CANONICAL LIFTINGS OF EDWARDS CURVES

LIAM BITTING AND LUÍS R. A. FINOTTI

Abstract. Twisted Edwards curves are genus 1 curves given by equations of the form $bx^2 + y^2 = 1 + ax^2y^2$. Due to their simplified formulas for point arithmetic, they most often offer better performance in concrete applications, such as cryptography. Here we study the canonical liftings of such curves and their associated elliptic Teichmüller lift. The coordinate functions of the latter are proved to be polynomials, and their degrees and derivatives are given. Moreover, an algorithm is described for explicit computations, and some properties of the general formulas for are given.

1. Introduction

In [5], 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 yield better results than the more usual Weierstrass equation.

Although over an algebraically closed field every elliptic curve can be expressed an Edwards curve, this often not the case over finite fields. Therefore, [2] and [1] introduce generalizations which can represent a larger number of elliptic curves over finite fields. Here we will focus on the case of *twisted Edwards curves*, introduced in the latter reference.

Our interest here is to study canonical liftings of Edwards curves, with particular interest in computational aspects, similar to what was done for the Weierstrass equation in [6], [7],

2010 *Mathematics Subject Classification.* Primary 11G07; Secondary 11F03.

Key words and phrases. Edwards curves, canonical lifting, elliptic Teichmüller lift, modular functions.

and [10]. We study the coordinate functions of the associated *elliptic Teichmüller* lift (of points), showing that these are given by odd polynomials in one variable in Section 4. We then obtain the exact degrees and formulas for the derivatives of these polynomials in Section 5. This allow us to give an algorithm for computing these canonical liftings and their elliptic Teichmüller lift in Section 8.

We then study formulas for the canonical lifting and elliptic Teichmüller lift, starting in Section 10, showing that there are formulas that work in every possible case in Section 11, and finally that these can be chosen to be modular functions in Section 12.

2. Canonical Liftings

Let $\Bbbk$ be a perfect field of characteristic $p > 0$. Associated to an *ordinary* elliptic curve E over $\Bbbk$, there exists a unique (up to isomorphisms) elliptic curve $\boldsymbol{E}$ over $\boldsymbol{W}(\Bbbk)$, the ring of Witt vectors over $\Bbbk$, called the *canonical lifting* of E, and a map $\tau : E(\bar{\Bbbk}) \to \boldsymbol{E}(\boldsymbol{W}(\bar{\Bbbk}))$, i.e., a *lift of points*, called the *elliptic Teichmüller lift*, characterized by the following properties:

(1) the reduction modulo p of $\boldsymbol{E}$ is E;
(2) τ is an injective group homomorphism and a section of the reduction modulo p, which we denote by π;
(3) if σ denote the Frobenius of both $\Bbbk$ and $\boldsymbol{W}(\Bbbk)$ and if $\phi : E \to E^{\sigma}$ denotes the p-th power Frobenius, then there exists a map $\boldsymbol{\phi} : \boldsymbol{E} \to \boldsymbol{E}^{\sigma}$, such that the diagram

$$\begin{tikzcd}
\boldsymbol{E}(\boldsymbol{W}(\Bbbk)) \arrow[r, dashed, "\boldsymbol{\phi}"] \arrow[d, bend right, "\pi"'] & \boldsymbol{E}^{\sigma}(\boldsymbol{W}(\Bbbk)) \arrow[d, bend right, "\pi"'] \\
E(\Bbbk) \arrow[r, "\phi"] \arrow[u, bend right, "\tau"'] & E^{\sigma}(\Bbbk) \arrow[u, bend right, "\tau^{\sigma}"']
\end{tikzcd}$$

commutes. (In other words, there exists a *lifting of the Frobenius.*)

This concept of canonical lifting of elliptic curves was first introduced by Deuring in [4] and then generalized to Abelian varieties by Serre and Tate in [14]. Apart from being of independent interest, this theory has been used in many interesting applications, such as counting rational points in ordinary elliptic curves, as in Satoh's [16], coding theory, as in Voloch and Walker's [18], and counting torsion points of curves of genus $g \geq 2$, as in Poonen's [15] or Voloch's [17].

One can compute canonical liftings of elliptic curves using the modular polynomial, as shown in [14]. On the other hand, Voloch and Walker in [18] developed an algorithm to compute the second coordinate of the Weierstrass coefficients of the canonical lifting, together with the second coordinate of the elliptic Teichmüller lift, which can be used to obtain the lifting of the Frobenius. The second author, in [10] (or previously, although less explicitly, in [8]) extended this algorithm to arbitrary length.

Here we take a similar approach to compute the canonical lifting using the Edwards curve form. Before doing so, some properties about the canonical lifting and its associated elliptic Teichmüller lift need to be deduced.

3. Twisted Edwards Curves

In this section we review *twisted Edwards curves*. The main reference here is [1].

Let $\Bbbk$ be a perfect field of characteristic $p > 2$. Edwards, in [5], originally used equations of the form

$$x^2 + y^2 = c^2(1 + x^2y^2).$$

In [2], Bernstein and Lange generalized these to curves of form

$$x^2 + y^2 = 1 + ax^2y^2, \tag{3.1}$$

while [1] further generalized them to

$$bx^2 + y^2 = 1 + ax^2y^2.$$

This increases the number of possible curves over finite fields. On the other hand, we will often need the square root of this coefficient b, and hence instead of introducing a new symbol for this square root, we will simply replace b by b^2 in the above equation, while keeping in mind that b itself might be in an extension of the base field. Thus, our twisted Edward curve equation will be given by

$$E_{a,b}/\Bbbk : \ b^2x^2 + y^2 = 1 + ax^2y^2, \qquad \text{with } \Delta \overset{\text{def}}{=} ab^2(a-b^2) \neq 0. \tag{3.2}$$

(Clearly, a change of variables $x' \mapsto x/b$ would yield an equation of the form of Eq. (3.1).) Note then that Edward curves have at least two rational affine points: $(0, \pm 1)$.

The corresponding *j-invariant* is given by

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

The projective model of $E_{a,b}$ above is given by

$$\begin{aligned} b^2X_1^2 + X_2^2 &= X_0^2 + aX_3^2, \\ X_0X_3 &= X_1X_2, \end{aligned}$$

where $(x,y) \mapsto [1, x, y, xy]$. This yields two points at infinity over a field where a has a square root $a^{1/2}$, and another two if b itself is in the base field (instead of simply b^2):

$$\mathcal{O}^{\pm} \overset{\text{def}}{=} [0, 0, \pm a^{1/2}, 1], \quad \mathcal{Q}^{\pm} \overset{\text{def}}{=} [0, \pm \frac{a^{1/2}}{b}, 0, 1].$$

If neither a nor b^2 have square roots in the base field, then $\mathcal{Q}^{\pm}$ are rational.

The group law in the projective model is given by $[T_1, X_1, Y_1, Z_1] + [T_2, X_2, Y_2, Z_2] = [T_3, X_3, Y_3, Z_3]$, where

$$\begin{aligned} T_3 &= (T_1T_2 + aZ_1Z_2)(T_1T_2 - aZ_1Z_2), & X_3 &= (X_1Y_2 + X_2Y_1)(T_1T_2 - aZ_1Z_2), \\ Y_3 &= (T_1T_2 + aZ_1Z_2)(Y_1Y_2 - b^2X_1X_2), & Z_3 &= (X_1Y_2 + X_2Y_1)(Y_1Y_2 - b^2X_1X_2), \end{aligned}$$

with identity $[1, 0, 1, 0]$ and $-[T_0, X_0, Y_0, Z_0] = [T_0, -X_0, Y_0, -Z_0]$. Thus, one can check that $|\mathcal{O}^{\pm}| = 4$, and $|\mathcal{Q}^{\pm}| = 2$.

Also, for affine points we get

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + ax_1x_2y_1y_2}, \frac{y_1y_2 - b^2x_1x_2}{1 - ax_1x_2y_1y_2} \right),$$

the identity is $(0,1)$, and $-(x,y) = (-x,y)$.

