathbf{1} - \mathbf{y}^2}\right).$$

which we know to be a holomorphic differential [12]. Thus there is some $\lambda \in k^\times$ such that

$$\omega = \lambda\frac{2x_0dy_0}{1 - y_0^2}.$$

Applying the $n-$th power of the Cartier Operator, we see

$$\mathcal{C}^n(\omega) = \lambda^{1/p^n}A_E^{1/p+1/p^2+...+1/p^n}\frac{2x_0dy_0}{1 - y_0^2}.$$

But also, since $\left(\frac{1}{p}\phi\right)^*$ is the "inverse of the Cartier Operator", we must also have

$$\mathcal{C}^n(\omega) = \frac{2x_0dy_0}{1 - y_0^2}.$$

Thus

$$\lambda^{1/p^n} = A_E^{-1/p-1/p^2-\ldots-1/p^n} \implies \lambda = A_E^{-p^{n-1}-p^{n-2}-\ldots-1} = A_E^{-(p^n-1)/(p-1)}.$$

As such,

$$\omega = A_E^{-(p^n-1)/(p-1)} \frac{2x_0 dy_0}{1-y_0^2}.$$

Using what we know about $\left(\frac{1}{p^n}\phi^n\right)^* d\mathbf{y}$, we may also write

$$\omega = \frac{2x_0^{p^n}\left(dy_n + y_{n-1}^{p-1}dy_{n-1} + \ldots + y_1^{p^{n-1}-1}dy_1 + y_0^{p^n-1}dy_0\right)}{(1-y_0^2)^{p^n}}$$

Rearranging terms yields

$$A_E^{-(p^n-1)/(p-1)} \frac{(1-y_0^2)^{p^n}}{x_0^{p^n-1}(1-y_0^2)} = \sum_{k=0}^{n} y_k^{p^{n-k}-1}\frac{dy_k}{dy_0}$$

Rewriting x_0^2 as $(1-y_0^2)/(b_0^2 - a_0 y_0^2)$ and isolating dy_n/dy_0 finally results in

$$\frac{dy_n}{dy_0} = A_E^{-(p^n-1)/(p-1)}(b_0^2 - a_0 y_0^2)^{\frac{p^n-1}{2}}(1-y_0^2)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} y_k^{p^{n-k}-1}\frac{dy_k}{dy_0}. \tag{4.5.3}$$

Similarly, we compute the derivative of x_n by appealing to Equation (2.1.14), writing

$$\omega = A_E^{-(p^n-1)/(p-1)} \frac{2y_0 dx_0}{b_0^2 x_0^2 - 1}.$$

Consider the pullback of the invariant differential of $\mathbf{E}_{\mathbf{a},\mathbf{b}}^{p^n}$

$$\left(\frac{1}{p}\phi^*\right)^n \left(\frac{\mathbf{2y}d\mathbf{x}}{\mathbf{b}^{2p^n}\mathbf{x}^2 - \mathbf{1}}\right)$$

which is equal to

$$\frac{2y_0^{p^n}(dx_n + x_{n-1}^{p-1}dx_{n-1} + ... + x_1^{p^{n-1}-1}dx_1 + x_0^{p^n-1}dx_0)}{(b_0^2x_0^2 - 1)^{p^n}}.$$

Rearranging as before gives

$$A_E^{-(p^n-1)/(p-1)}\frac{(b_0^2x_0^2-1)^{p^n-1}}{y_0^{p^n-1}} = \sum_{k=0}^{n} x_k^{p^{n-k}-1}\frac{dx_k}{dx_0}.$$

Rewriting y_0^2 as $(b_0^2x_0^2 - 1)/(a_0x_0^2 - 1)$ and isolating dx_n/dx_0

$$\frac{dx_n}{dx_0} = A_E^{-(p^n-1)/(p-1)}(b_0^2x_0^2-1)^{\frac{p^n-1}{2}}(a_0x_0^2-1)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} x_k^{p^{n-k}-1}\frac{dx_k}{dx_0} \tag{4.5.4}$$

□

Define the function $M(n)$ by

$$M(n) := \begin{cases} 1 & n = 1 \\ (n+1)p^{n-1} - np^{n-2} & n \geq 2 \end{cases}.$$

Letting F_n be the formal integral of $\frac{dx_n}{dx_0}$, we see

$$x_n = F_n + \sum_{k=1}^{M(n)} \epsilon_k x_0^{pk} \tag{4.5.5}$$

where we know $\epsilon_{2k} = 0$ by virtue of the fact x_n is an odd function. Similarly we see

$$y_n = G_n + \sum_{j=1}^{M(n)} \delta_j y_0^{pj} \tag{4.5.6}$$

where again $\delta_{2k} = 0$ as y_n is also an odd function.

4.2 The Algorithm

We describe an analog of the algorithm due to Voloch and Walker from [16], later extended by Finotti in [10], that computes the Canonical Lifting and Elliptic Teichmüller associated with an elliptic curve by computing its Weierstrass coefficients. Our algorithm computes the Canonical Lift and Elliptic Teichmüller of a Twisted Edwards Curve given by

$$E_{a_0,b_0}/k: \qquad b_0^2x_0^2 + y_0^2 = 1 + a_0x_0^2y_0^2$$

Let $\Bbbk := k(a_0, b_0)$, with a_0, b_0 indeterminates. In this way, $E_{a_0,b_0}/k$ is an ordinary curve as it has a non-zero Hasse Invariant, so we may consider its Canonical Lift

$$\mathbf{E_{a,b}/W}(\Bbbk) : \mathbf{b}^2\mathbf{x}^2 + \mathbf{y}^2 = \mathbf{1} + \mathbf{a}\mathbf{x}^2\mathbf{y}^2$$

where $\mathbf{a} = (a_0, a_1, ...), \mathbf{b} = (b_0, b_1, ...)$. Applying Theorem (3.4), we find the $n+1$st coordinate of the Greenberg Transform (for $n \geq 1$) is given by

$$\begin{aligned} &2b_nb_0^{p^n}x_0^{2p^n} + 2b_0^{2p^n}x_0^{p^n}x_n + 2y_0^{p^n}y_n + ... \\ =&a_nx_0^{2p^n}y_0^{2p^n} + 2a_0^{p^n}x_0^{p^n}y_0^{2p^n}x_n + 2a_0^{p^n}x_0^{2p^n}y_0^{p^n}y_n + ... \end{aligned} \tag{4.5.7}$$

where all omitted terms are polynomials in $k[x_0, ..., x_{n-1}, y_0, ..., y_{n-1}, a_0, ..., a_{n-1}, b_0, ...b_{n-1}]$. As usual, let

$$\tau(x_0, y_0) = ((x_0, x_1, ...), (y_0, y_1, ...))$$

be the Teichmüller Lift.

Proposition 4.6. *For all $n \in \mathbb{Z}_{\geq 0}$, $a_n, b_n \in \Bbbk$, $x_n \in \Bbbk[x_0]$ and $y_n \in \Bbbk[y_0]$.*

The remainder of this section and the next are dedicated to the proof of this proposition. We prove this inductively seeing the $n = 0$ case is trivial, as this is our base curve E_{a_0,b_0}. We thus assume $n \geq 1$, and the result holds for all $k < n$.

We rearrange the terms in Equation (4.5.7) such that our right-hand side is entirely determined by the induction hypothesis. This results in

$$\begin{aligned} 2x_0^{p^n} x_n \left(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}\right) + 2y_0^{p^n} y_n \left(1 - a_0^{p^n} x_0^{2p^n}\right) \\ + 2b_n b_0^{p^n} x_0^{2p^n} - a_n x_0^{2p^n} y_0^{2p^n} = \Omega_1 \end{aligned} \tag{4.6.1}$$

where $\Omega_1 \in \Bbbk[x_0, y_0]$ is entirely determined by the induction hypothesis.

Using 2.6 and comparing coefficients of the resulting monomials gives a linear system in $a_n, b_n, \epsilon_1, ..., \epsilon_{M(n)}, \delta_1, ..., \delta_{M(n)}$. The existence of a solution to the system is guaranteed by the existence of $\mathbf{E_{a,b}}$ and τ, but not all solutions produce $\mathbf{E_{a,b}}$ and τ. To this end, we introduce the following proposition:

Proposition 4.7. *$\tau(\mathcal{O}^\pm) = \mathcal{O}^\pm$ and $\tau(\mathcal{Q}^\pm) = \mathcal{Q}^\pm$. Moreover, $\tau \circ \kappa_i = \kappa_i \circ \tau$ for κ_i defined as in Equations (2.1.7).*

Proof. Since τ is a section of the reduction modulo p, we have that it must take points at infinity to points at infinity. Also, since τ is an injective group homomorphism, and $|\mathcal{O}^\pm| = 4$ and $|\mathcal{Q}^\pm| = 2$, we have that $\tau(\mathcal{O}^\pm)$ must be one of $\mathcal{O}^\pm$ and $\tau(\mathcal{Q}^\pm)$ must be one of $\mathcal{Q}^\pm$. But, using the projective representation of Edwards curves (where $(x, y) \mapsto [1/(xy), 1/x, 1/y, 1]$), we have $\tau(\mathcal{O}^\pm) = \mathcal{O}^\pm$ and $\tau(\mathcal{Q}^\pm) = \mathcal{Q}^\pm$.

Note that $\tau(\mathcal{K}_i) = \mathcal{K}_i$ as x_n, y_n are odd functions. Thus, since τ is a group homomorphism, Equation (2.1.6) gives the second part of the lemma. □

The first part of our lemma also yields the following corollary:

Corollary 4.8.

$$\mathbf{y}^{-1}(\tau(\mathcal{O}^\pm)) = \mathbf{0} \qquad \mathbf{x}^{-1}(\tau(\mathcal{Q}^\pm)) = \mathbf{0}. \tag{4.8.1}$$

To make more use of the lemma, and to put its importance into practice, we introduce the following lemma which will later serve to give a concrete computational requirement for our algorithm.

Lemma 4.9. *Let* $\mathbf{y} = (y_0, y_1, ...)$. *For all* $n \geq 1$, *the* $n+1$*st coordinate of* $\mathbf{y}^{-1}$ *is given by*

$$-\frac{y_n}{y_0^{2p^n}} + \frac{z_n}{y_0^{(n+1)p^n}}$$

where $z_n \in \mathbb{F}_p[y_0, ...y_{n-1}]$.

Proof. A quick computation gives us the second coordinate of $\mathbf{y}^{-1}$ is given by

$$-\frac{y_1}{y_0^{2p}}$$

thus proving the base $n = 1$ case. To prove our result for $n \geq 2$, assume we may write

$$\mathbf{y}^{-1} = \left(\frac{1}{y_0}, -\frac{y_1}{y_0^{2p}}, ..., -\frac{y_{n-1} + z_{n-1}}{y_0^{np^{n-1}}}, \beta_n, ...\right).$$

By Lemma 2.1 of [8], we may write

$$\bar{P}_n(X, Y) = \sum_{i=0}^{n} X_i^{p^{n-i}} Y_{n-i}^{p^i} + \bar{Q}_n$$

where $\bar{Q}_n \in \mathbb{F}_p[X_0, ...X_{n-1}Y_0, ..., Y_{n-1}]$ and if $\prod X_i^{a_i} \prod Y_j^{b_j}$ is a monomial in $\bar{P}_n$, then

$$\sum_{j=0}^{n} b_j p^j = p^n \qquad \sum_{i=0}^{n} a_i p^i + \sum_{j=0}^{n} b_j p^j \leq np^n$$

Viewing the $n+1$st coordinate of $\mathbf{y} \cdot \mathbf{y}^{-1} = (1, 0, ...)$ as

$$\bar{P}_n(\mathbf{y}, \mathbf{y}^{-1})$$

we write this coordinate as

$$y_0^{p^n}\beta_n + \frac{y_n}{y_0^{p^n}} + w_n$$

where $w_n \in \mathbb{F}_p[y_0, \frac{1}{y_0}, y_1, ..., y_{n-1}]$. Further using Finotti's lemma, we have the largest possible power of y_0 in the denominator of w_n can be computed by

$$\sum_{j=0}^{n-1} b_j(j+1)p^j \leq n\sum_{j=0}^{n-1} b_j p^j = np^n.$$

as no monomials of w_n involve $(\mathbf{y}^{-1})_n = \beta_n$, thus $b_n = 0$ for those monomials. Thus we have $y_0^{np^n} w_n \in \mathbb{F}_p[y_0, y_1, ..., y_{n-1}]$. We conclude our argument by observing we have

$$0 = y_0^{p^n}\beta_n + \frac{y_n}{y_0^{p^n}} + \frac{y_0^{np^n} w_n}{y_0^{np^n}} \implies \beta = -\frac{y_n}{y_0^{2p^n}} - \frac{y_0^{np^n} w_n}{y_0^{(n+1)p^n}}.$$

taking $z_n = -y_0^{np^n} w_n$ gives the desired result. □

Similarly, we also have the $n+1$st coordinate of $\mathbf{x}^{-1}$ given by

$$-\frac{x_n}{x_0^{2p^n}} + \frac{t_n}{x_0^{(n+1)p^n}}$$

where $t_n \in \mathbb{F}_p[x_0, x_1, ..., x_{n-1}]$. Knowing

$$\deg(x_1) = 2p-1 \qquad \deg(y_1) = 2p-1$$

and $t_1, z_1 = 0$, we see $\mathbf{y}^{-1}(\tau(\mathcal{O}^{\pm})) \equiv \mathbf{0} \mod p^2$ and $\mathbf{x}^{-1}(\tau(\mathcal{Q}^{\pm})) \equiv \mathbf{0} \mod p^2$. Thus we may assume $n \geq 2$.

We now split Equations (4.5.5) and (4.5.6) in twain as

$$F_{n,1} := F_n + \sum_{i=M'(n)+1}^{M(n)} \epsilon_i x_0^{ip} \qquad F_{n,2} := \sum_{i=1}^{M'(n)} \epsilon_i x_0^{ip}$$

$$G_{n,1} := G_n + \sum_{j=M'(n)+1}^{M(n)} \delta_i y_0^{jp} \qquad G_{n,2} := \sum_{j=1}^{M'(n)} \delta_i y_0^{jp}$$

with $M'(n) := 2p^{n-1} - 1$. In this way we have

$$x_n = F_{n,1} + F_{n,2} \qquad y_n = G_{n,1} + G_{n,2}$$

which in turn gives the following theorem.

Theorem 4.10. *The value of $F_{n,1}, G_{n,1}$ is determined entirely by the induction hypothesis.*

Proof. Note that the derivatives of x_n, y_n are entirely determined by the induction hypothesis, thus the values of F_n, G_n are as well. Thus we need only show the induction hypothesis uniquely determines the values of ϵ_i, δ_j for $M'(n)+1 \leq i, j \leq M(n)$. Observe that decomposing x_n, y_n as above and using this decomposition in the formulation of Lemma 4.9, we see $F_{n,2}, G_{n,2}$ have poles of small enough order at the relevant points at infinity that the quotients will be regular and equal to 0. Thus we need only find ϵ_i, δ_j such that

$$\frac{t_n - x_0^{(n-1)p^n} F_{n,1}}{x_0^{(n+1)p^n}}, \frac{z_n - y_0^{(n-1)p^n} G_{n,1}}{y_0^{(n+1)p^n}} \tag{4.10.1}$$

are regular and equal to 0 at $\mathcal{Q}^{\pm}, \mathcal{O}^{\pm}$ respectively, where $t_n \in \Bbbk[x_0]$ and $z_n \in \Bbbk[y_0]$ are entirely known by the induction hypothesis.