Furthermore, we have that

$$\mathrm{ord}_{\mathcal{O}^{\pm}}(x) = 0, \quad \mathrm{ord}_{\mathcal{O}^{\pm}}(y) = -1, \quad \mathrm{ord}_{\mathcal{Q}^{\pm}}(x) = -1, \quad \mathrm{ord}_{\mathcal{Q}^{\pm}}(y) = 0,$$

and

$$|\mathcal{O}^{\pm}| = 4, \quad |\mathcal{Q}^{\pm}| = 2.$$

Additionally, from the equation of $E_{a,b}$ we get involutions given by

$$\kappa_0(x,y) \overset{\text{def}}{=} (-x,y), \quad \kappa_1(x,y) \overset{\text{def}}{=} (x,-y), \quad \kappa_2(x,y) \overset{\text{def}}{=} \left(\frac{y}{b}, bx\right). \tag{3.3}$$

These extend to the points at infinity as:

$$\begin{aligned} &\kappa_0(\mathcal{O}^{\pm}) = \mathcal{O}^{\mp}, \qquad && \kappa_1(\mathcal{O}^{\pm}) = \mathcal{O}^{\pm}, \qquad && \kappa_2(\mathcal{O}^{\pm}) = \mathcal{Q}^{\pm}, \\ &\kappa_0(\mathcal{Q}^{\pm}) = \mathcal{Q}^{\pm}, && \kappa_1(\mathcal{Q}^{\pm}) = \mathcal{Q}^{\mp}, && \kappa_2(\mathcal{Q}^{\pm}) = \mathcal{O}^{\pm}. \end{aligned}$$

Letting $\mathcal{K}_1 \overset{\text{def}}{=} (0,-1)$ and $\mathcal{K}_2 \overset{\text{def}}{=} \left(\frac{1}{b}, 0\right)$, we have

$$\kappa_0(P) = -P, \quad \kappa_1(P) = \mathcal{K}_1 - P, \quad \kappa_2(P) = \mathcal{K}_2 - P. \tag{3.4}$$

This yields $\mathcal{K}_1 = 2\mathcal{O}^{\pm}$, $\mathcal{K}_2 = \mathcal{O}^{\pm} + \mathcal{Q}^{\pm}$, $\mathcal{K}_1 = 2\mathcal{K}_2$, $|\mathcal{K}_1| = 2$, and $|\mathcal{K}_2| = 4$.

Also,

$$\omega \overset{\text{def}}{=} \frac{2x}{1-y^2}\,\mathrm{d}y$$

is an invariant differential. Moreover, since the *Hasse invariant* of $E_{a,b}$ is the element $\mathfrak{h} \in \Bbbk$ such that $\mathcal{C}(\omega) = \mathfrak{h}^{1/p}\omega$, where $\mathcal{C}$ is the Cartier operator, we find that $\mathfrak{h}$ is the coefficient of x^{p-1} (or, equivalently, of y^{p-1}) in $((1-y^2)(b^2-ay^2))^{(p-1)/2}$.

4. The Elliptic Teichmüller Lift

Let $\Bbbk$ be a perfect field of characteristic $p > 2$,

$$E_{a,b}/\Bbbk : \ b_0^2x_0^2 + y_0^2 = 1 + a_0x^2y^2$$

be an ordinary twisted Edwards curve,

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

be its canonical lifting, and $\tau : E_{a,b}(\Bbbk) \to \boldsymbol{E_{a,b}}(\boldsymbol{W}(\Bbbk))$ be the elliptic Teichmüller. Then

$$\tau(x_0, y_0) = ((x_0, F_1, F_2, \ldots), (y_0, G_1, G_2, \ldots,)),$$

where F_i and G_i are in the function field $\Bbbk(E_{a,b})$.

The following lemma describes how τ acts on the points at infinity and how it interacts with the aforementioned involutions of $E_{a,b}$:

Lemma 4.1. *We have that $\tau(\mathcal{O}^{\pm}) = \boldsymbol{\mathfrak{O}}^{\pm}$ and $\tau(\mathcal{Q}^{\pm}) = \boldsymbol{\mathfrak{Q}}^{\pm}$. Moreover, if κ_i, for $i = 0, 1, 2$, represent both the involutions of $E_{a,b}$ and $\boldsymbol{E_{a,b}}$ (as in Eq.* (3.3)*), then we have that $\kappa_i \circ \tau = \tau \circ \kappa_i$.*

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

Note that this implies, since $\mathcal{K}_1 = 2\mathcal{O}^{\pm}$ and $\mathcal{K}_2 = 2\mathcal{K}_1$, we have that τ takes $\mathcal{K}_1$ and $\mathcal{K}_2$ to their corresponding points on $\boldsymbol{E_{a,b}}$. Thus, since τ is a group homomorphism, Eq. (3.4) gives the second part of the lemma. □

We now start to describe the coordinate functions F_i and G_i of τ.

Proposition 4.2. *The coordinate functions of the elliptic Teichmüller lift F_i and G_i are in the affine coordinate ring $\Bbbk[E_{a,b}]$, i.e., they can be given by polynomial functions.*

Proof. Since τ is a section of the reduction modulo p, we have that it must map the affine part of $E_{a,b}$ to the affine part of $\boldsymbol{E_{a,b}}$ (over $\overline{\Bbbk}$). Therefore, F_i and G_i are regular on the affine part of $\boldsymbol{E_{a,b}}$ (over $\overline{\Bbbk}$). □

Before we can refine our description of F_i and G_i, we need to introduce a simple unique representation for elements of $\Bbbk[E_{a,b}]$:

Lemma 4.3. *Let $f \in \Bbbk[E_{a,b}]$. Then,*

$$f = f_1(x_0) + f_2(y_0) + y_0 f_3(x_0) + x_0 f_4(y_0),$$

for some $f_1, f_2, f_3, f_4 \in \Bbbk$, with $f_2(0) = f_3(0) = f_4(0) = f_4'(0) = 0$. Moreover, this representation is unique in $\Bbbk[E_{a,b}]$.

Proof. First, we prove the existence of the representation. It suffices to prove for $f = x_0^r y_0^s$ for $r, s \geq 2$. We proceed by induction on $\min(r, s)$.

If $\min(r, s) = 2$, we may assume due to symmetry, that $r = 2$. Then,

$$\begin{aligned} x_0^2 y_0^s &= (x_0^2 y_0^2) y_0^{s-2} \\ &= \frac{1}{a_0} \left(b_0^2 x_0^2 + y_0^2 - 1 \right) y_0^{s-2} \\ &= \frac{1}{a_0} \left(b_0^2 x_0^2 y_0^{s-2} + y_0^s - y_0^{s-2} \right). \end{aligned}$$

If $s - 2 \leq 1$, then we are done. If not, we can repeat this process with $x_0^2 y_0^{s-2}$ until we have a representation as in the statement.

Now assume the statement is true for monomials $x_0^r y_0^s$ with $\min(r, s) \leq m$. Again, due to symmetry, it suffices to prove that the statement also holds for $x_0^{m+1} y_0^s$ (and $s \geq m + 1$). By the induction hypothesis, we have:

$$\begin{aligned} x_0^{m+1} y_0^s &= x_0 \left(f_1(x_0) + f_2(y_0) + y_0 f_3(x_0) + x_0 f_4(y_0) \right) \\ &= x_0 f_1(x_0) + x_0 f_2(y_0) + y_0(x_0 f_3(x_0)) + x_0^2 f_4(y_0). \end{aligned}$$

But we can again apply the induction hypothesis to the monomials of $x_0^2 f_4(y_0)$, which gives us the result.

For uniqueness, assume that in $\Bbbk[x_0, y_0]$ we have

$$\begin{aligned} f_1(x_0) + f_2(y_0) + y_0 f_3(x_0) + x_0 f_4(y_0) &= (b_0^2 x_0^2 + y_0^2 - 1 - a_0 x_0^2 y_0^2) \cdot h \\ &= y_0^2(1 - a_0 x_0^2) h + (b_0^2 x_0^2 - 1) h, \end{aligned}$$

for some $h \in \Bbbk[x_0, y_0]$. But then, if $h \neq 0$, let $cx_0^k y_0^l$ be one of the monomials of h with maximal degree on y_0. Then, we would necessarily have the term $a_0 c x_0^{k+2} y_0^{l+2}$ on the left side of the equation, which is a contradiction. □

We can now be more precise on the coordinate functions F_i and G_i.