The given condition can be restated as

$$ord_{\mathcal{Q}^{\pm}} \left(t_n - x_0^{(n-1)p^n} F_{n,1} \right) > -(n+1)p^n \qquad ord_{\mathcal{O}^{\pm}} \left(z_n - y_0^{(n-1)p^n} G_{n,1} \right) > -(n+1)p^n.$$

But since $x_0^{(n-1)p^n} F_{n,1}, y_0^{(n-1)p^n} G_{n,1}$ are polynomials of degree $2np^n - np^{n-1} > (n+1)p^n$, this uniquely determines those coefficients of $F_{n,1}$,$G_{n,1}$ thus uniquely determines the value of ϵ_i, δ_j for $M'(n)+1 \leq i,j \leq M(n)$, thus proving the desired result. □

Corollary 4.11.

$$\deg\left(t_n - x_0^{(n-1)p^n} F_{n,1}\right) < (n+1)p^n \qquad \deg\left(z_n - y_0^{(n-1)p^n} G_{n,1}\right) < (n+1)p^n.$$

We claim any solution to the remaining linear system will indeed give $\mathbf{E_{a,b}}, \tau$. This amounts to proving the following:

Theorem 4.12. *Let E_{a_0,b_0} be an ordinary elliptic curve and $\mathbf{E_{a,b}}$ a lifting of E_{a_0,b_0}. Let τ be a section of the reduction modulo p map between the affine parts of E_{a_0,b_0} and $\mathbf{E_{a,b}}$. If τ is regular at $\mathcal{O}^{\pm}, \mathcal{Q}^{\pm}$ in such a way that*

$$\tau(\mathcal{O}^{\pm}) = \mathcal{O}^{\pm}, \qquad \tau(\mathcal{Q}^{\pm}) = \mathcal{Q}^{\pm}$$

then $\mathbf{E_{a,b}}$ is the canonical lift and τ is the elliptic Teichmüller .

Proof. This is just Proposition 4.2 in [16] adapted to Edwards Curves. □

We are now left to solve the resulting linear system

$$\begin{aligned}\Omega_2 =& 2x_0^{p^n} \sum_{i=1}^{M'(n)} \epsilon_i x_0^{pi} \left(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}\right) \\ &+ 2y_0^{p^n} \sum_{j=1}^{M'(n)} \delta_j y_0^{pj} \left(1 - a_0^{p^n} x_0^{2p^n}\right) + 2b_n b_0^{p^n} x_0^{2p^n} - a_n x_0^{2p^n} y_0^{2p^n}\end{aligned} \tag{4.12.1}$$

where $\Omega_2 \in \Bbbk[x_0, y_0]$ is entirely determined by the induction hypothesis and the requirements on the terms with index $M'(n)+1 \leq i,j \leq M(n)$. Further, by 4.12, any solution to this system gives a representation of $\mathbf{E_{a,b}}$ and τ.

4.3 Solving the System

Assume we have two solutions to the $n+1$st coordinate given by

$$\left(a_n, b_n, \epsilon_0, ..., \epsilon_{M'(n)}, \delta_0, ..., \delta_{M'(n)}\right) \qquad \left(a'_n, b'_n, \epsilon'_0, ..., \epsilon'_{M'(n)}, \delta'_0, ..., \delta'_{M'(n)}\right),$$

both giving representations of $\mathbf{E_{a,b}}, \tau$. Observe both solutions give maps τ, τ' that map

$$\mathcal{O}^{\pm} \mapsto \mathcal{O}^{\pm}, \qquad \mathcal{Q}^{\pm} \mapsto \mathcal{Q}^{\pm}$$

thus the isogeny between them must be an Edwards Isogeny. Such an isogeny must exist as $\mathbf{E_{a,b}}$ is unique up to birational equivalence. Thus there exists $\boldsymbol{\alpha} \in W_{n+1}(\bar{\mathbb{k}})^{\times}$ such that

$$\frac{\mathbf{1}}{\boldsymbol{\alpha}^2}(a_0, a_1, ..., a_n) = (a_0, a_1, ..., a'_n) \qquad \frac{\mathbf{1}}{\boldsymbol{\alpha}}(b_0, b_1, ..., b_n) = (b_0, b_1, ..., b'_n).$$

Thus $\boldsymbol{\alpha} \equiv 1 \mod p^n$, we see $\boldsymbol{\alpha} = (1, 0, ..., 0, \alpha_n)$ for some α_n. This yields

$$a'_n = a_n - 2\alpha_n a_0^{p^n} \qquad b'_n = b_n - \alpha_n b_0^{p^n}.$$

Note that this value of α_n entirely determines that value of a_n, b_n, thus entirely determines $\mathbf{E_{a,b}}, \tau$. Thus we will have a single choice for the values of ϵ_i, δ_j for a given value of α_n. Taking the difference between our two solutions we find

$$\begin{aligned} 0 =& 2x_0^{p^n} \sum_{i=1}^{M'(n)} (\epsilon'_i - \epsilon_i) x_0^{pi} \left(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}\right) \\ &+ 2y_0^{p^n} \sum_{j=1}^{M'(n)} (\delta'_j - \delta_j) y_0^{pj} \left(1 - a_0^{p^n} x_0^{2p^n}\right) \\ &- 2\alpha_n b_0^{2p^n} x_0^{2p^n} + 2\alpha_n a_0^{p^n} x_0^{2p^n} y_0^{2p^n} \end{aligned} \tag{4.12.2}$$

Observe the assignment

$$\delta'_j = \delta_j \qquad \epsilon'_i := \begin{cases} \epsilon_i & i \neq p^{n-1} \\ \epsilon_i + \alpha_n & i = p^{n-1} \end{cases}$$

from which we get

$$2\alpha_n x_0^{2p^n}\left(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}\right) - 2\alpha_n b_0^{2p^n} x_0^{2p^n} + 2\alpha_n a_0^{p^n} x_0^{2p^n} y_0^{2p^n} = 0$$

which yields a consistent solution, which therefore must be the unique solution. Thus we have a single free parameter and our null space is generated by

$$\left(-2a_0^{p^n}, -b_0^{p^n}, 0, ..., 0, 1, 0, ..., 0\right)$$

where the 1 occurs in the place of ϵ_{p^n-1}.

4.4 Reduction modulo p^3

We now determine exactly the conditions for the reduction modulo p^3 of the Canonical Lift. Observe the third coordinate of $\mathbf{x}^{-1}, \mathbf{y}^{-1}$ is given by

$$\frac{x_1^{2p} - x_0^{p^2} x_2}{x_0^{3p^2}}, \qquad \frac{y_1^{2p} - y_0^{p^2} y_2}{y_0^{3p^2}}.$$

Thus modulo p^3, our required condition is

$$\deg(x_1^{2p} - x_0^{p^2} x_2), \deg(y_1^{2p} - y_0^{p^2} y_2) \leq 3p^2 - 1. \tag{4.12.3}$$

It follows for $n > M'(1) = 2p - 1$ the coefficient of x_0^{pn} in x_2 is equal to the $p-$th power of the coefficient of x_0^{n+p} in x_1^2 and the coefficient of y_0^{pn} in y_2 is equal to the $p-$th power of the coefficient of y_0^{n+p} in y_1^2.

In general, the set of conditions imposed by Corollary 4.11 are simpler than those for Weierstrass Equations.

4.5 Universal Representations

We show we may refine these solutions in such a way that a_n, b_n, x_n, y_n are *universal*, i.e. is well defined at any pair $(a_0, b_0) \in k^2$ such that

$$E_{a_0,b_0}/k: \quad b_0 x_0^2 + y_0^2 = 1 + a_0 x_0^2 y_0^2$$

is an ordinary elliptic curve in Twisted Edwards form. This result is known for elliptic curves in Weierstrass Form, the proof of which can be found in [10]. We prove this in a similar way.

Proposition 4.13. *Let a_0, b_0 indeterminants, $\Delta := ab^2(a - b^2)$ be the discriminant of our curve and A_E the Hasse Invariant. Let $\mathbb{L} := \mathbb{F}_p\left[a_0, b_0, \frac{1}{A\Delta}\right]$. Then there exists $a_i, b_i \in \mathbb{L}$ and $x_i, y_i \in \mathbb{L}[x_0], \mathbb{L}[y_0]$ respectively for $i = 1, 2, ...$ such that the Canonical Lift of E_{a_0,b_0} is given by $((a_0, a_1, ...), (b_0, b_1, ...))$ and the associated Teichmüller Lift is given by*

$$\tau(x_0, y_0) = ((x_0, x_1, ...), (y_0, y_1, ...)).$$

This has the following corollary:

Corollary 4.14. *There exists a representation of the Canonical Lift and τ that is universal.*

We dedicate the remainder of this section to proving the proposition, again by induction. Note the base case is trivially complete as it is just the curve $E_{a_0,b_0}/k$.

Assume we have computed the Canonical Lift up to the $n-$th coordinate, with a_i, b_i, x_i, y_i satisfying the induction hypothesis for $0 \leq i < n$. We again use the

linear system given in Equation (4.12.1) to prove the result holds for the $n+1$st coordinate.

To begin, note $0 \in \mathbb{L}[x_0]$. Likewise, all those ϵ_i, δ_j for $M'(n) < i, j \leq M(n)$ are known to be in $\mathbb{L}$ by the induction hypothesis and by virtue of the fact that they are chosen such that

$$\frac{t_n - x_0^{(n-1)p^n} F_{n,1}}{x_0^{(n+1)p^n}}, \qquad \frac{z_n - y_0^{(n-1)p^n} G_{n,1}}{y_0^{(n+1)p^n}},$$

are regular and equal to 0 at the relevant points at infinity, whereby the induction hypothesis $t_n, z_n \in \mathbb{L}[x_0], \mathbb{L}[y_0]$ respectively. F_n, G_n are in $\mathbb{L}[x_0], \mathbb{L}[y_0]$ respectively by virtue of the fact they are the formal integral of polynomials in $\mathbb{L}[x_0], \mathbb{L}[y_0]$.

For those ϵ_i, δ_j with $0 \leq i, j \leq M'(n)$ and $i \neq p^n - 1$, ϵ_i, δ_j is independent of our choice of α_n, thus are universal. But this means they are defined for all a_0, b_0 such that E_{a_0,b_0} is an ordinary curve, thus (as functions in a_0, b_0) cannot have a pole at any such pair, so they must be elements of $\mathbb{L}$. To prove $\epsilon_{p^n-1} \in \mathbb{L}$, we observe we may pick the value of $\epsilon_{p^n-1} = 0$. This fixes a representation of the Canonical Lift and Teichmüller such that, when looking at the coefficients of $x_0^{2p^n}, y_0^{2p^n}$ in our reduced system, $a_n, b_n \in \mathbb{L}$, thus completing the proof.

4.6 Modularity of a_n, b_n

Again let a_0, b_0 be indeterminants and assign them weights $-2, -1$ respectively. Define

$$\mathcal{S}_n := \left\{ \frac{f}{g} \in \mathbb{F}(a_0, b_0) : f, g \in \mathbb{F}[a_0, b_0] \text{ weight}(f) - \text{weight}(g) = n \right\}.$$

were f, g are homogeneous polynomials. Similarly, we define the weights of x_0, y_0 to be $1, 0$ respectively and define

$$\widehat{\mathcal{S}_n} := \left\{ \frac{f}{g} \in \mathbb{F}(a_0, b_0, x_0, y_0) : f, g \in \mathbb{F}[a_0, b_0, x_0, y_0] \text{ weight}(f) - \text{weight}(g) = n \right\}.$$

where again f, g are assumed to be homogeneous polynomials. Clearly, we have

$$\mathcal{S}_n = \mathbb{F}(a_0, b_0) \cap \widehat{\mathcal{S}}_n.$$

This motivates the following lemma, proven in [10]:

Lemma 4.15. *Let $\pi_i : \mathbf{W}(\Bbbk) \to \Bbbk$ be the projection map onto the $i+1$st coordinate (i.e. $\pi_i(\mathbf{s}) = s_i$). Then if $\pi_i(\mathbf{f}) \in \mathcal{S}_{rp^i}$ and $\pi_i(\mathbf{g}) \in \mathcal{S}_{sp^i}$ then $\pi_i(\mathbf{fg}) \in \mathcal{S}_{(r+s)p^i}$. Further, if $r = s$, then $\pi_i(\mathbf{f} + \mathbf{g}) \in \mathcal{S}_{rp^i}$.*

Clearly the result also holds for $\widehat{\mathcal{S}}_n$. With this in mind, we claim the following:

Proposition 4.16. *If there exists*

$$\mathbf{E}/\mathbf{W}(k) \qquad (b_0, b_1, ...)^2\mathbf{x}^2 + \mathbf{y}^2 = \mathbf{1} + (a_0, a_1, ...)\mathbf{x}^2\mathbf{y}^2$$

a representation of the Canonical Lift of E_{a_0,b_0}. such that $a_i \in \mathcal{S}_{r_i}, b_i \in \mathcal{S}_{s_i}$. Then $r_i = -2p^i$ and $s_i = -p^i$.

Proof. Before we proceed, observe if the functions $a_1, ..., a_n, b_1, ..., b_n$ are chosen (giving the Canonical Lifting), then given $\lambda_0 \in \Bbbk$, there must be some $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, ...)$ such that

$$\boldsymbol{\lambda}^{-2}(a_0, a_1, ...) = \left(\lambda_0^{-2}a_0, a_1\left(\lambda_0^{-2}a_0, \lambda_0^{-1}b_0\right), ...\right).$$

$$\boldsymbol{\lambda}^{-1}(b_0, b_1, ...) = \left(\lambda_0^{-2}b_0, b_1\left(\lambda_0^{-2}a_0, \lambda_0^{-1}b_0\right), ...\right).$$

Clearly, each of the λ_i is a function in λ_0. We prove if a_i, b_i are modular, then there are of weight $-2p^i$ and $-p^i$ respectively and at the same time prove $\lambda_i = 0$ for $i > 0$.

We again proceed by induction and see by definition this holds true for $i = 0$. To see the result hold for $i = 1$ (where we begin proving $\lambda_i = 0$ for $i > 0$), we assume a_1, b_1 are modular functions or weight r_1, s_1 respectively. By our above equality, we have

$$\begin{aligned}(\lambda_0^{-2}, -\lambda_0^{-2p}\lambda_1)(a_0, a_1(a_0, b_0)) = \left(\lambda_0^{-2}a_0, a_1\left(\lambda^{-2}a_0, \lambda^{-1}b_0\right)\right) \implies \\ \lambda_0^{-2p}a_1(a_0, b_0) - a_0^p\lambda_0^{-2p}\lambda_1 = \lambda_0^{r_1}a_1\left(a_0, b_0\right).\end{aligned}$$

Moving terms around, we see

$$\left(\lambda_0^{-2p} - \lambda_0^{r_1}\right) a_1(a_0, b_0) = a_0^p\lambda_0^{-2p}\lambda_1.$$

By construction, our right-hand side is in $\mathcal{S}_{-2p}$, thus our left-hand side must be as well. But $a_1 \in \mathcal{S}_{r_1}$, so it must be the case $r_1 = -2p$ or $a_1 = 0$ (which is always an element of $\mathcal{S}_{-2p}$). In either case, our left-hand side is 0, so our right-hand side must be as well, thus $\lambda_1 = 0$. Similar argumentation shows $b_1 \in \mathcal{S}_{-p}$.

We assume the induction hypothesis holds true for all $0 \leq i < n$. But this same above argumentation shows $r_n = -2p^n$ and $\lambda_n = 0$ as we will be looking at the $n + 1$st coordinate of the equality

$$(\lambda_0^{-2}, 0, ..., 0, -\lambda_0^{-2p^n}\lambda_n)(a_0, ..., a_n(a_0, b_0)) = \left(\lambda_0^{-2}a_0, ..., a_n\left(\lambda^{-2}a_0, \lambda^{-2}b_0\right)\right)$$

given by

$$\lambda_0^{-2p^n}a_n(a_0, b_0) - a_0^{p^n}\lambda_0^{-2p^n}\lambda_n = \lambda_0^{-2r_n}a_n\left(a_0, b_0\right).$$

Then $a_n \in \mathcal{S}_{-2p^n}$, and following the same argumentation will give $b_n \in \mathcal{S}_{-p^n}$ □

This guarantees a unique weight to any modular solution but does not itself guarantee the existence of a modular solution. We make the following claim:

Proposition 4.17. *For all $i \geq 0$, the functions a_i, b_i can be taken so $a_i(a_0, b_0) \in \mathcal{S}_{-2p^i}, b_i(a_0, b_0) \in \mathcal{S}_{-p^i}$.*

Proof. Note it suffices to prove $a_i \in \widehat{\mathcal{S}}_{-2p^i}, b_i \in \widehat{\mathcal{S}}_{-p^i}$ as $a_i, b_i \in k(a_0, b_0)$. We again proceed by induction, observing the base case $i = 0$ trivially holds. Thus we assume the result holds for $i < n$. We consider the solution to the system to Equation (4.6.1) found by taking $\epsilon_{p^{i-1}} = 0$. A quick calculation shows that, by the induction hypothesis, the formal integral of dx_n/dx_0 and dy_n/dy_0 are elements of $\widehat{\mathcal{S}}_{p^n}$ and $\widehat{\mathcal{S}}_0$ respectively, which can be seen as we know $A_E \in \widehat{\mathcal{S}}_{1-p}$.

Similarly, Lemma (4.15) tells us if $\pi_n(\mathbf{s}) \in \widehat{\mathcal{S}}_n$, then $\pi_n(\mathbf{s}^{-1}) \in \widehat{\mathcal{S}}_{-n}$. From this, we again write

$$\pi_n\left(\mathbf{x}^{-1}\right) = \frac{t_n - x_0^{(n-1)p^n} x_n}{x_0^{(n+1)p^n}}, \qquad \pi_n\left(\mathbf{y}^{-1}\right) = \frac{z_n - y_0^{(n-1)p^n} y_n}{y_0^{(n+1)p^n}}$$

and observe $t_n \in \widehat{\mathcal{S}}_{np^n}$ and $z_n \in \widehat{\mathcal{S}}_0$ by construction. Since the polynomials $F_{n,1}, G_{n,1}$ are entirely determined by t_n, z_n respectively such that

$$deg\left(t_n - x_0^{(n-1)p^n} F_{n,1}\right) \leq (n+1)p^n - 1, \qquad deg\left(z_n - y_0^{(n-1)p^n} G_{n,1}\right) \leq (n+1)p^n - 1$$

it must be the case $F_{n,1} \in \widehat{\mathcal{S}}_{np^n}, G_{n,1} \in \widehat{\mathcal{S}}_0$ as terms of degree $2p^n$ or higher (which are comprised entirely of the unknowns ϵ_i, δ_j for $M'(n) + 1 \leq i, j \leq M(n)$) must cancel with the terms of the same degree in t_n, z_n respectively.

Since we fixed our representation to have $\epsilon_{p^{n-1}} = 0$, the system must have a unique solution. Further, the choice of $\epsilon_{p^{n-1}} = 0$ guarantees any denominators are powers of $A_E \in \widehat{\mathcal{S}}_{1-p}$ and $\Delta \in \widehat{\mathcal{S}}_{-6}$. Further, all the values on the left-hand side of Equation (4.6.1) are elements of $\widehat{\mathcal{S}}_0$, thus our right-hand side is an element of $\widehat{\mathcal{S}}_0$.

Assume we have *the unique* solution to Equation (4.12.1). Decompose $a_n, b_n, \epsilon_i, \delta_j$ for

$1 \leq i, j \leq M'(n)$ as

$$a_n = a_{n,0} + a_{n,1} \qquad b_n = b_{n,0} + b_{n,1} \qquad \epsilon_i = \epsilon_{i,0} + \epsilon_{i,1} \qquad \delta_j = \delta_{j,0} + \delta_{j,1}$$

where the polynomials are such that

$$a_{n,0} \in \widehat{\mathcal{S}}_{-2p^n} \qquad b_{n,0} \in \widehat{\mathcal{S}}_0 \qquad \epsilon_{i,0} \in \widehat{\mathcal{S}}_{p^n - ip} \qquad \delta_{j,0} \in \widehat{\mathcal{S}}_0$$

and each $a_{n,0}, b_{n,0}, \epsilon_{i,0}, \delta_{j,0}$ contains *all such monomials*. Thus Equation (4.12.1) becomes

$$\begin{aligned}
&2x_0^{p^n} \sum_{i=1}^{M'(n)} \epsilon_{i,0} x_0^{pi} \left(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}\right) + 2y_0^{p^n} \sum_{j=1}^{M'(n)} \delta_{j,0} y_0^{pj} \left(1 - a_0^{p^n} x_0^{2p^n}\right) \\
&+2b_{n,0} b_0^{p^n} x_0^{2p^n} - a_{n,0} x_0^{2p^n} y_0^{2p^n} \\
&+2x_0^{p^n} \sum_{i=1}^{M'(n)} \epsilon_{i,1} x_0^{pi} \left(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}\right) + 2y_0^{p^n} \sum_{j=1}^{M'(n)} \delta_{j,1} y_0^{pj} \left(1 - a_0^{p^n} x_0^{2p^n}\right) \\
&+2b_{n,1} b_0^{p^n} x_0^{2p^n} - a_{n,1} x_0^{2p^n} y_0^{2p^n} = \Omega_2
\end{aligned}$$

where $\Omega_2 \in \widehat{\mathcal{S}}_0$. But since the latter part of our sum would not be an element of $\widehat{\mathcal{S}}_0$ if it is non-zero, it must be the case

$$\begin{aligned}
2x_0^{p^n} \sum_{i=1}^{M'(n)} \epsilon_{i,1} x_0^{pi} \left(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}\right) &+2y_0^{p^n} \sum_{j=1}^{M'(n)} \delta_{j,1} y_0^{pj} \left(1 - a_0^{p^n} x_0^{2p^n}\right) \\
&+2b_{n,1} b_0^{p^n} x_0^{2p^n} - a_{n,1} x_0^{2p^n} y_0^{2p^n} = 0.
\end{aligned}$$

But then there is a solution to the system given by

$$(a_{n,0}, b_{n,0}, \epsilon_{1,0}, ..., \epsilon_{M'(n),0}, \delta_{1,0}, ..., \delta_{M'(n),0}),$$

contradicting the uniqueness of the original solution. Thus

$$a_{n,1}, b_{n,1}, \epsilon_{i,1}, \delta_{j,1} = 0,$$

which in turn gives us the desired result. □

Chapter 5

Minimal Liftings of Twisted Edwards Curves

5.1 Definitions, Degrees, and Derivatives

Throughout this section, we let E be a Twisted Edwards Curve over a perfect field k of characteristic $p \geq 3$ and $\mathbf{E}$ a Twisted Edwards Curve over $\mathbf{W}(k)$ whose reduction modulo p is E. Let $U, \mathbf{U}$ denote the affine parts of $E, \mathbf{E}$ respectively.

Definition 5.1 (Edwards Lift)**.** Define a Edwards Lift from E to $\mathbf{E}$ to be a regular map $\nu : U(\bar{k}) \to \mathbf{U}(\mathbf{W}(\bar{k}))$ given by

$$(x_0, y_0) \mapsto ((x_0, x_1, ...), (y_0, y_1, ...)) = (\mathbf{x}, \mathbf{y})$$

where $x_i, y_i \in k[x_0, y_0]$ for all i and ν respects the usual curve involutions

$$\nu((-x_0, y_0)) = (-\mathbf{x}, \mathbf{y}) \qquad \nu((x_0, -y_0)) = (\mathbf{x}, -\mathbf{y})$$

$$\nu\left(\left(\frac{y_0}{b_0}, b_0 x_0\right)\right) = \left(\frac{\mathbf{y}}{\mathbf{b}}, \mathbf{bx}\right).$$

Similar to the Canonical Lift, we have a nice representation of the possible Edwards Lifts given by odd functions.

Theorem 5.2. *If $\nu : U(\bar{k}) \to \mathbf{U}(\mathbf{W}(\mathbf{k})$ is an Edwards Lift, then for all n, there exist $F_n, G_n \in k[t]$ such that $x_n = x_0 F_n(x_0^2)$ and $y_n = y_0 G_n(y_0^2)$.*

Proof. The result follows by the same argumentation as used in Theorem 4.1, though the involutions are assumed rather than derived by group-theoretic means. □

Definition 5.3 (Minimal Degree Edwards Lift)**.** Let $E, \mathbf{E}$ be as above. A *Minimal Degree Edwards Lift modulo p^2 from E to* $\mathbf{E}/\mathbf{W}_2(k)$ is an Edwards Lift

$$\nu(x_0, y_0) = ((x_0, x_1(x_0)), (y_0, y_1(y_0)))$$

where $\deg(x_1)$ is minimal. Inductively, a *Minimal Degree Edwards Lift modulo p^{n+1} from E to* $\mathbf{E}/\mathbf{W}_{n+1}(k)$ is an Edwards Lift

$$\nu(x_0, y_0) = ((x_0, x_1(x_0), ..., x_n(x_0)), (y_0, y_1(y_0), ...y_0 y_n(y_0)))$$

whose reduction modulo p^n is a minimal degree lift modulo p^n from E to $\mathbf{E}/\mathbf{W}_n(k)$ and $\deg(x_n)$ is minimal.

It is worth noting that our third involution guarantees that $\deg(x_n) = \deg(y_n)$, so the choice that x_n is minimal is equivalent to both coordinates being minimal.

Definition 5.4 (Absolute Minimal Degree Curve)**.** Let E be as above. We define an *Absolute Minimal Degree Curve modulo p^2* over E to be a curve $\mathbf{E}/\mathbf{W}_2(k)$ that reduces to E modulo p and satisfies the following additional property: Let

$$\nu(x_0, y_0) = ((x_0, x_1(x_0)), (y_0, y_1(y_0)))$$

be a minimal degree Edwards Lift E to some $\mathbf{E}$ and let $\tilde{\mathbf{E}}/\mathbf{W}_2(k)$ be any curve that reduces to E modulo p. Then for any minimal degree Edwards lift

$$\tilde{\nu}(x_0, y_0) = ((x_0, \tilde{x}_1(x_0)), (y_0, \tilde{y}_1(y_0)))$$

from E to $\tilde{\mathbf{E}}$ we have $\deg x_1 \leq \deg \tilde{x}_1$. In this case we call ν an absolute minimal degree lift modulo p^2.

Inductively, an *Absolute Minimal Degree Curve modulo* p^{n+1} is a curve $\mathbf{E}/\mathbf{W}_{n+1}(k)$ whose reduction modulo p^n is an absolute minimal degree curve modulo p^n over E, satisfying the following property: Let

$$\nu(x_0, y_0) = ((x_0, x_1(x_0), ..., x_n(x_0)), (y_0, y_1(y_0), ..., y_n(y_0)))$$

be a minimal degree Edwards lift E to some $\mathbf{E}$ and let $\tilde{\mathbf{E}}/\mathbf{W}_{n+1}(k)$ be any curve whose reduction modulo p^n is equal to the reduction modulo p^n of $\mathbf{E}$. Then for any minimal lift

$$\tilde{\nu}(t_0, u_0) = ((x_0, \tilde{x}_1(x_0), ..., \tilde{x}_n(x_0)), (y_0, \tilde{y}_1(y_0), ..., \tilde{y}_n(y_0))).$$

from E to $\tilde{\mathbf{E}}$ we have $\deg x_n \leq \deg \tilde{x}_n$. In this case, we call the minimal degree lift ν from E to $\mathbf{E}$ an *Absolute Minimal Degree Edwards Lift* modulo p^{n+1}.

We prove an upper bound for the degree of a minimal degree lifting independent of the choice of the curve $\mathbf{E}$, stated as the following:

Theorem 5.5. *Let E be an Edwards Curve over k a perfect field of characteristic $p \geq 3$ and U be the affine part of E. Let $\mathbf{E}$ be an Edwards Curve over $\mathbf{W}(k)$ whose reduction modulo p is E and $\mathbf{U}$ the affine part of $\mathbf{E}$. Then there is a lifting of points $\nu : U \to \mathbf{U}$ whose entries are odd polynomials in a single variable (not necessarily an Edwards Lift) given by*

$$\nu((x_0, y_0)) = ((x_0, x_1(x_0), ...), (y_0, y_1(y_0), ...)$$

such that for all n

$$\deg(x_n), \deg(y_n) \leq (n+2)p^n + np^{n-1} + 1.$$

To prove this, we first introduce some notation from [8].

Definition 5.6. Let $\nu : K \to \mathbb{R} \cup \{\infty\}$ be a valuation of the field K. For $e \geq 0$, define:

$$U(e) := \{\mathbf{s} = (s_0, s_1, ...) \in \mathbf{W}(K)^\times : \nu(s_n) \geq p^n(\nu(s_0) - ne),\ \forall n \geq 0\}$$

$$U_r(e) := \{\mathbf{s} = (s_0, s_1, ...) \in \mathbf{W}(K)^\times : \nu(s_n) \geq p^n(\nu(s_0) - ne),\ \forall 0 \leq n \leq r\}.$$

Lemma 2.2 of this paper shows that $U_r(e), U(e)$ form groups.

Proof. Throughout we use the valuation $\upsilon := ord_{\mathcal{Q}^+}$, which has

$$\upsilon(x_0) = -1 \qquad \upsilon(y_0) = 0.$$

Again we prove this by induction, observing it clearly holds for $n = 0$, thus we will assume $n \geq 1$. Consider the $n+1$st coordinate of the $\mathcal{G}(\mathbf{E})$, given as in Equation 4.6.1. We work in $U\left(\frac{p+1}{p}\right)$. Then we have all the omitted terms have valuation greater than or equal to $p^n\left(-2 - n\frac{p+1}{p}\right)$ by Lemma 3.2 of [9]. Thus the degree in x_0 (and then consequently in y_0) is of degree at most $(n+2)p^n + np^{n-1}$. But note that since x_i, y_i are both odd functions for all $i < n$, the omitted terms in the Greenberg Transform use only *even* powers of x_0, y_0 by Lemma 5.1 of [9], seen by applying said lemma to $\mathbf{x}^2, \mathbf{y}^2$ before doing any multiplications that might result in mixed variables.

Thus we may see the $n+1$st coordinate of the Greenberg Transform as

$$\begin{aligned} ... &= 2\left(b_0^2 - a_0y_0^2\right)^{p^n} x_0^{p^n} x_n + 2\left(1 - a_0x_0^2\right)^{p^n} y_0^{p^n} y_n \\ &= 2(1-y_0)^{\frac{p^n+1}{2}}(b_0^2 - a_0y_0^2)^{\frac{p^n-1}{2}}\tilde{F}_n + 2(1-b_0^2x_0^2)^{\frac{p^n+1}{2}}(1-a_0x_0^2)^{\frac{p^n-1}{2}}\tilde{G}_n \end{aligned}$$

Using 2.12 with $t = x_0^2$, and $s = y_0^2$ as our variables and

$$A := 2(1-b_0^2x_0^2)^{\frac{p^n+1}{2}}(1-a_0x_0^2)^{\frac{p^n-1}{2}}, \qquad B := 2(1-y_0^2)^{\frac{p^n+1}{2}}(b_0^2-a_0y_0^2)^{\frac{p^n-1}{2}}$$

and C to be the omitted terms as our functions we find a solution satisfying the desired property. To see $1 \in (A, B)$, observe

$$\left(\frac{y_0^{p^n-1}(b_0^2 - a_0 y_0^2)^{p^n}}{(b_0^2 - a_0)^{p^n}}\right) A + \left(x_0^{p^n-1}\right) B = 2\left(y_0^2\right)^{p^n} + 2\left(1 - y_0^2\right)^{p^n} = 2$$

and since $p \neq 2$, $2 \in k^\times$. □

Note the given lift need not be an Edwards life, all Edwards lifts satisfy the theorem. Thus we have an upper bound for the degree of an Edwards Lift, to an arbitrary Twisted Edwards Curve $\mathbf{E}/\mathbf{W}(k)$ whose reduction modulo p is E.

In order to construct a lower bound, we first compute the derivatives for our absolute minimal degree Edwards lifts, we introduce two theorems which can be found in [9] as Theorem 4.1 and Lemma 4.3.