Proposition 4.4. *We have that $F_i \in \Bbbk[x_0]$ and $G_i \in \Bbbk[y_0]$, and both are odd.*

Proof. Since τ is a group homomorphism, we have that $\tau(-x_0, y_0) = -\tau(x_0, y_0)$. Hence, since $p > 2$, for all $i \geq 1$ we must have:

$$F_i(-x_0, y_0) = -F_i(x_0, y_0), \tag{4.1}$$

$$G_i(-x_0, y_0) = G_i(x_0, y_0). \tag{4.2}$$

Moreover, since the involutions κ_1 commutes with τ, we have that for all $i \geq 1$,

$$F_i(x_0, -y_0) = F_i(x_0, y_0), \tag{4.3}$$

$$G_i(x_0, -y_0) = -G_i(x_0, y_0). \tag{4.4}$$

Thus, by Lemma 4.3, if we write $F_i = f_1(x_0) + f_2(y_0) + y_0 f_3(x_0) + x_0 f_4(y_0)$, with $f_2(0) = f_3(0) = f_4(0) = f_4'(0) = 0$, then by Eq. (4.1), we have that f_2 is zero and f_1 and f_3 are odd. By Eq. (4.3), we must have that f_3 is zero and f_4 is even. Hence $F_i = f_1(x_0) + x_0 f_4(y_0)$.

But, as noted before, we have that $\operatorname{ord}_{\mathcal{O}^+} x_0 = \operatorname{ord}_{\boldsymbol{\mathcal{O}}^+} \boldsymbol{x} = 0$ and $\operatorname{ord}_{\mathcal{O}^+} y_0 = -1$, which imply that $\tau^* \boldsymbol{x}$ must be regular at $\mathcal{O}^+$, and thus we must have that f_4 is zero (since f_4 has no constant term).

A similar argument yields that $G_i = g_2(y_0)$, with g_2 odd. □

5. Degrees of the Elliptic Teichmüller Lift

We can also determine the degrees of F_i and G_i. For that, we need some terminology and results from [6].

Let $K \overset{\text{def}}{=} \overline{\mathbb{k}}(E_{a,b})$ and $\boldsymbol{K}$ be the function field of $\boldsymbol{E_{a,b}}$ over the field of fractions $\boldsymbol{k}$ of $\boldsymbol{W}(\overline{\mathbb{k}})$. An element $\boldsymbol{g} \in \boldsymbol{K}$ can be written as a quotient $\boldsymbol{g}_1/\boldsymbol{g}_2$, where $\boldsymbol{g}_1, \boldsymbol{g}_2 \in \boldsymbol{W}(\overline{\mathbb{k}})[\boldsymbol{x}, \boldsymbol{y}]$. Let $\boldsymbol{R}$ be the ring of functions $\boldsymbol{g} = \boldsymbol{g}_1/\boldsymbol{g}_2 \in \boldsymbol{K}$, such that $\boldsymbol{g}_2 \not\equiv 0 \pmod{p}$. (Then $\boldsymbol{R}$ is the valuation ring of $\boldsymbol{K}$ with respect to the valuation associated to p). We can identify $\boldsymbol{R}$ with a subring of $\boldsymbol{W}(K)$ (via τ^*). Then, for every $\boldsymbol{g} \in \boldsymbol{R}$ we have $\tau^*\boldsymbol{g} = (g_0, g_1, \dots) \in \boldsymbol{W}(K)$, and if $\boldsymbol{g}$ is regular at $\tau(P)$, for $P \in E_{a,b}(\overline{\mathbb{k}})$, then g_i is regular at P for every $i \geq 0$ and $\boldsymbol{g}(\tau(P)) = (g_0(P), g_1(P), \dots)$.

Define, for $P \in E_{a,b}(\overline{\mathbb{k}})$,

$$\boldsymbol{U}(P) \overset{\text{def}}{=} \{\boldsymbol{g} \in \boldsymbol{R}^\times \mid \operatorname{ord}_{\tau(P)}(\boldsymbol{g}) = \operatorname{ord}_P(g_0)\}.$$

Observe that clearly $\boldsymbol{U}(P)$ is a subgroup of $\boldsymbol{R}^\times$.

We can now state [6, Theorem 3.1] and [6, Corollary 4.5]:

Theorem 5.1. *Let $\boldsymbol{g} \in \boldsymbol{U}(P)$ with $\tau^*\boldsymbol{g} = (g_0, g_1, \dots)$. Then*

$$\operatorname{ord}_P(g_n) \geq p^n(\operatorname{ord}_P(g_0) - n) + np^{n-1}, \text{ for all } n \geq 0.$$

Theorem 5.2. *The inequality of Theorem 5.1 is an equality if and only if*

$$\binom{\operatorname{ord}_P(g_0)}{n} \not\equiv 0 \pmod{p}.$$

Thus, we obtain:

Corollary 5.3. *For all $n \geq 1$ we have*

$$\deg_{x_0} F_n = \deg_{y_0} G_n = (n+1)p^n - np^{n-1}.$$

Proof. First observe that $\operatorname{ord}_{\mathcal{Q}^{\pm}}(x_0) = \operatorname{ord}_{\mathcal{O}^{\pm}}(y_0) = -1$, $\boldsymbol{x} \in \boldsymbol{U}(\mathcal{Q}^{\pm})$, $\boldsymbol{y} \in \boldsymbol{U}(\mathcal{O}^{\pm})$, and

$$\binom{-1}{n} = (-1)^n \not\equiv 0 \pmod{p}.$$

Then, Theorems 5.1 and 5.2 give us the result. □

6. Derivatives of F_n and G_n

We now follow [7] to obtain formulas for the derivatives of F_n and G_n. Applying [7, Corollary 4.2] to the elliptic Teichmüller lift, we obtain:

Theorem 6.1. *If $\boldsymbol{\phi}$ denotes the lift of the Frobenius, then the reductions modulo p of*

$$\left(\frac{1}{p^n}\boldsymbol{\phi}^n\right)^{*} \mathrm{d}\boldsymbol{x} \quad \text{and} \quad \left(\frac{1}{p^n}\boldsymbol{\phi}^n\right)^{*} \mathrm{d}\boldsymbol{y}$$

are

$$\begin{aligned} &\mathrm{d}F_n + F_{n-1}^{p-1}\mathrm{d}F_{n-1} + \cdots + F_1^{p^{n-1}-1}\mathrm{d}F_1 + x_0^{p^n-1}\mathrm{d}x_0, \\ &\mathrm{d}G_n + G_{n-1}^{p-1}\mathrm{d}G_{n-1} + \cdots + G_1^{p^{n-1}-1}\mathrm{d}G_1 + y_0^{p^n-1}\mathrm{d}y_0, \end{aligned}$$

respectively.

We then have:

Theorem 6.2. *We have*

$$\begin{aligned} \frac{\mathrm{d}F_n}{\mathrm{d}x_0} &= \mathfrak{h}^{(p^n-1)/(p-1)}(b_0^2x_0^2-1)^{(p^n-1)/2}(a_0x_0^2-1)^{(p^n-1)/2} - \sum_{k=0}^{n-1} F_k^{p^{n-k}-1}\frac{\mathrm{d}F_k}{\mathrm{d}x_0}, \\ \frac{\mathrm{d}G_n}{\mathrm{d}y_0} &= \mathfrak{h}^{(p^n-1)/(p-1)}(b_0^2-ay_0^2)^{(p^n-1)/2}(1-y_0^2)^{(p^n-1)/2} - \sum_{k=0}^{n-1} G_k^{p^{n-k}-1}\frac{\mathrm{d}G_k}{\mathrm{d}y_0}, \end{aligned}$$

where $\mathfrak{h}$ is the Hasse invariant of $E_{a,b}$.

Proof. Let ω be the reduction modulo p of

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

Then, we have that $\omega = \lambda\omega_0$ for some $\lambda \in \Bbbk^\times$, where $\omega_0 \overset{\text{def}}{=} \dfrac{2x_0}{1-y_0^2}\mathrm{d}y_0$. Applying the Cartier operator $\mathcal{C}$, we obtain

$$\mathcal{C}^n(\omega) = \lambda^{1/p}\mathfrak{h}^{1/p+1/p^2+\cdots+1/p^n}\omega_0.$$

On the other hand, since $(1/p\,\boldsymbol{\phi})^*$ is the "inverse" of the Cartier operator, we must have that $\mathcal{C}^n(\omega) = \omega_0$, which yields

$$\lambda = \mathfrak{h}^{-(p^n-1)/(p-1)},$$

and thus $\omega = \mathfrak{h}^{-(p^n-1)/(p-1)}\omega_0$.