Theorem 5.7. *Let k be a perfect field of characteristic $p > 0$ and*

$$U/k: \qquad g(x_0, y_0) = 0$$

and an affine curve in $\mathbb{A}^2$. Let

$$\mathbf{U}/\mathbf{W}_{n+1}(k): \qquad \mathbf{g}(\mathbf{x}, \mathbf{y}) = \mathbf{0}$$

be an affine curve with reduction U, i.e. $\mathbf{g}$ reduces to g modulo p. If we have a lift of points $\nu : U(\bar{k}) \to \mathbf{U}(\mathbf{W}_{n+1}(\bar{k}))$ given by

$$\nu((x_0, y_0)) = ((x_0, x_1, ..., x_n), (y_0, y_1, ..., y_n))$$

with $x_i, y_i \in k[x_0, y_0]$, then we have a lift $\boldsymbol{\phi}^n : \mathbf{U} \to \mathbf{U}^{\sigma^n}$ of the p^n-th power Frobenius map associated to ν given by

$$\boldsymbol{\phi}^n((\mathbf{x}, \mathbf{y})) := \left(\mathbf{x}^{p^n} + p\mathbf{x}_1^{p^{n-1}} + ... + p^n\mathbf{x}_n, \mathbf{y}^{p^n} + p\mathbf{y}_1^{p^{n-1}} + ... + p^n\mathbf{y}_n\right)$$

where $\mathbf{x}_i, \mathbf{y}_i \in \mathbf{W}_{n+1}(k)[\mathbf{x}, \mathbf{y}]$ and $\mathbf{x}_i, \mathbf{y}_i$ are lifts of $x_i, y_i \in k[x_0, y_0]$.

Theorem 5.8. *Let C be a curve, $\mathbf{C}$ a lift of C and $\boldsymbol{\phi} : \mathbf{U} \to \mathbf{U}^{\sigma}$ be any lift of the Frobenius between the affine parts. Then if we set $\mathbf{x} = (x_0, x_1, ...)$ and $\mathbf{y} = (y_0, y_1, ...)$, the reductions of $(\boldsymbol{\phi}^*)^n(\mathbf{x}), (\boldsymbol{\phi}^*)^n(\mathbf{y})$ modulo p^{n+1} depend only on x_0, y_0.*

Note Theorem 5.7 is distinct from Proposition 4.3, as Proposition 4.3 relies on the existence of a lifting of the p^n-th power Frobenius map, whereas Theorem 5.7 gives a construction of one modulo p^{n+1}.

With these two theorems, we can approach finding the derivatives of minimal degree Edwards lifts in a similar fashion to the Elliptic Teichmüller . Doing so, allows us to finally introduce a lower bound for the degree of our absolute minimal-degree lifts.

Proposition 5.9. *Let $\nu((x_0, y_0)) = ((x_0, x_1, ..., x_n), (y_0, y_1, ..., y_n))$ (for $n \geq 1$) be a lifting of points (not necessarily an Edwards Lift) from the affine part of an Edwards Curve E_{a_0,b_0} to a lift $\mathbf{E}$ in Edwards Form, where $x_i \in k[x_0], y_i \in k[y_0]$ and*

$$\deg(x_i) = \deg(y_i) = 2p^i - 1$$

for $i = 0, 1, ..., (n-1)$. Then $\deg(x_n), \deg(y_n) \geq 2p^n - 1$ and if equality holds then

$$\frac{dx_n}{dx_0} = A_E^{-(p^n-1)/(p-1)}(b_0^2x_0^2 - 1)^{\frac{p^n-1}{2}}(a_0x_0^2 - 1)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} x_k^{p^{n-k}-1}\frac{dx_k}{dx_0}$$

$$\frac{dy_n}{dy_0} = A_E^{-(p^n-1)/(p-1)}(b_0^2 - a_0y_0^2)^{\frac{p^n-1}{2}}(1 - y_0^2)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} y_k^{p^{n-k}-1}\frac{dy_k}{dy_0}.$$

where A_E is the (necessarily non-zero) coefficient of y_0^{p-1} in $((1-y_0^2)(b_0^2-a_0y_0^2))^{\frac{p-1}{2}}$.

Proof. Firstly, by the above, we have $\boldsymbol{\phi}^n$, a lifting of the p^n-th power Frobenius ϕ^n. As before, let $\mathbf{U}$ denote the affine part of $\mathbf{E}$ and U the affine part of E. Then the reduction modulo p of

$$\left(\frac{1}{p^n}\boldsymbol{\phi}^n\right)^*\left(\frac{\mathbf{2y}d\mathbf{x}}{\mathbf{b}^{2p^n}\mathbf{x}^2-\mathbf{1}}\right)=\left(\frac{1}{p^n}\boldsymbol{\phi}^n\right)^*\left(\frac{\mathbf{2x}d\mathbf{y}}{\mathbf{1}-\mathbf{y}^2}\right)$$

is given by

$$\omega:=\frac{2y_0^{p^n}\left(\sum_{i=0}^n x_i^{p^{n-i}-1}\frac{dx_i}{dx_0}\right)dx_0}{b_0^{2p^n}x_0^{2p^n}-1}=\frac{2x_0^{p^n}\left(\sum_{i=0}^n y_i^{p^{n-i}-1}\frac{dy_i}{dy_0}\right)dy_0}{1-y_0^{2p^n}},$$

by virtue of the fact that

$$\frac{\mathbf{2y}d\mathbf{x}}{\mathbf{b}^{2p^n}\mathbf{x}^2-\mathbf{1}}=\frac{\mathbf{2x}d\mathbf{y}}{\mathbf{1}-\mathbf{y}^2}$$

by Equation (2.1.14).

To ease reading and make computations more intelligible, we write

$$\omega_x:=\frac{2y_0^{p^n}\left(\sum_{i=0}^n x_i^{p^{n-i}-1}\frac{dx_i}{dx_0}\right)dx_0}{b_0^{2p^n}x_0^{2p^n}-1}\qquad\omega_y:=\frac{2x_0^{p^n}\left(\sum_{i=0}^n y_i^{p^{n-i}-1}\frac{dy_i}{dy_0}\right)dy_0}{1-y_0^{2p^n}}$$

as equal representations of the same differential. Again using Equation (2.1.14) we rewrite our representations as

$$\omega_x=\frac{2y_0^{p^n-1}\left(\sum_{i=0}^n x_i^{p^{n-i}-1}\frac{dx_i}{dx_0}\right)x_0dy_0}{(b_0^2x_0^2-1)^{p^n-1}(1-y_0^2)}=\lambda_n\frac{2x_0dy_0}{1-y_0^2}$$

$$\omega_y=\frac{2x_0^{p^n-1}\left(\sum_{i=0}^n y_i^{p^{n-i}-1}\frac{dy_i}{dy_0}\right)y_0dx_0}{(1-y_0^2)^{p^n-1}(b_0^2x_0^2-1)}=\lambda_n\frac{2y_0dx_0}{b_0^2x_0^2-1}$$

for some $\lambda_n\in k(E)$. Note since our invariant differential is regular on U, it must be the case ω_x,ω_y are as well. Thus ω_x must be regular at those points $(\pm 1/b,0)$ and ω_y

must be regular at those points $(0, \pm 1)$. Therefore

$$y_0^{p^n-1} \sum_{i=0}^{n} x_i^{p^{n-i}-1} \frac{dx_i}{dx_0} = \lambda_n \left(b_0^2 x_0^2 - 1\right)^{p^n-1}$$

$$x_0^{p^n-1} \sum_{i=0}^{n} y_i^{p^{n-i}-1} \frac{dy_i}{dy_0} = \lambda_n \left(1 - y_0^2\right)^{p^n-1}$$

where we now see λ_n must be a polynomial. Rewriting

$$\left(b_0^2 x_0^2 - 1\right)^{p^n-1} = y_0^{p^n-1} \left(b_0^2 x_0^2 - 1\right)^{\frac{p^n-1}{2}} \left(a_0 x_0^2 - 1\right)^{\frac{p^n-1}{2}}$$

$$\left(1 - y_0^2\right)^{p^n-1} = x_0^{p^n-1} \left(1 - y_0^2\right)^{\frac{p^n-1}{2}} \left(b_0^2 - a_0 y_0^2\right)^{\frac{p^n-1}{2}}$$

we get

$$\sum_{i=0}^{n} x_i^{p^{n-i}-1} \frac{dx_i}{dx_0} = \lambda_n(x_0, y_0) \left(b_0^2 x_0^2 - 1\right)^{\frac{p^n-1}{2}} \left(a_0 x_0^2 - 1\right)^{\frac{p^n-1}{2}}$$

$$\sum_{i=0}^{n} y_i^{p^{n-i}-1} \frac{dy_i}{dy_0} = \lambda_n(x_0, y_0) \left(1 - y_0^2\right)^{\frac{p^n-1}{2}} \left(b_0^2 - a_0 y_0^2\right)^{\frac{p^n-1}{2}}.$$

Moving terms around gives

$$\frac{dx_n}{dx_0} = \lambda_n (b_0^2 x_0^2 - 1)^{\frac{p^n-1}{2}} (a_0 x_0^2 - 1)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} x_k^{p^{n-k}-1} \frac{dx_k}{dx_0}$$

and

$$\frac{dy_n}{dy_0} = \lambda_n (b_0^2 - a_0 y_0^2)^{\frac{p^n-1}{2}} (1 - y_0^2)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} y_k^{p^{n-k}-1} \frac{dy_k}{dy_0}.$$

Since

$$\deg \left(\lambda_n (b_0^2 x_0^2 - 1)^{\frac{p^n-1}{2}} (a_0 x_0^2 - 1)^{\frac{p^n-1}{2}}\right), \deg \left(\lambda_n (b_0^2 - a_0 y_0^2)^{\frac{p^n-1}{2}} (1 - y_0^2)^{\frac{p^n-1}{2}}\right) \geq 2p^n - 2$$

the inequality of degrees follows.

We show that when the given inequality for the degree of x_n, y_n is an equality,

$\lambda_n = A_E^{-(p^n-1)/(p-1)}$. For $n = 1$ it must be the case that $\lambda_1 = A_E^{-1} \in k^\times$ as our derivative is in characteristic p, thus cannot have a term of degree $p-1$.

To extend the result when we have an equality of degrees to arbitrary n, we proceed by induction, assuming $\lambda_{n-1} = A_E^{-(p^{n-1}-1)/(p-1)}$, i.e.

$$y_0^{p^{n-1}-1} \sum_{i=0}^{n-1} x_i^{p^{n-1-i}-1} \frac{dx_i}{dx_0} = A_E^{-(p^{n-1}-1)/(p-1)} \left(b_0^2 x_0^2 - 1\right)^{p^{n-1}-1},$$

$$x_0^{p^{n-1}-1} \sum_{i=0}^{n-1} y_i^{p^{n-1-i}-1} \frac{dy_i}{dy_0} = A_E^{-(p^{n-1}-1)/(p-1)} \left(1 - y_0^2\right)^{p^{n-1}-1},$$

from which we derive the equalities

$$\left(\frac{y_0^{p^{n-1}-1} \sum_{i=0}^{n-1} x_i^{p^{n-1-i}-1} \frac{dx_i}{dx_0}}{\left(b_0^2 x_0^2 - 1\right)^{p^{n-1}-1}} \right) \left(\frac{2x_0 dy_0}{1 - y_0^2} \right) = A_E^{-(p^{n-1}-1)/(p-1)} \left(\frac{2x_0 dy_0}{1 - y_0^2} \right),$$

$$\left(\frac{x_0^{p^{n-1}-1} \sum_{i=0}^{n-1} y_i^{p^{n-1-i}-1} \frac{dy_i}{dy_0}}{\left(1 - y_0^2\right)^{p^{n-1}-1}} \right) \left(\frac{2y_0 dx_0}{b_0^2 x_0^2 - 1} \right) = A_E^{-(p^{n-1}-1)/(p-1)} \left(\frac{2y_0 dx_0}{b_0^2 x_0^2 - 1} \right).$$

Since we are assuming equality for the degrees in the $n+1$st coordinate, we see it must be the case that $\lambda_n \in k^\times$, else

$$\deg\left(\lambda_n (b_0^2 x_0^2 - 1)^{\frac{p^n-1}{2}} (a_0 x_0^2 - 1)^{\frac{p^n-1}{2}}\right), \deg\left(\lambda_n (b_0^2 - a_0 y_0^2)^{\frac{p^n-1}{2}} (1 - y_0^2)^{\frac{p^n-1}{2}}\right) \geq 2p^n - 1$$

thus the formal integral of them would be of degree at least $2p^n$. Applying the Cartier Operator to our representations yields

$$\begin{aligned}
\mathcal{C}(\omega_x) &= \mathcal{C}\left(\frac{2y_0^{p^n}\left(\sum_{i=0}^{n} x_i^{p^{n-i}-1}\frac{dx_i}{dx_0}\right)dx_0}{b_0^{2p^n}x_0^{2p^n}-1}\right) \\
&= \frac{2y_0^{p^{n-1}}\left(\sum_{i=0}^{n-1} x_i^{p^{n-1-i}-1}\frac{dx_i}{dx_0}\right)dx_0}{(b_0^2x_0^2-1)^{p^{n-1}}} \\
&= \frac{2y_0^{p^{n-1}-1}\left(\sum_{i=0}^{n-1} x_i^{p^{n-1-i}-1}\frac{dx_i}{dx_0}\right)x_0dy_0}{(b_0^2x_0^2-1)^{p^{n-1}-1}(1-y_0^2)} \\
&= A_E^{-(p^{n-1}-1)/(p-1)}\frac{2x_0dy_0}{1-y_0^2}
\end{aligned}$$

and

$$\begin{aligned}
\mathcal{C}(\omega_y) &= \mathcal{C}\left(\frac{2x_0^{p^n}\left(\sum_{i=0}^{n} y_i^{p^{n-i}-1}\frac{dy_i}{dy_0}\right)dy_0}{1-y_0^{2p^n}}\right) \\
&= \frac{2x_0^{p^{n-1}}\left(\sum_{i=0}^{n-1} y_i^{p^{n-1-i}-1}\frac{dy_i}{dy_0}\right)dy_0}{(1-y_0^2)^{p^{n-1}}} \\
&= \frac{2x_0^{p^{n-1}-1}\left(\sum_{i=0}^{n-1} y_i^{p^{n-1-i}-1}\frac{dy_i}{dy_0}\right)y_0dx_0}{(1-y_0^2)^{p^{n-1}-1}(b_0^2x_0^2-1)} \\
&= A_E^{-(p^{n-1}-1)/(p-1)}\frac{2y_0dy_x}{b_0^2x_0^2-1}.
\end{aligned}$$

But we would also then have

$$\mathcal{C}(\omega_x) = \lambda_n^{1/p}A_E^{1/p}\frac{2x_0dy_0}{1-y_0^2} \qquad \mathcal{C}(\omega_y) = \lambda_n^{1/p}A_E^{1/p}\frac{2y_0dx_0}{b_0^2x_0^2-1}$$

hence $\lambda_n = A_E^{-(p^n-1)/(p-1)}$ giving the desired result. □

5.2 Existence of Absolute Minimal Lifts Modulo p^3

Let $\mathbf{E_{a,b}}/\mathbf{W}(k)$ be the Canonical Lift of an Edwards Curve $E_{a_0,b_0}/k$, and τ the Elliptic Teichmüller Lift. Note

$$\deg(x_1) = \deg(y_1) = 2p - 1$$

and τ satisfies the requirement of an Edwards Lift modulo p^2. Thus there exists an absolute minimal degree curve modulo p^2 (namely, $\mathbf{E_{a,b}}$) with an absolute minimal degree Edwards lift modulo p^2 (namely τ). We claim there exists an absolute minimal degree lifting of points $\nu((x_0, y_0)) = ((x_0, x_1, \tilde{x}_2), (y_0, y_1, \tilde{y}_2))$ from E_{a_0,b_0} to $\mathbf{E_{a,b}}$.

The Case $p = 5, 7$

For the $p = 5, 7$ cases, we computationally verify the existence of an absolute minimal degree lift modulo p^3 of $b_0^2x_0^2 + y_0^2 = 1 + a_0x_0^2y_0^2$ to its Canonical Lift and in fact, verify the method below gives the absolute minimal degree lifting of points. However, a step used in the computation involves considering a polynomial of degree $\frac{p-9}{2}$, so we will assume that $p > 7$ and hope to assuage any concerns the reader may have by directing them to the code available at https://github.com/lrfinotti/witt.

The Case $p > 7$

Assume we have chosen a representation of the Canonical Lift such that $\mathbf{b} = (b_0, 0, 0)$ modulo p^3. Such an assumption can be made by taking advantage of our degree of freedom within our given algorithm. By 4.12.3

$$deg\left(x_0^{p^2}x_2 - x_1^{2p}\right) \leq 3p^2 - 1, \qquad deg\left(y_0^{p^2}y_2 - y_1^{2p}\right) \leq 3p^2 - 1.$$

Apply the division algorithm to x_1^2, y_1^2 to get

$$x_1^2 = x_0^{p+1}(b_0^2x_0^2 - 1)^{\frac{p+1}{2}}(a_0x_0^2 - 1)(a_0b_0^2x_0^4 - 2b_0^2x_0^2 + 1) \cdot q(x_0^2) + r(x_0^2) \tag{5.9.1}$$

$$y_1^2 = y_0^{p+1}(y_0^2 - 1)^{\frac{p+1}{2}}(a_0y_0^2 - b_0^2)(a_0y_0^4 - 2b_0^2y_0^2 + b_0^2) \cdot g(y_0^2) + h(y_0^2). \tag{5.9.2}$$

where $\deg(q), \deg(g) = p - 5$ and $\deg(r), \deg(h) \leq p + 3$. Such decompositions exist by looking at the division algorithm applied to

$$tF_1^2(t) = t^{\frac{p+1}{2}}(b_0^2t - 1)^{\frac{p+1}{2}}(a_0t - 1)(a_0t^2 - 2t + 1)q(t) + r(t)$$

$$tG_1^2(t) = t^{\frac{p+1}{2}}(t - 1)^{\frac{p+1}{2}}(a_0t - b_0^2)(a_0t^2 - 2b_0^2t + b_0^2) \cdot g(t) + h(t)$$

since $x_1 = x_0F_1(x_0^2), y_1 = y_0G_1(y_0^2)$ as they must be odd functions. Additionally, we observe

$$\begin{aligned}(a_0b_0^2x_0^4 - 2b_0^2x_0^2 + 1)(a_0y_0^2 - b_0^2) &= (b_0^2 - a_0)(b_0^2x_0^2 - y_0^2).\\ (a_0y_0^4 - 2b_0^2y_0^2 + b_0^2)(a_0x_0^2 - 1) &= -(b_0^2 - a_0)(b_0^2x_0^2 - y_0^2).\end{aligned} \tag{5.9.3}$$

Continuing, we further decompose the results of our division by writing $q(t), g(t)$ as

$$q(t) = \sum_{i=0}^{\frac{p-5}{2}} \alpha_i(t(b_0^2t - 1))^{\frac{p-5}{2}-i}(a_0t - 1)^i + \tilde{q}(t)$$

$$g(t) = \sum_{i=0}^{\frac{p-5}{2}} \beta_i(t(t - 1))^{\frac{p-5}{2}-i}(a_0t - b_0^2)^i + \tilde{g}(t)$$

where $\alpha_i, \beta_i \in k$ and $\deg(\tilde{q}), \deg(\tilde{g}) \leq \frac{p-7}{2}$. In both cases, such a decomposition is unique by repeated use of the division algorithm.

Lemma 5.10. *For all i, $\alpha_i = \beta_i$.*

Proof. The assumption $\mathbf{b} = (b_0, 0, 0)$ in combination with the third involution for the elliptic Teichmüller $(x_0, y_0) \mapsto \left(\frac{y_0}{b_0}, b_0 x_0\right)$ gives us the equality

$$y_1(b_0 x_0) = b_0^p x_1.$$

where $y_1(b_0 x_0)$ denotes the evaluation of y_1 at the value of $b_0 x_0$. Thus

$$\begin{aligned}
y_1^2(b_0 x_0) &= b_0^{p+1} x_0^{p+1} (b_0^2 x_0^2 - 1)^{\frac{p+1}{2}} (a_0 b_0^2 x_0^2 - b_0^2)(a_0 b_0^4 x_0^4 - 2b_0^4 x_0^2 + b_0^2) \cdot g(b_0^2 y_0^2) + h(b_0^2 y_0^2) \\
&= b_0^{p+5} x_0^{p+1} (b_0^2 x_0^2 - 1)^{\frac{p+1}{2}} (a_0 x_0^2 - 1)(a_0 b_0^2 x_0^4 - 2b_0^2 x_0^2 + 1) \cdot g(b_0^2 y_0^2) + h(b_0^2 y_0^2) \\
&= b_0^{2p} x_0^{p+1} (b_0^2 x_0^2 - 1)^{\frac{p+1}{2}} (a_0 x_0^2 - 1)(a_0 b_0^2 x_0^4 - 2b_0^2 x_0^2 + 1) \\
&\times \left(\sum_{i=0}^{\frac{p-5}{2}} \beta_i (x_0^2 (b_0^2 x_0^2 - 1))^{\frac{p-5}{2} - i} (a_0 x_0^2 - 1)^i + \tilde{g}(b_0^2 x_0^2) \right) + h(b_0^2 x_0^2).
\end{aligned}$$

Note (by expanding $q(x_0^2)$) the decomposition of x_1^2 as

$$\begin{aligned}
&x_0^{p+1} (b_0^2 x_0^2 - 1)^{\frac{p+1}{2}} (a_0 x_0^2 - 1)(a_0 b_0^2 x_0^4 - 2b_0^2 + 1) \\
&\times \left(\sum_{i=0}^{\frac{p-5}{2}} \alpha_i (x_0^2 (b_0^2 x_0^2 - 1))^{\frac{p-5}{2} - i} (a_0 x_0^2 - 1)^i + \tilde{q}(x_0^2) \right) + r(x_0^2)
\end{aligned}$$

must be the unique decomposition satisfying $\deg(r) \leq p + 3$ and since

$$\begin{aligned}
\frac{1}{b_0^{2p}} y_1^2(b_0 x_0) &= x_0^{p+1} (b_0^2 x_0^2 - 1)^{\frac{p+1}{2}} (a_0 x_0^2 - 1)(a_0 b_0^2 x_0^4 - 2b_0^2 + 1) \\
&\times \left(\sum_{i=0}^{\frac{p-5}{2}} \beta_i (x_0^2 (b_0^2 x_0^2 - 1))^{\frac{p-5}{2} - i} (a_0 x_0^2 - 1)^i + \tilde{g}(b_0^2 x_0^2) \right) \\
&+ \frac{1}{b_0^{2p}} h(b_0^2 x_0^2)
\end{aligned}$$

gives a decomposition of x_1^2 such that $deg\left(\frac{1}{b_0^{2p}} h\right) \leq p+3$, it follows these decompositions must be equal. Thus the quotients and the remainders are equal and so $\alpha_i = \beta_i$

for all i by descent counting on leading coefficients, $\tilde{g}(b_0^2x_0^2) = \tilde{q}(x_0^2)$, and $h(b_0^2x_0^2) = b_0^{2p}r(x_0^2)$. $\square$

Lemma 5.11. *In the above* $\deg(\tilde{q}), \deg(\tilde{g}) \leq \frac{p-9}{2}$.

Proof. It suffices to prove $\deg(\tilde{q}) \leq \frac{p-9}{2}$ as we know $\tilde{g}(b_0^2x_0^2) = \tilde{q}(x_0^2)$ and thus their degrees are equal. To this end, let c be the coefficient of $t^{\frac{p-7}{2}}$ in $\tilde{q}$. We now define two polynomials that will prove important to current future constructions

$$\begin{aligned} f &:= \sum_{i=0}^{\frac{p-5}{2}} \alpha_i (t(b_0^2t-1))^{\frac{p-5}{2}-i}(a_0t-1)^i \\ \varphi &:= \sum_{i=0}^{\frac{p-5}{2}} \alpha_i (t(t-1))^{\frac{p-5}{2}-i}(a_0t-b_0^2)^i. \end{aligned} \tag{5.11.1}$$

which allows us to write $q(t) = f(t) + \tilde{q}(t)$ and $g(t) = \varphi(t) + \tilde{g}(t)$. Consider the derivative of the function x_1^3 with respect to x_0, given by

$$\begin{aligned} &3x_1^2\frac{dx_1}{dx_0} \\ =&3\left(x_0^{p+1}(b_0^2x_0^2-1)^{\frac{p+1}{2}}(a_0x_0^2-1)(a_0b_0^2x_0^4-2b_0^2x_0^2+1)q(x_0^2)+r(x_0^2)\right) \\ &\times\left(A_E^{-1}(b_0^2x_0^2-1)^{\frac{p-1}{2}}(a_0x_0^2-1)^{\frac{p-1}{2}}-x_0^{p-1}\right) \\ =&3\left(x_0^{p+1}(b_0^2x_0^2-1)^{\frac{p+1}{2}}(a_0x_0^2-1)(a_0b_0^2x_0^4-2b_0^2x_0^2+1)f(x_0^2)+r(x_0^2)\right) \\ &\times\left(A_E^{-1}(b_0^2x_0^2-1)^{\frac{p-1}{2}}(a_0x_0^2-1)^{\frac{p-1}{2}}-x_0^{p-1}\right) \\ +&3\left(x_0^{p+1}(b_0^2x_0^2-1)^{\frac{p+1}{2}}(a_0x_0^2-1)(a_0b_0^2x_0^4-2b_0^2x_0^2+1)\tilde{q}(x_0^2)\right) \\ &\times\left(A_E^{-1}(b_0^2x_0^2-1)^{\frac{p-1}{2}}(a_0x_0^2-1)^{\frac{p-1}{2}}-x_0^{p-1}\right) \end{aligned}$$

Note the coefficient of x_0^{5p-1} in the last product is given by $3A_E^{-1}a_0^{\frac{p+3}{2}}b_0^{2p+2}c$. Since our curve is assumed to be ordinary,

$$3A_E^{-1}a_0^{\frac{p+3}{2}}b_0^{2p+2} \neq 0,$$

so the coefficient is 0 exactly when $c = 0$.

The remainder of this proof will show the derivative of x_1^3 has no other term in x_0^{5p-1}, and thus such a coefficient must be 0 and therefore $c = 0$. To this end, observe that

$$\deg\left(r(x_0^2)\left(A_E^{-1}(b_0^2x_0^2-1)^{\frac{p-1}{2}}(a_0x_0^2-1)^{\frac{p-1}{2}}-x_0^{p-1}\right)\right) \leq 4p+4 < 5p-1$$

$$\deg\left(3x_0^{2p}(x_0^2-1)^{\frac{p+1}{2}}(a_0x_0^2-1)(a_0b_0^2x_0^4-2b_0^2x_0^2+1)f(x_0^2)\right) \leq 5p-3 < 5p-1.$$

Thus neither product may contribute a term in x_0^{5p-1}. As such, any additional term in x_0^{5p-1} must come from the product

$$3x_0^{p+1}(b_0^2x_0^2-1)^{\frac{p+1}{2}}(a_0x_0^2-1)(a_0b_0^2x_0^4-2b_0^2x_0^2+1)f(x_0^2)\cdot A_E^{-1}(b_0^2x_0^2-1)^{\frac{p-1}{2}}(a_0x_0^2-1)^{\frac{p-1}{2}}$$

which we can simplify to

$$3A_E^{-1}x_0^{p+1}(b_0^2x_0^2-1)^p(a_0x_0^2-1)^{\frac{p+1}{2}}(a_0b_0^2x_0^4-2b_0^2x_0^2+1)f(x_0^2). \tag{5.11.2}$$

We now drop the non-zero coefficient $3A_E^{-1} \neq 0$ from subsequent computations. Since

$$deg\left(x_0^{p+1}(a_0x_0^2-1)^{\frac{p+1}{2}}(a_0b_0^2x_0^4-2b_0^2x_0^2+1)f(x_0^2)\right) = 4p-4 < 5p-1$$

and

$$(b_0^2x_0^2-1)^p = (b_0^{2p}x_0^{2p}-1)$$

the coefficient of x_0^{5p-1} in their product must be the coefficient of x_0^{3p-1} in the former. This in turn must be the coefficient of x_0^{2p-2} in

$$(a_0x_0^2-1)^{\frac{p+1}{2}}(a_0b_0^2x_0^4-2b_0^2x_0^2+1)f(x_0^2)$$

which is then the coefficient of t^{p-1} in

$$(a_0t-1)^{\frac{p+1}{2}}(a_0b_0^2t^2-2b_0^2t+1)f(t).$$

Expanding $f(t)$, we show for all $0\leq i\leq \frac{p-5}{2}$ the coefficient of t^{p-1} in

$$\begin{aligned}&(a_0t-1)^{\frac{p+1}{2}}(a_0b_0^2t^2-2b_0^2t+1)(t(b_0^2t-1))^{\frac{p-5}{2}-i}(a_0t-1)^i\\ =&(a_0t-1)^{\frac{p+1}{2}+i}(t(b_0^2t-1))^{\frac{p-5}{2}-i}(a_0b_0^2t^2-2b_0^2t+1)\end{aligned}$$

is 0. For $0\leq i\leq \frac{p-7}{2}$ we expand our product as

$$\begin{aligned}&\left(\sum_{\ell=0}^{\frac{p+1}{2}+i}\sum_{k=0}^{\frac{p-5}{2}-i}(-1)^{\ell+k}\binom{\frac{p+1}{2}+i}{\ell}\binom{\frac{p-5}{2}-i}{k}a_0^{\frac{p+1}{2}+i-\ell}b_0^{2\left(\frac{p-5}{2}-i-k\right)}t^{\frac{3p-9}{2}-i-k-\ell}\right)\\ &\times(a_0b_0^2t^2-2b_0^2t+1)\\ =&\sum_{\ell=0}^{\frac{p+1}{2}+i}\sum_{k=0}^{\frac{p-5}{2}-i}(-1)^{\ell+k}\binom{\frac{p+1}{2}+i}{\ell}\binom{\frac{p-5}{2}-i}{k}a_0^{\frac{p+3}{2}+i-\ell}b_0^{2\left(\frac{p-3}{2}-i-k\right)}t^{\frac{3p-5}{2}-i-k-\ell}\\ &+2\sum_{\ell=0}^{\frac{p+1}{2}+i}\sum_{k=0}^{\frac{p-5}{2}-i}(-1)^{\ell+k+1}\binom{\frac{p+1}{2}+i}{\ell}\binom{\frac{p-5}{2}-i}{k}a_0^{\frac{p+1}{2}+i-\ell}b_0^{2\left(\frac{p-3}{2}-i-k\right)}t^{\frac{3p-7}{2}-i-k-\ell}\\ &+\sum_{\ell=0}^{\frac{p+1}{2}+i}\sum_{k=0}^{\frac{p-5}{2}-i}(-1)^{\ell+k}\binom{\frac{p+1}{2}+i}{\ell}\binom{\frac{p-5}{2}-i}{k}a_0^{\frac{p+1}{2}+i-\ell}b_0^{2\left(\frac{p-5}{2}-i-k\right)}t^{\frac{3p-9}{2}-i-k-\ell}\end{aligned}$$

The coefficient of t^{p-1} in each of the three sums, comes from $k+\ell=\frac{p-3}{2}-i$ in the first sum, $\frac{p-5}{2}-i$ in the second, and $\frac{p-7}{2}-i$ in the third. Thus the coefficient of t^{p-1} is

$$\begin{aligned}
&\sum_{k=0}^{\frac{p-5}{2}-i}(-1)^{\frac{p-3}{2}-i}\binom{\frac{p+1}{2}+i}{\frac{p-3}{2}-i-k}\binom{\frac{p-5}{2}-i}{k}a_0^{3+2i+k}b_0^{2\left(\frac{p-3}{2}-i-k\right)}\\
&+2\sum_{k=0}^{\frac{p-5}{2}-i}(-1)^{\frac{p-3}{2}-i}\binom{\frac{p+1}{2}+i}{\frac{p-5}{2}-i-k}\binom{\frac{p-5}{2}-i}{k}a_0^{3+2i+k}b_0^{2\left(\frac{p-3}{2}-i-k\right)}\\
&+\sum_{k=0}^{\frac{p-7}{2}-i}(-1)^{\frac{p-7}{2}-i}\binom{\frac{p-5}{2}-i}{k}\binom{\frac{p+1}{2}+i}{\frac{p-7}{2}-k-i}a_0^{2i+k+4}b_0^{2\left(\frac{p-5}{2}-i-k\right)}\\
&=(-1)^{\frac{p-3}{2}-i}a_0^{2i+3}b_0^{p-3-2i}\left(\sum_{k=0}^{\frac{p-5}{2}-i}\binom{\frac{p+1}{2}+i}{\frac{p-3}{2}-i-k}\binom{\frac{p-5}{2}-i}{k}a_0^kb_0^{-2k}\right.\\
&+2\sum_{k=0}^{\frac{p-5}{2}-i}\binom{\frac{p+1}{2}+i}{\frac{p-5}{2}-i-k}\binom{\frac{p-5}{2}-i}{k}a_0^kb_0^{-2k}\\
&\left.+\sum_{k=0}^{\frac{p-7}{2}-i}\binom{\frac{p-5}{2}-i}{k}\binom{\frac{p+1}{2}+i}{\frac{p-7}{2}-k-i}a_0^{k+1}b_0^{-2(k+1)}\right).
\end{aligned}$$

Dropping the non-zero constant $(-1)^{\frac{p-3}{2}-i}a_0^{2i+3}b_0^{p-3-2i}$, isolating the $k=0$ terms in the first two summations, and then re-parameterizing, we are left with

$$\begin{aligned}
&\binom{\frac{p+1}{2}+i}{\frac{p-3}{2}-i}+2\binom{\frac{p+1}{2}+i}{\frac{p-5}{2}-i}\\
&+\sum_{k=0}^{\frac{p-7}{2}-i}\left(\binom{\frac{p-5}{2}-i}{k+1}\binom{\frac{p+1}{2}+i}{\frac{p-5}{2}-k-i}+2\binom{\frac{p-5}{2}-i}{k+1}\binom{\frac{p+1}{2}+i}{\frac{p-7}{2}-k-i}\right.\\
&\left.+\binom{\frac{p-5}{2}-i}{k}\binom{\frac{p+1}{2}+i}{\frac{p-7}{2}-k-i}\right)\frac{a_0^{k+1}}{b_0^{2(k+1)}}
\end{aligned}$$

where the first pair of terms comes from the $k=0$ part of the first two sums.