On the other hand, by Theorem 6.1, we obtain

$$\omega = \frac{2x_0^{p^n}}{(1-y_0^2)^{p^n}}\left(\mathrm{d}G_n + G_{n-1}^{p-1}\mathrm{d}G_{n-1} + \cdots + G_1^{p^{n-1}-1}\mathrm{d}G_1 + y_0^{p^n-1}\mathrm{d}y_0\right).$$

Setting these two expressions for ω equal to each other yields

$$\mathrm{d}G_n = \mathfrak{h}^{-(p^n-1)/(p-1)}\frac{(1-y_0^2)^{p^n-1}}{x_0^{p^{n-1}}} - \sum_{k=0}^{n-1} G_k^{p^n-k-1}\mathrm{d}G_k.$$

Since we have that $x_0^2 = (1-y_0^2)/(b_0^2 - ay_0^2)$, we obtain the formula for $\mathrm{d}G_n/\mathrm{d}y_0$.

The formula for $\mathrm{d}F_n/\mathrm{d}x_0$ can be obtained by observing that

$$\omega_0 = \frac{2y_0}{b_0^2x_0^2-1}\mathrm{d}x_0$$

and following the same approach as above. □

7. Criterion

In explicit computations we need a concrete criterion to determine if we obtained the actual canonical lifting and elliptic Teichmüller lift. In this section we present such criterion. The crucial result is found in the proof of [18, Proposition 4.2], which we adapt to Edwards curves below:

Theorem 7.1. *Let $E_{a,b}/\Bbbk$ be an ordinary Edwards curve, $\boldsymbol{E_{a,b}}/\boldsymbol{W}(\Bbbk)$ be a lifting of $E_{a,b}$, and τ be a section of the reduction modulo p between the* affine *parts of $E_{a,b}$ and $\boldsymbol{E_{a,b}}$. If τ is regular at the points at infinity $\mathcal{O}^\pm$, $\mathcal{Q}^\pm$, with $\tau(\mathcal{O}^\pm) = \boldsymbol{\mathcal{O}}^\pm$, $\tau(\mathcal{Q}^\pm) = \boldsymbol{\mathcal{Q}}^\pm$, respectively, then $\boldsymbol{E_{a,b}}$ is the canonical lifting of $E_{a,b}$ and τ is the elliptic Teichmüller lift.*

We then immediately have:

Corollary 7.2. *Let $E_{a,b}/\Bbbk$ be an ordinary Edwards curve, $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}(\Bbbk)$ be a lifting of $E_{a,b}$, and $\tau = ((x_0, F_1, F_2, \ldots), (y_0, G_1, G_2, \ldots))$ be a section of the reduction modulo p between the* affine *parts of $E_{a,b}$ and $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$. Then, $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ is the canonical lifting of $E_{a,b}$ and τ is the elliptic Teichmüller lift if and only if $\tau^*(1/\boldsymbol{x})(\mathcal{Q}^{\pm}) = \tau^*(1/\boldsymbol{y})(\mathcal{O}^{\pm}) = 0$.*

Proof. This follows from the previous theorem and the already observed facts that

$$\mathrm{ord}_{\mathcal{O}^{\pm}}(y_0) = \mathrm{ord}_{\boldsymbol{\mathcal{O}}^{\pm}}(\boldsymbol{y}) = \mathrm{ord}_{\mathcal{Q}^{\pm}}(x_0) = \mathrm{ord}_{\boldsymbol{\mathcal{Q}}^{\pm}}(\boldsymbol{x}) = 0.$$

□

8. The Algorithm

We now describe an algorithm to simultaneously compute the canonical lifting and elliptic Teichmüller lift of an Edwards curve. We inductively assume that we have computed the first n coordinates and need to find the $(n+1)$-st coordinated of $\boldsymbol{a}$, $\boldsymbol{b}$ and τ, i.e., a_n, b_n, F_n, and G_n.

We know that F_n and G_n are *odd* polynomials of degree $(n+1)p^n - np^{n-1}$ in x_0 and y_0 respectively, and we know their derivatives. Thus, let $\hat{F}_n$ and $\hat{G}_n$ be the formal integrals of $\mathrm{d}F_n/\mathrm{d}x_0$ and $\mathrm{d}G_n/\mathrm{d}y_0$ with respect to x_0 and y_0 respectively. Then,

$$F_1 = \hat{F}_1 + c_1 x_0^p \qquad G_1 = \hat{G}_1 + d_1 y_0^p,$$

and if we let $N_n \overset{\text{def}}{=} ((n+1)p^{n-1} - np^{n-2} - 1)/2$, for $n \geq 2$ we can write,

$$F_n = \hat{F}_n + \sum_{i=0}^{N_n} c_{2i+1} x_0^{(2i+1)p}, \qquad G_n = \hat{G}_n + \sum_{i=0}^{N_n} d_{2i+1} y_0^{(2i+1)p},$$

where the c_i's and d_i's (for i odd) are unknown. (We might refer to c_i and d_i for i even with the implicit assumption that these terms are zero.)

By the criterion above, we need $\tau^*(1/\boldsymbol{x})(\mathcal{Q}^{\pm}) = \tau^*(1/\boldsymbol{y})(\mathcal{O}^{\pm}) = 0$. In general, if $\boldsymbol{t} = (t_0, t_1, \ldots)$, then the $(n+1)$-st coordinate of $1/\boldsymbol{t}$ is given by

$$\frac{-t_0^{(n-1)p^n} t_n + h}{t_0^{(n+1)p^n}}, \text{ for some } h \in \mathbb{F}_p[t_0, t_1, \ldots, t_{n-1}].$$

Thus, since $\tau^*(1/\boldsymbol{x})(\mathcal{Q}^{\pm}) = 0$ and $\operatorname{ord}_{\mathcal{Q}^{\pm}} x_0 = -1$, the terms in x_0^i for $i \geq (n+1)p^n$ in $x_0^{(n-1)p^n} F_n + h(x_0, F_1, \ldots, F_{n-1})$ cancel out, and since $F_1, \ldots, F_{n-1}$ are all known, we can find all c_i's with $i \geq 2p^{n-1}$.

Similarly, $\tau^*(1/\boldsymbol{y})(\mathcal{O}^{\pm}) = 0$ and $\operatorname{ord}_{\mathcal{O}^{\pm}} y_0 = -1$ allow us to find all d_i's with $i \geq 2p^{n-1}$. Thus, only c_i's and d_i's for $i = 0, \ldots, (2p^{n-1} - 1)$ and odd remain to be found (along with a_n and b_n).

Since τ is a lifting of points, it follows that

$$\tau^*(\boldsymbol{b}^2 \boldsymbol{x}^2 + \boldsymbol{y}^2) = \tau^*(1 + \boldsymbol{a}\boldsymbol{x}^2\boldsymbol{y}^2),$$

and at the $(n+1)$-st coordinate we get:

$$2(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}) x_0^{p^n} F_n + 2(1 - a_0^{p^n} x_0^{2p^n}) y_0^{p^n} G_n + \tilde{b}_n x_0^{2p^n} - a_n x_0^{2p^n} y_0^{2p^n} = \cdots, \tag{8.1}$$

where all the omitted terms are known by our induction hypothesis and $\tilde{b}_n$ is the $(n+1)$-st coordinate of $\boldsymbol{b}^2$, and hence equal to $2b_0^{p^n} b_n + \cdots$ where all the omitted terms are also known. Using our expressions for F_n and G_n (in terms of the unknown F_i's and G_i's) above and Lemma 4.3, we can expand both sides of the above equation using the unique representation of the lemma. Thus, we can compare coefficients of both sides of the equation, giving a linear system on the unknowns a_n, b_n, and c_i and d_i, for $i = 0, \ldots, (2p^{n-1} - 1)$. The existence of the canonical lifting guarantees the existence of a solution, and Theorem 7.1 guarantees that this solution will give the canonical lifting and the elliptic Teichmüller lift.