Firstly,

$$\begin{aligned}\binom{\frac{p+1}{2}+i}{\frac{p-3}{2}-i}+2\binom{\frac{p+1}{2}+i}{\frac{p-5}{2}-i} &= \left(\frac{\left(\frac{p+1}{2}+i\right)!}{\left(\frac{p-5}{2}-i\right)!\,(2+2i)!}\right)\left(\frac{1}{\frac{p-3}{2}-i}+\frac{2}{3+2i}\right)\\ &= \left(\frac{\left(\frac{p+1}{2}+i\right)!}{\left(\frac{p-5}{2}-i\right)!\,(2+2i)!}\right)\left(\frac{p}{\left(\frac{p-3}{2}-i\right)(3+2i)}\right).\end{aligned}$$

Given the bounds on i, both $\left(\frac{\left(\frac{p+1}{2}+i\right)!}{\left(\frac{p-5}{2}-i\right)!(2+2i)!}\right)$ and $\left(\frac{p-3}{2}-i\right)(3+2i)$ (as elements of $\mathbb{Z}$) are coprime to p, thus are units in $\mathbb{F}_p$. Thus

$$\binom{\frac{p+1}{2}+i}{\frac{p-3}{2}-i}+2\binom{\frac{p+1}{2}+i}{\frac{p-5}{2}-i}=0.$$

In a similar fashion, now using Pascal's Identity

$$\begin{aligned}&\binom{\frac{p-5}{2}-i}{k+1}\binom{\frac{p+1}{2}+i}{\frac{p-5}{2}-k-i}+2\binom{\frac{p-5}{2}-i}{k+1}\binom{\frac{p+1}{2}+i}{\frac{p-7}{2}-k-i}+\binom{\frac{p-5}{2}-i}{k}\binom{\frac{p+1}{2}+i}{\frac{p-7}{2}-k-i}\\ =&\binom{\frac{p-5}{2}-i}{k+1}\binom{\frac{p+3}{2}+i}{\frac{p-5}{2}-k-i}+\binom{\frac{p-3}{2}-i}{k+1}\binom{\frac{p+1}{2}+i}{\frac{p-7}{2}-k-i}\\ =&\frac{\left(\frac{p-5}{2}-i\right)!\left(\frac{p+1}{2}+i\right)!}{(k+1)!\left(\frac{p-5}{2}-i-k\right)!\left(\frac{p-7}{2}-i-k\right)!\,(2i+k+4)!}\left(\left(\frac{p+3}{2}+i\right)+\left(\frac{p-3}{2}-i\right)\right)\\ =&0\end{aligned}$$

as an element of $\mathbb{F}_p$, by virtue of the fact

$$\begin{aligned}k\leq\frac{p-7}{2}-i &\implies 2i+k+4\leq\frac{p+1}{2}+i\leq\frac{p+1}{2}+\frac{p-7}{2}=p-3\\ &\implies p\nmid(2i+k+4)!\end{aligned}$$

which is the only term not in our denominator not obviously coprime to p. Thus our result holds for $0\leq i\leq\frac{p-7}{2}$.

Lastly, for $i = \frac{p-5}{2}$ we see

$$\begin{aligned}
&(a_0t-1)^{p-2}(a_0b_0^2t^2-2b_0^2t+1)\\
=&\sum_{k=0}^{p-2}\binom{p-2}{k}(-1)^k a_0^{p-2-k}t^{p-2-k}(a_0b_0^2t^2-2b_0^2t+1)\\
=&\sum_{k=0}^{p-2}\binom{p-2}{k}(-1)^k a_0^{p-1-k}b_0^2t^{p-k}+2\sum_{k=0}^{p-2}\binom{p-2}{k}(-1)^{k+1}a_0^{p-2-k}b_0^2t^{p-1-k}\\
+&\sum_{k=0}^{p-2}\binom{p-2}{k}(-1)^k a_0^{p-2-k}t^{p-2-k}.
\end{aligned}$$

Thus the coefficient of t^{p-1} will be

$$-a_0^{p-2}b_0^2\left(\binom{p-2}{1}+2\right)=-pa_0^{p-2}=0.$$

Summarizing, we have shown the coefficient of x_0^{5p-1} in $\frac{d(x_1^3)}{dx_0}$ is exactly $3A_E^{-1}a_0^{\frac{p+3}{2}}b_0^{2p+2}c$, thus c must be 0, from which it follows $\deg(\tilde{q}), \deg(\tilde{g}) \leq \frac{p-9}{2}$. □

With our lemmas proven, we can write

$$\begin{aligned}
x_1^2 &= x_0^{p+1}(b_0^2x_0^2-1)^{\frac{p+1}{2}}(a_0x_0^2-1)(a_0b_0^2x_0^4-2b_0^2x_0^2+1)f(x_0^2)+\tilde{r}(x_0^2)\\
y_1^2 &= y_0^{p+1}(y_0^2-1)^{\frac{p+1}{2}}(a_0y_0^2-b_0^2)(a_0y_0^4-2b_0^2y_0^2+b_0^2)\varphi(y_0^2)+\tilde{h}(y_0^2),
\end{aligned} \tag{5.11.3}$$

where

$$\tilde{r}(x_0^2) := r(x_0^2)+x_0^{p+1}(b_0^2x_0^2-1)^{\frac{p+1}{2}}(a_0x_0^2-1)(a_0b_0^2x_0^4-2b_0^2x_0^2+1)\tilde{q}(x_0^2)$$

$$\tilde{h}(x_0^2) := h(y_0^2)+y_0^{p+1}(y_0^2-1)^{\frac{p+1}{2}}(a_0y_0^2-b_0^2)(a_0y_0^4-2b_0^2y_0^2+b_0^2)\tilde{g}(y_0^2),$$

both have degrees at most $3p-1$, as $r(x_0^2), h(y_0^2)$ both have degree at most $2p+6 \leq 3p-1$.

Define $d(x_0) := x_0^{p^2} x_2 - x_1^{2p}$, where we know $\deg(d) \leq 3p^2 - 1$. Observe

$$\begin{aligned} x_0^{p^2} x_2 &= x_1^{2p} + d(x_0) \\ &= x_0^{p^2+p}(b_0^2 x_0^2 - 1)^{\frac{p^2+p}{2}}(a_0 x_0^2 - 1)^p (a_0 b_0^2 x_0^4 - 2b_0^2 x_0^2 + 1)^p f(x_0^2)^p \\ &+ \left(\tilde{r}(x_0^2)^p + d(x_0)\right). \end{aligned}$$

Define

$$\tilde{x}_2 := \frac{\tilde{r}(x_0^2)^p + d(x_0)}{x_0^{p^2}} \in k[x_0].$$

Similarly define $\delta(y_0) := y_0^{p^2} y_2 - y_1^{2p}$ and

$$\tilde{y}_2 := \frac{\tilde{h}(y_0^2)^p + \delta(y_0)}{y_0^{p^2}} \in k[y_0].$$

We claim

$$(x_0, y_0) \mapsto ((x_0, x_1, \tilde{x}_2), (y_0, y_1, \tilde{y}_2))$$

gives and absolute minimal degree Edwards Lift modulo p^3 from E_{a_0,b_0} to $\mathbf{E_{a,b}}$.

Observe since $\deg(d), \deg(\delta), \deg(\tilde{r})^p, \deg(\tilde{h})^p \leq 3p^2 - 1$

$$\deg(\tilde{x}_2), \deg(\tilde{y}_2) \leq 2p^2 - 1$$

and it thus will be equality if the given map is an Edwards Lift.

Next, we show

$$\tilde{x}_2 = x_0 \tilde{F}_2(x_0^2)$$

for some polynomial $\tilde{F}_2$, as then we will have x_2 uses only odd powers of x_0. We know $x_1 = x_0 F_1(x_0^2)$ and $x_2 = x_0 F_2(x_0^2)$, thus

$$d(x_0) = x_0^{p^2+1} F_2(x_0^2) - x_0^{2p} F_1(x_0^2)^{2p}$$

thus $d(x_0)$ uses only even powers of x_0, i.e. $d(x_0) = \tilde{d}(x_0^2)$ for some $\tilde{d}$. But since $x_0^{p^2} \mid d(x_0) + r(x_0^2)^p = \tilde{d}(x_0^2) + r(x_0^2)^p$, it follows

$$x_0^{p^2+1} \mid \tilde{d}(x_0^2) + r(x_0^2)^p$$

Thus we can write

$$\tilde{d}(x_0^2) + r(x_0^2)^p = x_0^{p^2+1}\tilde{F}_2(x_0^2) \implies \tilde{x}_2 := \frac{\tilde{d}(x_0^2) + r(x_0^2)^p}{x_0^{p^2}} = x_0\tilde{F}_2(x_0^2).$$

Similar argumentation gives the result for $\tilde{y}_2$. Thus our map $((x_0, y_0)) \mapsto ((x_0, x_1, \tilde{x}_2), (y_0, y_1, \tilde{y}_2))$ satisfies

$$(-x_0, y_0) \mapsto ((-x_0, -x_1, -\tilde{x}_2), (y_0, y_1, \tilde{y}_2)) \qquad (x_0, -y_0) \mapsto ((x_0, x_1, \tilde{x}_2), (-y_0, -y_1, -\tilde{y}_2)).$$

Thirdly, we show ν gives a lifting of points modulo p^3, observing

$$\begin{aligned}
&2x_0^{p^2}x_2(a_0y_0^2 - b_0^2)^{p^2} + 2y_0^{p^2}y_2(a_0x_0^2 - 1)^{p^2} \\
=&2\left(x_0^{p^2+p}(b_0^2x_0^2 - 1)^{\frac{p^2+p}{2}}(a_0x_0^2 - 1)^p(a_0b_0^2x_0^4 - 2b_0^2x_0^2 + 1)^p f(x_0^2)^p + x_0^{p^2}\tilde{x}_2\right)(a_0y_0^2 - b_0^2)^{p^2} \\
+&2\left(y_0^{p^2+p}(y_0^2 - 1)^{\frac{p^2+p}{2}}(a_0y_0^2 - b_0^2)^p(a_0y_0^4 - 2b_0^2y_0^2 + b_0^2)^p\varphi(y_0^2)^p + y_0^{p^2}\tilde{y}_2\right)(a_0x_0^2 - 1)^{p^2} \\
=&2x_0^{p^2+p}y_0^{p^2+p}\left((a_0x_0^2 - 1)^{\frac{p^2+3p}{2}}(a_0b_0^2x_0^4 - 2b_0^2x_0^2 + 1)^p f(x_0^2)^p\right)(a_0y_0^2 - b_0^2)^{p^2} \\
+&2x_0^{p^2+p}y_0^{p^2+p}\left((a_0y_0^2 - b_0^2)^{\frac{p^2+3p}{2}}(a_0y_0^4 - 2b_0^2y_0^2 + b_0^2)^p\varphi(y_0^2)^p\right)(a_0x_0^2 - 1)^{p^2} \\
+&2x_0^{p^2}\tilde{x}_2(a_0y_0^2 - b_0^2)^{p^2} + y_0^{p^2}\tilde{y}_2(a_0x_0^2 - 1)^{p^2} \\
=&2x_0^{p^2+p}y_0^{p^2+p}(b_0^2 - a_0)^{\frac{p^2+5p}{2}}(b_0^2x_0^2 - y_0^2)^p\left(f(x_0^2)(a_0y_0^2 - b_0^2)^{\frac{p-5}{2}} - \varphi(y_0^2)(a_0x_0^2 - 1)^{\frac{p-5}{2}}\right)^p \\
+&2x_0^{p^2}\tilde{x}_2(a_0y_0^2 - b_0^2)^{p^2} + y_0^{p^2}\tilde{y}_2(a_0x_0^2 - 1)^{p^2} \\
=&2x_0^{p^2}\tilde{x}_2(a_0y_0^2 - b_0^2)^{p^2} + y_0^{p^2}\tilde{y}_2(a_0x_0^2 - 1)^{p^2}
\end{aligned}$$

where f, φ are as in 5.11.1 and we have implicitly used the fact

$$f(x_0^2)(a_0y_0^2 - b_0^2)^{\frac{p-5}{2}} = \varphi(y_0^2)(a_0x_0^2 - 1)^{\frac{p-5}{2}}$$

which can be seen by the construction of f, φ and the fact that

$$\begin{aligned}
&(a_0y_0^2 - b_0^2)^{\frac{p-5}{2}} \left(x_0^2(b_0^2x_0^2 - 1)\right)^{\frac{p-5}{2}-i} (a_0x_0^2 - 1)^i \\
=&(b_0^2 - a_0)^i(y_0^2 - 1)^{\frac{p-5}{2}-i}(b_0^2x_0^2 - 1)^{\frac{p-5}{2}-i} \\
=&(a_0x_0^2 - 1)^{\frac{p-5}{2}} \left(y_0^2(y_0^2 - 1)\right)^{\frac{p-5}{2}-i} (a_0y_0^2 - b_0^2)^i.
\end{aligned}$$

Lastly, we show our third condition holds, namely

$$\mathbf{x} \circ \nu \left(\frac{y_0}{b_0}, b_0x_0\right) = \frac{(y_0, y_1, \tilde{y}_2)}{\mathbf{b}}, \qquad \mathbf{y} \circ \nu \left(\frac{y_0}{b_0}, b_0x_0\right) = \mathbf{b} \cdot (x_0, x_1, \tilde{x}_2).$$

Since we know ν and τ are equivalent modulo p^2, we know this holds for the first two coordinates, thus we need only show it for the third.