Observe that the involution $\kappa_2(x, y) = (y/b, bx)$, and the fact that it commutes with the elliptic Teichmüller lift, allows us to find the coefficients d_i's from the c_i's, so we don't need as many unknowns in the system.

Note also that it is clear that, maybe extending the base field, one could take $\boldsymbol{b}$ in the canonical lifting as $(b_0, 0, 0, \ldots)$. In this case, the observation above gives that $F_n(y_0/b_0) = G(y_0)/b_0^{p^n}$, i.e., $d_i = b_0^{p^n - ip} c_i$. In particular, when $b_0 = 1$, we have that $F_n = G_n$.

p	n	time (in seconds)	memory (in MB)
3	2	0.01	32.09
3	3	1.56	46.04
3	4	1,115.91	3,882.94
5	1	0.01	32.09
5	2	0.62	64.12
5	3	9,009.399	23,747.53
7	1	0.04	32.09
7	2	15.58	242.25
11	1	0.03	32.09
11	2	1,483.42	9,158.34
13	1	0.03	32.09
13	2	8,131.18	37,400.62

Table 8.1. Time and memory usage in computing canonical lifting and elliptic Teichmüller lift.

Computations with Witt vectors in general are complex, but using the techniques from [9], one can obtain general formulas for small primes and short lengths in reasonable time. Table 8.1 shows the times and memory used to compute general formulas (as in Section 10) for characteristic p and length $n + 1$ for various p and n in a computer with an Intel Core i7-8700 CPU with 46 gigabytes of memory running MAGMA.

One computation that slows down the algorithm considerably is writing the coordinates of the Greenberg transform in the unique form of Lemma 4.3. This step makes these computations slower than the ones for elliptic curves given by a Weierstrass equation, as obtaining a unique representation is much simpler in that case.

On the other hand, once this step is accomplished, solving the obtained linear system is faster than the Weierstrass case. Moreover, the criterion for regularity at the points at infinity is considerably simpler to implement for $n \geq 3$ than for Weierstrass equations. (In fact, the second author's code for the Weierstrass case only works for $n \leq 2$, as $n = 1$ is trivial and for $n = 2$ a simpler implementation is given in [6].)

The code used in the computations is available at `https://github.com/lrfinotti/witt`.

9. Solutions to the System

Canonical liftings are unique only up to isomorphism, so clearly we will not have a unique solution to the linear system obtained by the algorithm described in the previous section. Note that the requirements on the elliptic Teichmüller lift, namely, that $\tau(\mathcal{O}^{\pm}) = \boldsymbol{\mathcal{O}}^{\pm}$ and $\tau(\mathcal{Q}^{\pm}) = \boldsymbol{\mathcal{Q}}^{\pm}$, force the isomorphism to send the points at infinity to their corresponding points on the isomorphic curve. So, if the pairs $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{a}', \boldsymbol{b}')$ are the coefficients of the equations for these isomorphic Edwards curves, then there is some $\boldsymbol{\lambda}$ such that

$$\boldsymbol{a}' = \frac{1}{\boldsymbol{\lambda}^2}\boldsymbol{a}, \quad \boldsymbol{b}' = \frac{1}{\boldsymbol{\lambda}}\boldsymbol{b} \tag{9.1}$$

In this section we will study the different possible solutions to the system, by investigating how isomorphisms affect the equations. But before we proceed, we need to briefly review the *Greenberg transform*. We will take a simple and computational approach, but more details can be found in [12] and [11], or, for more advanced references, see [3] and [13].

Let $R = \Bbbk[x_0, y_0, x_1, y_1, \ldots]$ and $\boldsymbol{x}_0 = (x_0, x_1, \ldots), \boldsymbol{y}_0 = (y_0, y_1, \ldots) \in \boldsymbol{W}(R)$. Thus, if $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}] \subseteq \boldsymbol{W}(R)[\boldsymbol{x}, \boldsymbol{y}]$, where $\boldsymbol{x}$ and $\boldsymbol{y}$ are the variables of the polynomial ring, then $\boldsymbol{f}(\boldsymbol{x}_0, \boldsymbol{y}_0) \in \boldsymbol{W}(R)$. (We are basically replacing the variables $\boldsymbol{x}$ and $\boldsymbol{y}$ by Witt vectors of variables $\boldsymbol{x}_0 = (x_0, x_1, \ldots)$ and $\boldsymbol{y}_0 = (y_0, y_1, \ldots)$.) Hence, we have that $\boldsymbol{f}(\boldsymbol{x}_0, \boldsymbol{y}_0) = (f_0, f_1, \ldots)$, where $f_i \in R$, or more precisely, where $f_i \in \Bbbk[x_0, \ldots, x_i, y_0, \ldots, y_i]$.

Definition 9.1. For $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$, we refer to $\boldsymbol{f}(\boldsymbol{x}_0, \boldsymbol{y}_0) \in \boldsymbol{W}(R)$ as above as the *Greenberg transform* of $\boldsymbol{f}$, and denote it by $G(\boldsymbol{f})$.

Moreover, if

$$\boldsymbol{C}/\boldsymbol{W}(\Bbbk) \ : \ \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{0},$$

we define the *Greenberg transform* $G(\boldsymbol{C})$ of $\boldsymbol{C}$ to be the (infinite dimensional) variety over $\Bbbk$ defined by the zeros of the coordinates f_n of $G(\boldsymbol{f})$, i.e., if $G(\boldsymbol{f}) = (f_0, f_1, \ldots)$ as above, then

$$\begin{aligned} G(\boldsymbol{C})/\Bbbk \ : & f_0(x_0, y_0) = 0 \\ & f_1(x_0, x_1, y_0, y_1) = 0 \\ & f_2(x_0, x_1, x_2, y_0, y_1, y_2) = 0 \\ & \vdots \end{aligned}$$

Note that in practice we deal with Witt vectors of finite length, in which case we can truncate the Greenberg transform and then have a *finite dimensional* variety over $\Bbbk$.

Moreover, it should be clear from the definition that there is a bijection between rational points $\boldsymbol{C}(\boldsymbol{W}(\Bbbk))$ and $G(\boldsymbol{C})(\Bbbk)$, as $\boldsymbol{f}(\boldsymbol{a}, \boldsymbol{b}) = \boldsymbol{0}$, with $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$, if and only if $f_n(a_0, \ldots, a_n, b_0, \ldots, b_n) = 0$ for all n.

Now, on the $(n+1)$-st coordinate of the Greenberg transform of $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ we have (similar to Eq. (8.1)):

$$2(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}) x_0^{p^n} x_n + 2(1 - a_0^{p^n} x_0^{2p^n}) y_0^{p^n} y_n + \tilde{b}_n x_0^{2p^n} - a_n x_0^{2p^n} y_0^{2p^n} = \cdots ,$$

where no omitted term involve either a_n, b_n, x_n, or y_n, and $\tilde{b}_n$ is the $(n+1)$-st coordinate of $\boldsymbol{b}^2$, and hence equal to $2b_0^{p^n} b_n + \cdots$ where all the omitted terms involve only b_i for $i < n$.