Since $\mathbf{b} = (b_0, 0, 0)$, by the third involution for the elliptic Teichmüller , we know

$$y_2 (b_0x_0) = b_0^{p^2} x_2.$$

Manipulating the definition of $\tilde{y}_2$, we find

$$\begin{aligned}
y_2(b_0x_0) &= (b_0x_0)^p(b_0^2x_0^2 - 1)^{\frac{p^2+p}{2}}(a_0b_0^2x_0^2 - b_0^2)^p(a_0b_0^4x_0^4 - 2b_0^4x_0^2 + b_0^2)^p\varphi(b_0^2x_0^2)^p + \tilde{y}_2(b_0x_0) \\
&= b_0^{p^2} \left(x_0^p(b_0^2x_0^2 - 1)^{\frac{p^2+p}{2}}(a_0x_0^2 - 1)^p(a_0b_0^2x_0^4 - 2b_0^2x_0^2 + 1)^p f(x_0^2)^p\right) + \tilde{y}_2(b_0x_0)
\end{aligned}$$

where we have implicitly used the fact $\varphi(b_0^2 x_0^2) = b_0^{p-5} f(x_0^2)$. Thus we have

$$\begin{aligned}\tilde{y}_2(b_0 x_0) &= b_0^{p^2}\left(x_2 - x_0^p(b_0^2 x_0^2 - 1)^{\frac{p^2+p}{2}}(a_0 x_0^2 - 1)^p(a_0 b_0^2 x_0^4 - 2b_0^2 x_0^2 + 1)^p f(x_0^2)^p\right) \\ &= b_0^{p^2}\tilde{x}_2.\end{aligned}$$

Thus

$$\mathbf{y} \circ \nu\left(\frac{y_0}{b_0}, b_0 x_0\right) = \mathbf{b} \cdot (x_0, x_1, \tilde{x}_2).$$

To see

$$\mathbf{x} \circ \nu\left(\frac{y_0}{b_0}, b_0 x_0\right) = \frac{(y_0, y_1, \tilde{y}_2)}{\mathbf{b}}$$

we observe that, by the equation of the curve,

$$\mathbf{x} \circ \nu\left(\frac{y_0}{b_0}, b_0 x_0\right) = \pm\frac{(y_0, y_1, \tilde{y}_2)}{\mathbf{b}}$$

but since the reduction modulo p is equal to $\frac{y_0}{b_0}$ (as our result holds modulo p^2, thus holds modulo p), it must be equal to exactly

$$\frac{(y_0, y_1, \tilde{y}_2)}{\mathbf{b}}.$$

Thus all conditions are met.

Bibliography

[1] Christophe Arene, Tanja Lange, Michael Naehrig, and Christophe Ritzenthaler, *Faster computation of the Tate pairing*, May 2010, arXiv:0904.0854 [math]. 8

[2] Daniel J. Bernstein and Tanja Lange, *Faster addition and doubling on elliptic curves*. 4, 7

[3] ———, *A complete set of addition laws for incomplete Edwards curves*, Journal of Number Theory **131** (2011), no. 5, 858–872 (en). 8

[4] Craig Costello and Benjamin Smith, *Montgomery curves and their arithmetic: The case of large characteristic fields*, Journal of Cryptographic Engineering **8** (2018), no. 3, 227–240 (en). 9, 10

[5] M. Deuring, *Die typen der multiplikatorenringe elliptischer funktionenköper*, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272. 26

[6] Harold Edwards, *A normal form for elliptic curves*, Bull. Amer. Math. Soc. **44** (2007), no. 3, 393–422 (en). 4

[7] L. R. A. Finotti, *Minimal degree liftings in characteristic 2*, J. Pure Appl. Algebra **207** (2006), no. 3, 631–673. MR MR2265544 25

[8] Luís R. A. Finotti, *Degrees of the Elliptic Teichmüller Lift*, Journal of Number Theory **95** (2002), no. 2, 123–141 (en). 31, 38, 54

[9] ———, *Minimal Degree Liftings of Hyperelliptic Curves*, (2004), 37 (en). 3, 31, 54, 55

[10] ———, *Weierstrass coefficients of the canonical lifting*, Int. J. Number Theory **16** (2020), no. 02, 397–422 (en). 36, 44, 46

[11] J. Lubin, J.-P. Serre, and J. Tate., *Elliptic curves and formal groups.* 26

[12] B. Mazur, *Frobenius and the Hodge Filtration (estimates)*, Annals of Mathematics **98** (1973), no. 1, 58–95, Publisher: Annals of Mathematics. 33

[13] Joseph Rabinoff, *The Theory of Witt Vectors*, arXiv:1409.7445 [math] (2014), arXiv: 1409.7445. 23

[14] Jean-Pierre Serre, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer New York, New York, NY, 1979 (en). 23

[15] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer New York, New York, NY, 2009. 1, 25, 77, 87

[16] José Voloch and Judy Walker, *Euclidean weights of codes from elliptic curves over rings*, Trans. Amer. Math. Soc. **352** (2000), no. 11, 5063–5076 (en). 36, 41

Appendix

Appendix A

A.1 Projective Closure

We consider the closure of the image of $E_{a,b}$ under the map

$$(x, y) \mapsto (1 : x : y : xy),$$

which will be a curve given by the common zeros of the homogeneous equations

$$F : b^2X^2 + Y^2 = T^2 + aZ^2, \qquad G : TZ = XY.$$

We first consider the dehomogenization with respect to T which yields two quadratic equations

$$f_1 : b^2x^2 + y^2 - 1 - az^2 = 0 \qquad f_2 : xy - z = 0$$

where our initial affine curve is their common roots. Call this curve C_0. A point $p = (\alpha, \beta, \gamma) \in C_0(\bar{k})$ is non-singular is singular if and only if $rank(M(p)) = 2$, where

$$M(p) = \begin{bmatrix} \frac{\partial f_1}{\partial x}(p) & \frac{\partial f_1}{\partial y}(p) & \frac{\partial f_1}{\partial z}(p) \\ \\ \frac{\partial f_2}{\partial x}(p) & \frac{\partial f_2}{\partial y}(p) & \frac{\partial f_2}{\partial z}(p) \end{bmatrix} = \begin{bmatrix} 2b^2\alpha & 2\beta & -2a\gamma \\ \beta & \alpha & -1 \end{bmatrix}$$

[15]. To show no singular point exists, we break into 2 cases, the first of which is $\gamma = 0$. Since $\gamma = 0$, it follows α or $\beta = 0$. When $\alpha = 0$, we see $\beta = \pm 1$, and when $\beta = 0$ we see $\alpha = \pm b^{-1}$. Then we check the possible matrices

$$\begin{bmatrix} 0 & \pm 1 & 0 \\ \pm 2 & 0 & -1 \end{bmatrix} \qquad \begin{bmatrix} \pm 2b & 0 & 0 \\ 0 & \pm b^{-1} & -1 \end{bmatrix}$$

and see they all have rank 2. Next, we check $\gamma \neq 0$, in which case $\alpha, \beta \neq 0$. Then $M(p)$ has rank 1 if and only if there is some $\lambda \neq 0$ such that

$$2b^2\alpha = \lambda\beta \qquad 2\beta = \lambda\alpha \qquad -2a\gamma = -\lambda.$$

One checks this implies $\lambda = \pm 2b$. If $\lambda = 2b$, we get $\beta = b\alpha$ and $a\gamma = b$. But since $\gamma = \alpha\beta = b\alpha^2$, we see this means

$$\begin{aligned} 2b^2\alpha^2 = b^2\alpha^2 + \beta^2 = 1 + a\gamma^2 = 1 + b\gamma = 1 + b^2\alpha^2 &\implies b^2\alpha^2 = 1 \\ &\implies \alpha^2 = 1/b^2 \\ &\implies \gamma = 1/b \\ &\implies a = b^2 \end{aligned}$$

which yields a contradiction. Likewise if $\lambda = -2b$, we have $\beta = -b\alpha$ and $a\gamma = -b$. But since $\gamma = \alpha\beta = -b\alpha^2$, we see

$$\begin{aligned} 2b^2\alpha^2 = b^2\alpha^2 + \beta^2 = 1 + a\gamma^2 = 1 - b\gamma = 1 + b^2\alpha^2 &\implies b^2\alpha^2 = 1 \\ &\implies \alpha^2 = 1/b^2 \\ &\implies \gamma = -1/b \\ &\implies a = b^2 \end{aligned}$$

again a contradiction. Thus singular points can only occur on the line at infinity, where $T = 0$. Immediately, we see that exactly one of $X, Y = 0$ as it cannot be the case that both are equal to 0, else we have

$$0 = aZ^2,$$

which only has solution $Z = 0$, resulting in the point $(0 : 0 : 0 : 0)$. As such, it follows that $T = 0 \implies Z \neq 0$ and so we may dehomogenize with respect to Z. Letting $t = X/Z$, $u = Y/Z$ and $v = T/Z$, we get the quadratics

$$g_1 : b^2t^2 + u^2 - v^2 - a = 0 \qquad g_2 : tu - v = 0.$$

Call this curve C_1. As before, a point $q = (\rho, \sigma, \tau) \in C_1(\bar{k})$ will be singular if and only if $rank(M'(q)) = 2$ where

$$M'(q) = \begin{bmatrix} \frac{\partial g_1}{\partial t}(q) & \frac{\partial g_1}{\partial u}(q) & \frac{\partial g_1}{\partial v}(q) \\ \\ \frac{\partial g_2}{\partial t}(q) & \frac{\partial g_2}{\partial u}(q) & \frac{\partial g_2}{\partial v}(q) \end{bmatrix} = \begin{bmatrix} 2b^2\rho & 2\sigma & -2\tau \\ \sigma & \rho & -1 \end{bmatrix}.$$

Since we are only concerned about the line at infinity, we need only consider the case when $\tau = 0$. Then we have exactly one of ρ, σ equal to 0. Checking the possible

matrices

$$\begin{bmatrix} 0 & \pm 2\sqrt{a} & 0 \\ \pm\sqrt{a} & 0 & -1 \end{bmatrix} \qquad \begin{bmatrix} \pm 2b\sqrt{a} & 0 & 0 \\ 0 & \pm\frac{\sqrt{a}}{b} & -1 \end{bmatrix}$$

and see they all have rank 2. Thus no such singular points can exist. Since any point on $E_{a,b}$ is on either C_0 or C_1, we see $E_{a,b}$ is a smooth curve as it has no non-singular points. Additionally, note we may view $E_{a,b}$ as C_0 and C_1 glued together on appropriate subsets via the maps

$$(x, y) \mapsto (1/y, 1/x) \qquad (t, u) = (1/u, 1/t).$$

A.2 Uniformizers at Affine Points

We begin at the point $(0, 1)$, we have the kernel of the evaluation map (which is known to be a maximal ideal) given by

$$M_{(0,1)} = \langle x, y - 1 \rangle$$

Note we can write

$$y - 1 = \frac{x^2(ay^2 - b^2)}{y + 1} \implies ord_{(0,1)}(y - 1) = 2ord_{(0,1)}(x).$$

Thus $ord_{(0,1)}(x) = 1, ord_{(0,1)}(y - 1) = 2$. Similarly at $(0, -1)$ we have $ord_{(0,-1)}(x) = 1$ and $ord_{(0,-1)}(y + 1) = 2$.

At $\left(\frac{1}{b}, 0\right)$ we have

$$M_{\left(\frac{1}{b},0\right)} = \langle bx - 1, y \rangle .$$

By similar methods we write

$$\begin{aligned} bx-1 &= \frac{y^2(ax^2-1)}{bx+1} \implies \\ ord_{\left(\frac{1}{b},0\right)}(bx-1) &= 2ord_{\left(\frac{1}{b},0\right)}(y) \implies \\ ord_{\left(\frac{1}{b},0\right)}(y) &= 1, ord_{\left(\frac{1}{b},0\right)}(bx-1) = 2. \end{aligned}$$

Similarly at $\left(-\frac{1}{b},0\right)$ we have $ord_{\left(-\frac{1}{b},0\right)}(y) = 1$ and $ord_{\left(-\frac{1}{b},0\right)}(bx+1) = 2$.

Let $P = (z,w)$ be an affine point such that $zw \neq 0$. Then

$$M_P = \langle x-z, y-w \rangle .$$

Since P is a point on $E_{a,b}$, we find the following equality

$$b^2z^2 + w^2 = 1 + az^2w^2.$$

Thus

$$\begin{aligned} b^2(x^2-z^2) + (y^2-w^2) = a(x^2y^2 - z^2w^2) &= a(x^2y^2 - x^2w^2 + x^2w^2 - z^2w^2) \\ &= ax^2(y^2-w^2) + aw^2(x^2-z^2) \end{aligned}$$

Rearranging terms, we have

$$y^2 - w^2 = \frac{(b^2-aw^2)(x^2-z^2)}{ax^2-1}.$$

This gives us

$$y-w = \frac{(b^2-aw^2)(x+z)}{(ax^2-1)(y+w)}(x-z) \implies ord_P(y-w) = ord_P(x-z) = 1.$$

as no affine point has $x-$coordinate $a^{-1/2}$.

A.3 Birational Equivalence to Montgomery Curves

Proposition A.1. *Let a, b^2 be distinct elements of $\Bbbk^\times$. Let $A = 2\frac{b^2+a}{b^2-a}$ and $B = \frac{4}{b^2-a}$. Then*

$$E_{a,b}/k: \qquad b^2x^2 + y^2 = 1 + ax^2y^2$$

and

$$M_{A,B}/k: \qquad Bu^2 = t^3 + At^2 + t$$

are birationally equivalent via the map

$$(x, y) \mapsto \left(\frac{1+y}{1-y}, \frac{1+y}{x(1-y)}\right)$$

with inverse

$$(t, u) \mapsto \left(\frac{t}{u}, \frac{t-1}{t+1}\right)$$

Proof. To begin, observe that $A^2 = 4$ if and only if

$$b^2 + a = \pm(b^2 - a).$$

This would require either a or $b^2 = 0$, which is never the case. To ensure all points are being considered appropriately, we find a projective model for $M_{A,B}$ given by the usual embedding

$$(t, u) \mapsto (t, u, 1)$$

which yields

$$BU^2V = T^3 + AT^2V + TV^2$$

as our projective model. The smoothness of this model follows from the usual verification of the smoothness of a Weierstrass curve.

Next, observe we can view our forward map as

$$(W : X : Y : Z) \mapsto (X(W+Y) : W(W+Y) : X(W-Y))$$

by replacing $x = X/W$ and $y = Y/W$. For all points not $(1 : 0 : -1 : 0)$ we may simplify this to

$$\begin{aligned}(WX + XY : W(W+Y) : WX - XY) &= (W(X+Z) : W(W+Y) : W(X-Z)) \\ &= (X+Z : W+Y : X-Z)\end{aligned}$$

and see this map is regular at those points not $(1 : 0 : -1 : 0)$. To reconcile this point, we perform the following operations

$$\begin{aligned}&(X(W+Y) : W(W+Y) : X(W-Y)) \\ =&(X(W^2-Y^2) : W(W^2-Y^2) : X(W-Y)^2) \\ =&(X(W^2-Y^2) : W(X^2-aZ^2) : X(W-Y)^2) \\ =&(X(W^2-Y^2) : WX^2-aXYZ : X(W-Y)^2) \\ =&(W^2-Y^2 : WX-aYZ : (W-Y)^2)\end{aligned}$$

which we see is regular at $(1 : 0 : -1 : 0)$.

Next, we go about checking that the image of our map is in fact $M_{A,B}$. Observe

$$\begin{aligned}&(X+Z)^3 + A(X+Z)^2(X-Z) + (X+Z)(X-Z)^2 - B(W+Y)^2(X-Z) \\ =&AX^3 + AZX^2 - AZ^2X - AZ^3 - BW^2X - BY^2X - 2BWYX + BW^2Z \\ &+BY^2Z + 2BWYZ + 2X^3 + 2ZX^2 + 2Z^2X + 2Z^3 \\ =&\frac{4}{b^2-a}\left(b^2X^3 + b^2X^2Z - aXZ^2 - aZ^3 - W^2X - WXY + Y^2Z + WYZ\right)\end{aligned}$$

where we have used the facts

$$A+2=\frac{4b^2}{b^2-a} \qquad 2-A=\frac{-4a}{b^2-a} \qquad B=\frac{4}{b^2-a}$$

Since a, b^2 are distinct elements of $k^\times$, and we seek to show this expression is 0, we now drop the scalar $4/(b^2-a)$ from our computations. Continuing, we get

$$\begin{aligned}
&b^2X^3+b^2X^2Z-aXZ^2-aZ^3-W^2X-WXY+Y^2Z+WYZ\\
=&X(b^2X^2-aZ)^2+Z(b^2X^2-aZ^2)-W^2X-WXY+Y^2Z+WYZ\\
=&X(W^2-Y^2)+Z(W^2-Y^2)-W^2X-W^2Z+Y^2Z+XY^2\\
=&0.
\end{aligned}$$

Thus we have

$$\begin{aligned}
0&=(X+Z)^3+A(X+Z)^2(X-Z)-(X+Z)(X-Z)^2-B(W+Y)^2(X-Z)\\
&=T^3-AT^2V+TV^2-BU^2V
\end{aligned}$$

so our map satisfies the projective equation of the Montgomery Curve.

Now we show the proposed inverse map is both well-defined and an inverse map. To check the well-definedness, we observe we may see the backward map as

$$(T:U:V)\mapsto(U(T+V):T(T+V):U(T-V):T(T-V))$$

as this is the extension of

$$(t,u)\mapsto\left(1:\frac{t}{u}:\frac{t-1}{t+1}:\frac{t(t-1)}{u(t+1)}\right)$$

with the substitutions $t = T/V$, $U/U/V$. Clearly, this maps $M_{A,B}$ to a subset of the zeros of $WZ = XY$. We show it also maps to a subset of

$$b^2X^2 + Y^2 = W^2 + aZ^2$$

thus is our inverse map (quick inspection shows compositions of the forwards and backward maps give the necessary identities).

We next observe

$$\begin{aligned}
&b^2T^2(T+V)^2 + U^2(T-V)^2 - U^2(T+V)^2 - aT^2(T-V)^2 \\
=&T^2\left(b^2T^2 + 2b^2TV + b^2V^2 - aT^2 + 2aTV - aV^2\right) - 4TU^2V \\
=&T\left(b^2T^3 + 2b^2T^2V + b^2V^2T - aT^3 + 2aT^2V - aV^2T\right) \\
&-T(b^2-a)\left(T^3 + 2\frac{b^2+a}{b^2-a}T^2V + TV^2\right) \\
=&T\left(b^2T^3 + 2b^2T^2V + b^2V^2T - aT^3 + 2aT^2V - aV^2T\right) \\
&-T\left(b^2T^3 + 2b^2T^2V + b^2V^2T - aT^3 + 2aT^2V - aV^2T\right) \\
=&0
\end{aligned}$$

thus showing our map sends $M_{A,B}$ to $E_{a,b}$.

To see this map is regular everywhere except $(0:0:1)$ and $(0:1:0)$, as if $T = 1$, then $T - V$ and $T + V$ cannot both be 0 as we are not in characteristic 2. Thus the only points where we fail to have regularity are those points such that $T = 0$ and $UV = 0$.

At the point $(0:1:0)$, we observe our map can also be seen as

$$\begin{aligned}
&(U(T+V):T(T+V):U(T-V):T(T-V)) \\
&= \big(BTU^2 + BU^2V : BUT(T+V) : BU^2T - BU^2V : BUT(T-V)\big) \\
&= \big(BU^2 + (T^2+ATV+V^2) : BU(T+V) : BU^2 - (T^2+ATV+V^2) : BU(T-V)\big)
\end{aligned}$$

which maps the point $(0:1:0)$ to $(B:0:B:0) = (1:0:1:0)$. Similarly, at the point $(0:0:1)$ this maps evaluates to $(1:0:-1:0)$. Thus our maps are regular everywhere and we have established the birational equivalence of our curves. □

Note that if we give $M_{A,B}$ the usual group structure on an elliptic curve defined by $y^2 = f(x)$, for some non-singular cubic equation $f(x)$, then our birational equivalence maps the identity of $E_{a,b}$ to the identity of $M_{A,b}$, thus is an isogeny between our curves. Thus our map is a group homomorphism between $E_{a,b}(\bar{k})$ and $M_{A,B}(\bar{k})$. Further, the existence of an inverse shows it is in fact an isomorphism.

A.4 Unused Misc Result: The Derivatives $\frac{d}{dx}y^2$ and $\frac{d}{dx}xy^2$

The following contains a result that was once thought to potentially be important to the development of the algorithm, but more efficient and intelligible methods were later discovered. However, due to the counter-intuitive nature of the resulting derivative, we have elected to include the following in hope that readers will find these derivatives as interesting as we do.

By the equation of our curve, we have

$$y^2 - a_0x^2y^2 = 1 - b_0^2x^2.$$

Taking derivatives, we get

$$2y \cdot \frac{dy}{dx} - a_0(2x^2 \cdot y \cdot \frac{dy}{dx} + 2xy^2) = -2b_0^2 x.$$

Thus

$$y\left(1 - ax^2\right)\frac{dy}{dx} = x\left(a_0 y^2 - b_0^2\right).$$

Using the fact that $(a_0x^2 - 1)(a_0y^2 - b_0^2) = b_0^2 - a_0$ we get

$$y\frac{dy}{dx} = \frac{x(a_0y^2 - b_0^2)^2}{a_0 - b_0^2}.$$

Thus

$$\frac{d}{dx}\left(y^2\right) = 2y\frac{dy}{dx} = \frac{2x(a_0y^2 - b_0^2)^2}{a_0 - b_0^2} \in k[x,y]/(b_0^2x^2 + y^2 - 1 - a_0x^2y^2).$$

Therefore, for any polynomial $G(y^2)$ we have

$$\frac{d}{dx}G(y^2) = G'(y^2) \cdot \frac{d}{dx}\left(y^2\right) = G'(y^2) \cdot \frac{2x(a_0y^2 - b_0^2)^2}{a_0 - b_0^2}.$$

We now expand

$$(a_0y^2 - b_0^2)^2 = a_0^2y^4 - 2a_0b_0^2y^2 + b_0^4.$$

Thus we will have

$$\begin{aligned} x^2(a_0y^2 - b_0^2)^2 &= (a_0x^2y^2 - b_0^2x^2)(a_0y^2 - b_0^2) \\ &= (y^2 - 1)(a_0y^2 - b_0^2) \\ &= a_0y^4 - (b_0^2 + a_0)y^2 + b_0^2. \end{aligned}$$

Therefore, we have

$$\begin{aligned}\frac{d}{dx}\left(xG(y^2)\right) &= G(y^2) + x\frac{d}{dx}\left(G(y^2)\right) \\ &= G(y^2) + G'(y^2)\cdot\frac{2x^2(a_0y^2-b_0^2)^2}{a_0-b_0^2} \\ &= G(y^2) + \frac{2}{a_0-b_0^2}\cdot G'(y^2)\cdot\left(a_0y^4-(b_0^2+a_0)y^2+b_0^2\right).\end{aligned}$$

In particular, for y^{2n}, we have $G(t)=t^n$ and thus

$$\begin{aligned}\frac{d}{dx}\left(xy^{2n}\right) &= y^{2n} + \frac{2n}{a_0-b_0^2}(y^{2n-2})\cdot\left(a_0y^4-(b_0^2+a_0)y^2+b_0^2\right) \\ &= y^{2n} + \frac{2n}{a_0-b_0^2}\left(a_0y^{2n+2}-(b_0^2+a_0)y^{2n}+b_0^2y^{2n-2}\right)\end{aligned}$$

A.5 Formal Group Law

Throughout this section, we assume $E_{a,b}$ is defined over a local field K of characteristic 0 complete with respect to the $p-$adic metric for some fixed $p>3$. We assume R is the integer ring of K and pR is the unique maximal ideal of R. Furthermore, $E_{a,b}$ is assumed to have good reduction modulo p.

To achieve our formal group on $E_{a,b}$ we rewrite the equation of $E_{a,b}$ as

$$y^2(1-ax^2)=1-b^2x^2 \implies y^2=\frac{1-b^2x^2}{1-ax^2}=(1-b^2x^2)\sum_{i=0}^{\infty}a^ix^{2i}$$

and consider a solution to this around the point $(0,1)$, found by taking the solution from Hensel's Lemma (or the analog of it given by IV.1.1.2 of [15]).

We produce a formal group law by appealing to the group law inherent to Twisted Edwards Form, letting x_1, x_2 be independent indeterminants. Then $(x_1, y(x_1))$ and $(x_2, y(x_2))$ are two points on $E(K[[x_1,x_2]])$. As such, we may add the

points via the usual group law as $(x_1, y(x_1)) + (x_2, y(x_2)) = (x_3, y_3)$ with

$$x_3(x_1, x_2) = \frac{x_1 y(x_2) + x_2 y(x_1)}{1 + a x_1 x_2 y(x_1) y(x_2)} \qquad y_3(x_1, x_2) = \frac{y(x_1) y(x_2) - b^2 x_1 x_2}{1 - a x_1 x_2 y(x_1) y(x_2)}.$$

We observe both of our denominators are units in $K[[x_1, x_2]]$, having inverse given by the usual geometric series. Thus we get

$$x_3(x_1, x_2) = (x_1 y(x_2) + x_2 y(x_1)) \sum_{i=0}^{\infty} (-1)^i \left(a x_1 x_2 y(x_1) y(x_2)\right)^i \tag{A.1.1}$$

$$y_3(x_1, x_2) = \left(y(x_1) y(x_2) - b^2 x_1 x_2\right) \sum_{i=0}^{\infty} \left(a x_1 x_2 y(x_1) y(x_2)\right)^i. \tag{A.1.2}$$

Since $y(x) \equiv 1 \mod x$

$$x_3 = x_1 + x_2 + ... \qquad y_3(x_1, x_2) = 1 + \text{terms in } x_1, x_2.$$

Further, when $x_1, x_2 \in pR$, the power series $y(x_1), y(x_2)$ converge in the $p-$adic metric to well-defined values $y_1, y_2 \in 1 + pR$. Similarly, $x_3(x_1, x_2)$ converges to a well defined value $x_3 \in pR$, namely

$$\frac{x_1 y_2 + x_2 y_1}{1 + a x_1 x_2 y_1 y_2}$$

while $y_3(x_1, x_2)$ a well defined value in $1 + pR$, namely

$$\frac{y_1 y_2 - b^2 x_1 x_2}{1 - a x_1 x_2 y_1 y_2}.$$

We claim $y_3(x_1, x_2) = y(x_3)$. This can be seen as both $(x_3, y_3(x_1, x_2)), (x_3, y(x_3))$ are affine points of $E(R)$ lying on the line $x = x_3$. Since this line only intersects two affine points, namely

$$(x_3, y(x_3)) \qquad (x_3, -y(x_3))$$

it follows $(x_3, y_3(x_1, x_2))$ must be one of them. But $(x_3, -y(x_3))$ reduces to the point $(0, -1)$ modulo p and $(x_3, y_3(x_1, x_2))$ reduces to $(0, 1)$, it must be the case

$$(x_3, y_3(x_1, x_2)) = (x_3, y(x_3))$$

Thus we see we have an injection from the formal group of $E_{a,b}$ on pR (henceforth called $\hat{E}_{a,b}$) into the kernel of the reduction modulo p map (henceforth denoted $\ker(\pi)$) given by

$$t \mapsto (t, y(t)),$$

as only $t = 0$ maps to the identity. Note the image of $\hat{E}_{a,b}$ is a subset $E(pR) \cap \ker(\pi)$, as all x coordinates are $0 \mod p$ and all the y coordinates are $1 \mod p$. We claim this map is in fact an isomorphism.

To this end, we show our map has inverse $P \mapsto x(P)$. Clearly, this is a set-theoretic inverse mapping, but since the group law on $\hat{E}_{a,b}$ is defined using the group law on $E_{a,b}$, this also constitutes a homomorphism. Thus $x(P)$ is an inverse to our given map, so we have an isomorphism of groups $\hat{E}_{a,b}$ and $E(R) \cap \ker \pi$.

A.6 Absolute Minimal Degree Lifting for $p = 3$

Consider an ordinary Edwards Curve

$$E_{a_0,b_0}/k : \qquad b_0^2 x_0^2 + y_0^2 = 1 + a_0 x_0^2 y_0^2.$$

We find a curve over $\mathbf{W}_3(k)$ given by

$$\mathbf{E_{a,b}}/\mathbf{W}_3(k) : \qquad \mathbf{b}^2\mathbf{x}^2 + \mathbf{y}^2 = (1, 0, 0) + \mathbf{a}\mathbf{x}^2\mathbf{y}^2$$

$$\mathbf{a} = \left(a_0, \frac{2a_0^4 + a_0^3b_0^2}{a_0 + b_0^2}, \frac{a_0^{16}b_0^4 + a_0^{15}b_0^6 + 2a_0^{12}b_0^{12} + 2a_0^{11}b_0^{14} + 2a_0^9b_0^{18}}{a_0^9 + b_0^{18}}\right)$$
$$\mathbf{b} = \left(b_0, \frac{2a_0b_0^3 + b_0^5}{a_0 + b_0^2}, \frac{2a_0^9b_0^9 + a_0^7b_0^{13} + a_0^3b_0^{21} + 2a_0^2b_0^{23} + b_0^{27}}{a_0^9 + b_0^{18}}\right)$$

and a lifting of points $((x_0, y_0)) \mapsto ((x_0, x_1, \tilde{x}_2), (y_0, y_1, \tilde{y}_2))$ that constitutes and absolute minimal degree lifting of points given by

$$x_1 = \frac{a_0b_0^2}{a_0 + b_0^2}x_0^5 + \frac{2}{a_0 + b_0^2}x_0$$

$$\begin{aligned}\tilde{x}_2 = {} & \frac{2a_0^4b_0^8}{a_0^4 + a_0^3b_0^2 + a_0b_0^6 + b_0^8}x_0^{17} + \frac{2a_0^9b_0^6 + 2a_0^8b_0^8 + 2a_0^4b_0^{16}}{a_0^9 + b_0^{18}}x_0^{15} \\ & + \frac{a_0^3b_0^6}{a_0^4 + a_0^3b_0^2 + a_0b_0^6 + b_0^8}x_0^{13} + \frac{a_0^3b_0^2 + a_0b_0^6}{a_0^3 + b_0^6}x_0^{11} \\ & + \frac{2a_0^2 + 2b_0^4}{a_0^3 + b_0^6}x_0^7 + \frac{2a_0b_0^2}{a_0^4 + a_0^3b_0^2 + a_0b_0^6 + b_0^8}x_0^5 + \frac{2a_0^6 + a_0^5b_0^2 + a_0^3b_0^6 + a_0b_0^{10}}{a_0^9 + b_0^{18}}x_0^3 \\ & + \frac{1}{a_0^4 + a_0^3b_0^2 + a_0b_0^6 + b_0^8}x_0\end{aligned}$$

$$y_1 = \frac{a_0}{a_0 + b_0^2}y_0^5 + \frac{2a_0 + b_0^2}{a_0 + b_0^2}y_0^3 + \frac{2b_0^2}{a_0 + b_0^2}y_0$$

$$\begin{aligned}\tilde{y}_2 = {} & \frac{2a_0^4}{a_0^4 + a_0^3b_0^2 + a_0b_0^6 + b_0^8}y_0^{17} + \frac{a_0^9 + 2a_0^8b_0^2 + 2a_0^4b_0^{10} + a_0^3b_0^{12}}{a_0^9 + b_0^{18}}y_0^{15} \\ & + \frac{a_0^4 + a_0^3b_0^2 + 2a_0^2b_0^4}{a_0^4 + a_0^3b_0^2 + a_0b_0^6 + b_0^8}y_0^{13} + \frac{2a_0^2b_0^2}{a_0^3 + b_0^6}y_0^{11} \\ & + \frac{2a_0^9 + a_0^8b_0^2 + 2a_0^5b_0^8 + a_0^4b_0^{10} + a_0^3b_0^{12} + 2a_0b_0^{16} + b_0^{18}}{a_0^9 + b_0^{18}}y_0^9 + \frac{a_0b_0^4}{a_0^3 + b_0^6}y_0^7 \\ & + \frac{a_0^2b_0^4 + 2a_0b_0^6 + 2b_0^8}{a_0^4 + a_0^3b_0^2 + a_0b_0^6 + b_0^8}y_0^5 + \frac{a_0^5b_0^8 + a_0^3b_0^{12} + a_0b_0^{16} + 2b_0^{18}}{a_0^9 + b_0^{18}}y_0^3 \\ & + \frac{b_0^8}{a_0^4 + a_0^3b_0^2 + a_0b_0^6 + b_0^8}y_0\end{aligned}$$

Vita

William (Liam) Bitting was born in Saint Louis, MO, graduating from Clayton Highschool before attending Rhodes College where he earned a Bachelor's in Mathematics.