Let's then assume that we've computed the canonical lifting of $E_{a,b}$ up the n-th coordinate and now want to compute the $(n+1)$-st coordinate, i.e., we need a_n, b_n, F_n (i.e., the unknown c_i's) and G_n (i.e., the unknown d_i's). Suppose we have two extensions the $(n+1)$-st coordinate, given by $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$, with its associated elliptic Teichmüller lift τ, and $\boldsymbol{E}_{\boldsymbol{a}',\boldsymbol{b}'}$, with its associated elliptic Teichmüller lift τ'. Thus, if

$$\begin{aligned} \boldsymbol{a} &= (a_0, a_1, \ldots, a_{n-1}, a_n), \\ \boldsymbol{b} &= (b_0, b_1, \ldots, b_{n-1}, b_n), \\ \tau &= ((x_0, F_1, \ldots, F_{n-1}, F_n), (y_0, G_1, \ldots, G_{n-1}, G_n)), \end{aligned}$$

then we have

$$\begin{aligned}\boldsymbol{a}' &= (a_0, a_1, \dots, a_{n-1}, a_n')\\ \boldsymbol{b}' &= (b_0, b_1, \dots, b_{n-1}, b_n')\\ \tau' &= ((x_0, F_1, \dots, F_{n-1}, F_n'), (y_0, G_1, \dots, G_{n-1}, G_n')).\end{aligned}$$

Moreover, if

$$F_n = \hat{F}_n + \sum_{i=0}^{N_n} c_{2i+1} x_0^{(2i+1)p}, \qquad G_n = \hat{G}_n + \sum_{i=0}^{N_n} d_{2i+1} y_0^{(2i+1)p},$$

as above, we must have that

$$F_n' = \hat{F}_n + \sum_{i=0}^{N_n} c_{2i+1}' x_0^{(2i+1)p}, \qquad G_n' = \hat{G}_n + \sum_{i=0}^{N_n} d_{2i+1}' y_0^{(2i+1)p}.$$

Since τ and τ' lift points, the difference of the pull-backs of the $(n+1)$-st coordinate of the Greenberg transforms of $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ and $\boldsymbol{E}_{\boldsymbol{a}',\boldsymbol{b}'}$ by τ and τ' respectively give:

$$\begin{multline}2(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}) x_0^{p^n} \left(\sum_{i=0}^{N_n} (c_{2i+1}' - c_{2i+1}) x_0^{(2i+1)p} \right)\\ + 2(1 - a_0^{p^n} x_0^{2p^n}) y_0^{p^n} \left(\sum_{i=0}^{N_n} (d_{2i+1}' - d_{2i+1}) y_0^{(2i+1)p} \right)\\ + 2b_0^{p^n}(b_n' - b_n) x_0^{2p^n} - (a_n' - a_n) x_0^{2p^n} y_0^{2p^n} = 0\end{multline}$$

Since both solutions are canonical liftings (and hence isomorphic), the coefficients must satisfy Eq. (9.1), and since the coefficients agree up to the n-th coordinate, we must have that

$$\boldsymbol{\lambda} = (1, 0, 0, \dots, \lambda_n).$$

Thus,

$$a_n' = a_n - 2\lambda_n a_0^{p^n}, \qquad b_n' = b_n - \lambda_n b_0^{p^n}.$$

Hence, the equation above simplifies to

$$\begin{aligned} 2(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}) x_0^{p^n} \left(\sum_{i=0}^{N_n} (c'_{2i+1} - c_{2i+1}) x_0^{(2i+1)p} \right) \\ + 2(1 - a_0^{p^n} x_0^{2p^n}) y_0^{p^n} \left(\sum_{i=0}^{N_n} (d'_{2i+1} - d_{2i+1}) y_0^{(2i+1)p} \right) \\ - 2\lambda_n b_0^{2p^n} x_0^{2p^n} + 2\lambda_n a_0^{p^n} x_0^{2p^n} y_0^{2p^n} = 0. \quad (9.2) \end{aligned}$$

Now, the choice of λ_n uniquely determines $\boldsymbol{E}_{\boldsymbol{a}',\boldsymbol{b}'}$ (from $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$) and since the elliptic Teichmüller lift associate to a specific equation is unique, we have that there is only one possible way to define the c'_i's and d'_i's from the c_i's, d_i's and λ_n. We claim then that we must have:

$$c'_i = \begin{cases} c_i, \text{ for } i \neq p^{n-1}, \\ c_i + \lambda_n, \text{ for } i = p^{n-1}, \end{cases} \quad , \quad d'_i = d_i,$$

and to verify it, it suffices to show that Eq. (9.2) is satisfied. But, in this case, we that the left hand side becomes:

$$2(b_0^{2p^n} - a_0^{p^n} y_0^{2p^n}) \lambda_n x_0^{2p^n} - 2\lambda_n b_0^{2p^n} x_0^{2p^n} + 2\lambda_n a_0^{p^n} x_0^{2p^n} y_0^{2p^n}$$

which is clearly zero.

Hence, when finding the canonical lifting of Edwards curves (and the associated elliptic Teichmüller lifts) with the algorithm described above, the linear system has exactly one free parameter, which allows us to choose exactly one arbitrary value for either a_n, b_n, or $c_{p^{n-1}}$.

10. Formulas

We can obtain general formulas for the canonical lifting of an ordinary Edwards curve and its associated Teichmüller lift by applying the algorithm from Section 8 to

$$\boldsymbol{E}_{a,b}/\mathbb{K} : \; b^2 x_0 + y_0^2 = 1 + a x_0^2 y_0^2,$$

where $\mathbb{K} = \mathbb{F}_p(a, b)$, with a, b *indeterminates.*

For example, for $p = 3$ we obtain

$$\begin{aligned}
a_1 &= \frac{a^3(2a+b^2)}{a+b^2},\\
b_1 &= \frac{b^3(2a+b^2)}{a+b^2},\\
F_1 &= \frac{ab^2}{a+b^2}\, x_0^5 + \frac{2}{a+b^2}\, x_0,\\
G_1 &= \frac{a}{a+b^2}\, y_0^5 + \frac{2a+b^2}{a+b^2}\, y_0^3 + \frac{2b^2}{a+b^2}\, y_0.
\end{aligned}$$

Note that $a + b^2$ is the Hasse invariant of the curve in this case. Forcing $b_1 = 0$, we obtain:

$$\begin{aligned}
a_1 &= \frac{a^3(a+2b^2)}{a+b^2},\\
b_1 &= 0,\\
F_1 &= \frac{ab^2}{a+b^2}\, x_0^5 + \frac{2a+b^2}{a+b^2}\, x_0^3 + \frac{2}{a+b^2}\, x_0,\\
G_1 &= \frac{a}{a+b^2}\, y_0^5 + \frac{2a+b^2}{a+b^2}\, y_0^3 + \frac{2b^2}{a+b^2}\, y_0.
\end{aligned}$$

Note that $a_1, b_1 \in \mathbb{K}$, i.e., are rational functions on a and b. In fact, we have:

Proposition 10.1. *Given $p \geq 3$, there are rational functions $A_i, B_i \in \mathbb{K}$ and polynomials $F_i \in \mathbb{K}[x_0]$, $G_i \in \mathbb{K}[y_0]$, such that if a_0 and b_0 are coefficients of an ordinary twisted Edwards curve, then*

$$\boldsymbol{a} = (a_0, A_1(a_0, b_0), A_2(a_0, b_0), \ldots), \quad \boldsymbol{b} = (b_0, B_1(a_0, b_0), B_2(a_0, b_0), \ldots),$$

give coefficients of its canonical lifting, whenever A_i and B_i are defined on (a_0, b_0), and its elliptic Teichmüller lift is given by

$$\tau = ((x_0, F_1(a_0, b_0, x_0), F_2(a_0, b_0, x_0), \ldots), (y_0, G_1(a_0, b_0, y_0), G_2(a_0, b_0, y_0), \ldots)),$$

whenever the coefficients of F_i and G_i are defined on (a_0, b_0).

Proof. Again, we start by applying the algorithm to the twisted Edwards curve given by the coefficients $a, b \in \mathbb{K}$. Inductively, assume that for $i < n$ we have that the algorithm finds $a_i, b_i \in \mathbb{K}$, $F_i \in \mathbb{K}[x_0]$, $G_i \in \mathbb{K}[y_0]$.

Then, in computing the $(n+1)$-st coordinate, the obtained linear system is defined over $\mathbb{K}$. Therefore, choosing either a_n, b_n, or $c_{p^{n-1}}$ in $\mathbb{K}$ will give $a_n, b_n \in \mathbb{K}$, $F_n \in \mathbb{K}[x_0]$, $G_n \in \mathbb{K}[y_0]$.

Now, given the coefficients a_0 and b_0 of an ordinary twisted Edwards curve, the criterion from Theorem 7.1 will be satisfied by the twisted Edwards curve given by the coefficients $\boldsymbol{a} = (a_0, A_1(a_0, b_0), A_2(a_0, b_0), \ldots)$, $\boldsymbol{b} = (b_0, B_1(a_0, b_0), B_2(a_0, b_0), \ldots)$ and the lift of points given by

$$(x_0, y_0) \mapsto ((x_0, F_1(a_0, b_0, x_0), F_2(a_0, b_0, x_0), \ldots), (y_0, G_1(a_0, b_0, y_0), G_2(a_0, b_0, y_0), \ldots))$$

by construction, and therefore give the canonical lifting and elliptic Teichmüller lift. □

11. Universality

Proposition 10.1 tell us we can find formulas, given by rational functions, to get the canonical lifting of twisted Edwards curves (and its corresponding elliptic Teichmüller lift), but with the restriction that these functions must be defined on the coefficients of the original curve.

We call the formulas *universal* if they are defined for every pair (a_0, b_0) that give an *ordinary* twisted Edwards curve. In terms of rational functions, this is the same as saying that, with the notation of the proposition, we have $A_i, B_i \in \mathbb{U}$, $F_i \in \mathbb{U}[x_0]$, and $G_i \in \mathbb{U}[y_0]$, where $\mathbb{U} \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/(\Delta \cdot \mathfrak{h})]$. (Note that since $\Delta = ab^2(a - b^2)$, we have $\mathbb{U} = \mathbb{F}_p[a, b, 1/a, 1/b^2, 1/(a - b^2), 1/\mathfrak{h}]$.)

Note that we do not necessarily always get universal formulas, as we may freely choose a_1 in the algorithm, and thus a_1 could be some rational function not in $\mathbb{U}$. On the other hand, we can always obtain universal formulas:

Theorem 11.1. *There are universal formulas for the canonical lifting of twisted Edwards curves. More precisely, there are $A_i, B_i \in \mathbb{U}$, $F_i \in \mathbb{U}[x_0]$, and $G_i \in \mathbb{U}[y_0]$, such that if a_0 and b_0 are coefficients of an ordinary Edwards, then*

$$\boldsymbol{a} = (a_0, A_1(a_0, b_0), A_2(a_0, b_0), \ldots), \quad \boldsymbol{b} = (b_0, B_1(a_0, b_0), B_2(a_0, b_0), \ldots),$$

give coefficients of its canonical lifting, whenever A_i and B_i are defined on (a_0, b_0), and its elliptic Teichmüller lift is given by

$$\tau = ((x_0, F_1(a_0, b_0, x_0), F_2(a_0, b_0, x_0), \ldots), (y_0, G_1(a_0, b_0, y_0), G_2(a_0, b_0, y_0), \ldots)).$$

Moreover, all such liftings are obtained by choosing either a_n, b_n, or $c_{p^{n-1}}$ in $\mathbb{U}$ in the algorithm.

Proof. We can inductively assume that $a_i, b_i \in \mathbb{U}$, $F_i \in \mathbb{U}[x_0]$, $G_i \in \mathbb{U}[y_0]$, for $i < n$, and then proof that the same holds for $i = n$ for some choice of the free parameter of the system.

First note that, as observed in Section 9, only a_n, b_n, and $c_{p^{n-1}}$ can have different values, all other unknowns (i.e., the c_i's for $i \neq p^{n-1}$ and all d_i's) are automatically defined for *all* ordinary Edwards curves and thus these must be in $\mathbb{U}$.

Then, by choosing $c_{p^{n-1}} = 0 \in \mathbb{U}$, we get that $F_n \in \mathbb{U}[x_0]$ and $G_n \in \mathbb{U}[y_0]$. Moreover, by our induction hypothesis, all terms omitted terms in Eq. (8.1) are in $\mathbb{U}[x_0, y_0]$. (Hence, our system is over $\mathbb{U}$.)

Observing that

$$x_0^{2p^n} y_0^{2p^n} = \frac{1}{a^{p^n}} \left(b^{2p^n} x_0^{2p^n} + y_0^{2p^n} - 1 \right),$$

and since $1/a, 1/b \in \mathbb{U}$, Eq. (8.1) then gives us that

$$\left(2b^{p^n} b_n - \frac{b^{2p^n}}{a^{p^n}} a_n \right) x_0^{2p^n} - \frac{1}{a^{p^n}} a_n y_0^{2p^n} - \frac{1}{a^{p^n}} a_n = \cdots$$

where all omitted terms are in $\mathbb{U}[x_0, y_0]$. Noting that the left-hand side is in the form for which we have unique representation (by Lemma 4.3), expressing the omitted terms in this form and comparing terms without x_0 or y_0 we obtain that $a_n \in \mathbb{U}$. Then, comparing terms in $x_0^{2p^n}$ gives us that $b_n \in \mathbb{U}$.

Therefore, choosing $c_{p^{n-1}} = 0$ when solving the system gives formulas for a_n, b_n, F_n, and G_n that are universal. Then, with change of variables (as discussed in Section 9) given by $a'_n = a_n - 2\lambda_n a^{p^n}$, $b'_n = b_n - 2\lambda_n b^{p^n}$, $c'_{p^{n-1}} = 0 + \lambda_n$, since $1/a, 1/b \in \mathbb{U}$, we can choose any value in $\mathbb{U}$ for a_n, b_n, or $c_{p^{n-1}}$ and still obtain universal formulas. In particular, choosing $b_n = 0$ also gives us universal formulas (and improves our algorithm, as described in Section 8). □

12. Modularity

We now further study properties of the formulas for the canonical lifting. We start with a definition:

Definition 12.1. Assigning weights $\mathrm{wgt}(a) \overset{\text{def}}{=} -2$, $\mathrm{wgt}(b) \overset{\text{def}}{=} -1$, let

$$\mathcal{S}_n = \left\{ \frac{f}{g} \in \mathbb{K} \ : \ f, g \in \mathbb{F}_p[a,b] \text{ homog. and } \mathrm{wgt}(f) - \mathrm{wgt}(g) = n \right\} \cup \{0\}.$$

The elements of $\mathcal{S}_n$ are then *modular functions of weight n*.

Let also $\mathrm{wgt}(x_0) = 1$ and $\mathrm{wgt}(y_0) \overset{\text{def}}{=} 0$, so that $bx_0^2 + y_0^2$ and $1 + ax_0^2y_0^2 + b$ are both homogeneous of weight 0. Then, define:

$$\hat{\mathcal{S}}_n = \left\{ \frac{f}{g} \in \mathbb{K}(x_0, y_0) \ : \ f, g \in \mathbb{F}_p[a, b, x_0, y_0] \text{ homog. and } \mathrm{wgt}(f) - \mathrm{wgt}(g) = n \right\} \cup \{0\}.$$

We prove that:

Theorem 12.2. *There are universal formulas $A_i, B_i \in \mathbb{U}$, $F_i \in \mathbb{U}[x_0]$, $G_i \in \mathbb{U}[y_0]$, with $A_i \in \mathcal{S}_{-2p^i}$, $B_i \in \mathcal{S}_{-p^i}$, $F_i \in \hat{\mathcal{S}}_{p^i}$, $G_i \in \hat{\mathcal{S}}_0$. Moreover, these can be obtained by simply choosing $B_i = 0$ in the algorithm.*

We shall need [10, Lemma 3.1]:

Lemma 12.3. *Let $\pi_i : \boldsymbol{W}(\Bbbk) \to \Bbbk$ denote the map that gives the $(i+1)$-st coordinate of a Witt vector. Then, if $\pi_i(\boldsymbol{f}) \in \hat{\mathcal{S}}_{rp^i}$ and $\pi_i(\boldsymbol{g}) \in \hat{\mathcal{S}}_{sp^i}$, then $\pi_i(\boldsymbol{f} \cdot \boldsymbol{g}) \in \hat{\mathcal{S}}_{(r+s)p^i}$. If further $r = s$, then $\pi_i(\boldsymbol{f} + \boldsymbol{g}) \in \hat{\mathcal{S}}_{rp^i}$.*

We now can prove the theorem:

Proof of Theorem 12.2. We again use induction to prove the theorem. Assume that, for $i < n$, we have that $F_i \in \hat{\mathcal{S}}_{p^i}$, $G_i \in \hat{\mathcal{S}}_0$, $a_i \in \mathcal{S}_{-2p^i}$ and $b_i \in \mathcal{S}_{-p^i}$ and shall to prove that the algorithm, when choosing $b_n = 0 \in \mathcal{S}_{-p^n}$, gives that $a_n \in \hat{\mathcal{S}}_{-2p^n}$, $F_n \in \hat{\mathcal{S}}_{p^n}$, and $G_n \in \hat{\mathcal{S}}_0$. Of course, since $a_n \in \mathbb{F}_p(a, b)$, this means that $a_n \in \mathcal{S}_{-2p^n}$.

By Lemma 12.3, we have that the omitted terms in Eq. (8.1) are all in $\hat{\mathcal{S}}_0$. Also note that since $\mathfrak{h}$ is the coefficient of x^{p-1} in $((1-y^2)(b^2-ay^2))^{(p-1)/2}$, we have that $\mathrm{wgt}(\mathfrak{h}) = -(p-1)$. Then, we can check that the terms from F_n and G_n coming from the formal integral of the formulas given by Theorem 6.2 have weight $-p^n$ and 0, respectively.

Note also that Lemma 12.3 implies that if $\boldsymbol{t} \in \hat{\mathcal{S}}_r$, then $1/\boldsymbol{t} \in \hat{\mathcal{S}}_{-r}$. Therefore, since the $(n+1)$-st coordinate of $\tau^*(1/\boldsymbol{x})$ is of them form

$$\frac{-x_0^{(n-1)p^n} F_n + \cdots}{x_0^{(n+1)p^n}},$$

where by the induction hypothesis the omitted terms have weight np^n, we have that the terms from F_n that need to cancel with the omitted terms (i.e., the ones on x_0^i for $i \geq 2p^{n-1}$, as described in the algorithm) must also be in $\hat{\mathcal{S}}_{p^n}$. Note that this makes $\mathrm{wgt}(c_i) = p^n - ip$, and since in this case we have $d_i = b^{p^n - ip} c_i$ (since we take $b_i = 0$ for $i \geq 1$), we get $\mathrm{wgt}(d_i) = 0$.

Now suppose we have found a solution for the unknowns, i.e., for a_n and the c_i's for $i < 2p^{n-1}$, odd. Since we have that all b_i's are 0, we have that all of these solutions are universal, and therefore their denominators can be taken as powers of $\Delta\mathfrak{h}$, and hence homogeneous. So, we can break these solutions as

$$\begin{aligned} a_n &= a_{n,0} + a_{n,1}, \\ c_i &= c_{i,0} + c_{i,1}, \text{ for } i < 2p^{n-1}, \text{ odd,} \end{aligned}$$

where

$$\begin{aligned} a_{n,0} \in \mathcal{S}_{-2p^n} &\text{ and no term of } a_{n,1} \text{ is in } \mathcal{S}_{-2p^n}, \\ c_{i,0} \in \mathcal{S}_{p^n - ip} &\text{ and no term of } c_{i,1} \text{ is in } \mathcal{S}_{p^n - ip}. \end{aligned}$$

Hence, we can rewrite Eq. (8.1) as

$$2(b^{2p^n} - a^{p^n} y_0^{2p^n}) x_0^{p^n} \left(\sum_{\substack{i<2p^{n-1} \\ i \text{ odd}}} (c_{i,0} + c_{i,1}) x_0^{ip} \right) \\ + 2(1 - a^{p^n} x_0^{2p^n}) y_0^{p^n} \left(\sum_{\substack{i<2p^{n-1} \\ i \text{ odd}}} b^{p^n - ip} (c_{i,0} + c_{i,1}) x_0^{ip} \right) - (a_{n,0} + a_{n,1}) x_0^{2p^n} y_0^{2p^n} = \cdots ,$$

where all the omitted terms were previously known and are homogeneous of weight 0. Since the weights have to balance, we must have that

$$2(b^{2p^n} - a^{p^n} y_0^{2p^n}) x_0^{p^n} \left(\sum_{\substack{i<2p^{n-1} \\ i \text{ odd}}} c_{i,0} x_0^{ip} \right) \\ + 2(1 - a^{p^n} x_0^{2p^n}) y_0^{p^n} \left(\sum_{\substack{i<2p^{n-1} \\ i \text{ odd}}} b^{p^n - ip} c_{i,0} x_0^{ip} \right) - a_{n,0} x_0^{2p^n} y_0^{2p^n} = \cdots ,$$

with the same omitted terms as above, and

$$2(b^{2p^n} - a^{p^n} y_0^{2p^n}) x_0^{p^n} \left(\sum_{\substack{i<2p^{n-1} \\ i \text{ odd}}} c_{i,1} x_0^{ip} \right) \\ + 2(1 - a^{p^n} x_0^{2p^n}) y_0^{p^n} \left(\sum_{\substack{i<2p^{n-1} \\ i \text{ odd}}} b_0^{p^n - ip} c_{i,1} x_0^{ip} \right) - a_{n,1} x_0^{2p^n} y_0^{2p^n} = 0.$$

But this means that $a_{n,0}$ and the $c_{i,0}$'s also give a solution. But since the solution is unique, we must have that $a_{n,1} = 0$ and the $c_{i,1} = 0$ for all $i < 2p^{n-1}$ odd. Thus, we have that $a_n \in \mathcal{S}_{-2p^n}$ and $c_i \in \mathcal{S}_{p^n - ip}$, and hence $F_i \in \hat{\mathcal{S}}_{p^n}$ and $G_i \in \hat{\mathcal{S}}_0$. □

Note that all other possible formulas that are modular of the corresponding weight can be obtained for the $(n+1)$-st coordinate with an isomorphisms given by $\boldsymbol{\lambda} = (1, 0, 0, \ldots, \lambda_n)$, where $\lambda_n \in \mathcal{S}_0$, and if we want the formulas to remain universal, we also need $\lambda_n \in \mathbb{U}$.

Acknowledgments. Computations mentioned in the text were done with MAGMA.

References

[1] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted Edwards curves. In *Progress in cryptology—AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Comput. Sci.*, pages 389–405. Springer, Berlin, 2008.

[2] D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In *Advances in cryptology—ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Comput. Sci.*, pages 29–50. Springer, Berlin, 2007.

[3] A. Buium. Geometry of p-jets. *Duke Math. Journal*, 82:349–367, 1996.

[4] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenköper. *Abh. Math. Sem. Univ. Hamburg*, 14:197–272, 1941.

[5] H. M. Edwards. A normal form for elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 44(3):393–422, 2007.

[6] L. R. A. Finotti. Degrees of the elliptic Teichmüller lift. *J. Number Theory*, 95(2):123–141, 2002.

[7] L. R. A. Finotti. Minimal degree liftings of hyperelliptic curves. *J. Math. Sci. Univ. Tokyo*, 11(1):1–47, 2004.

[8] L. R. A. Finotti. Lifting the j-invariant: Questions of Mazur and Tate. *J. Number Theory*, 130(3):620 – 638, 2010.

[9] L. R. A. Finotti. Computations with Witt vectors and the Greenberg transform. *Int. J. Number Theory*, 10(6):1431–1458, 2014.

[10] L. R. A Finotti. Weierstrass coefficients of the canonical lifting. *Int. J. Number Theory*, 16(2):397–422, 2020.

[11] M. J. Greenberg. Schemata over local rings. *Ann. of Math. (2)*, 73:624–648, 1961.

[12] S. Lang. On quasi algebraic closure. *Ann. of Math. (2)*, 55:373–390, 1952.

[13] F. Loeser and J. Sebag. Motivic integration on smooth rigid varieties and invariants of degenerations. *Duke Math. J.*, 119(2):315–344, 2003.

[14] J. Lubin, J-P. Serre, and J. Tate. Elliptic curves and formal groups. *Proc. of Woods Hole summer institute in algebraic geometry*, 1964. Unpublished. Available at `http://www.ma.utexas.edu/users/voloch/lst.html`.

[15] B. Poonen. Computing torsion points on curves. *Experiment. Math.*, 10(3):449–465, 2001.

[16] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[17] J. F. Voloch. Torsion points of $y^2 = x^6 + 1$. *unpublished manuscript*, 1997. available at `http://www.ma.utexas.edu/users/voloch/oldpreprint.html`.

[18] J. F. Voloch and J. L. Walker. Euclidean weights of codes from elliptic curves over rings. *Trans. Amer. Math. Soc.*, 352(11):5063–5076, 2000.

Department of Mathematics, University of Tennessee, Knoxville, TN, 37996

Email address: wbitting@vols.utk.edu

URL: https://sites.google.com/vols.utk.edu/wcb-personal/

Department of Mathematics, University of Tennessee, Knoxville, TN, 37996

Email address: lfinotti@utk.edu

URL: www.math.utk.edu/~finotti