MINIMAL DEGREE LIFTINGS OF EDWARDS CURVES

LIAM BITTING AND LUÍS R. A. FINOTTI

Abstract. Voloch and Walker used liftings of elliptic curves to create error-correcting codes, for which lifting of points with smaller degrees for their coordinate functions give better parameters. Thus, one might be interested in constructing liftings with minimal possible degrees. Here we study liftings of twisted Edwards curve with minimal degrees. We prove that up to the second coordinate these minimal degrees are given by the canonical lifting and elliptic Teichmüller lift, give upper and lower bounds for the degrees of Edwards lifts, and prove that the lower bound can be achieved for the third coordinate.

1. Introduction

In [17], Voloch and Walker used canonical liftings of elliptic curves to construct error-correcting codes. They provided bounds for the parameters of the code, and these depend on the degrees of the associate lifting of points (the elliptic Teichmüller lift, in their case), which takes a point of the curve in characteristic $p > 0$ to a point on the canonical lifting, with smaller degrees giving better bounds. They proved that, modulo p^2, the elliptic Teichmüller lift provides the minimal degrees among all other possible lifts of points, and thus was the optimal choice for the construction.

Voloch then asked the second author if it would be the case that the elliptic Teichmüller would give minimal degrees also modulo higher powers of the characteristic, but in [8] (for characteristic $p > 2$) and [9] (for characteristic $p = 2$), the second author proved that this is not the case and thus introduced *minimal degree lifts*, which would therefore give better bounds for the codes obtained than the elliptic Teichmüller lift. The notion was also extended to *hyperelliptic curves*. In the latter reference, examples of binary error-correcting

2010 *Mathematics Subject Classification.* Primary 11G07; Secondary 11F03.
Key words and phrases. Edwards curves, canonical lifting, elliptic Teichmüller lift.

codes were constructed, illustrating that the method can yield good codes. In [12], J. Groves used minimal degree liftings of elliptic and hyperelliptic curves in characteristic $p > 2$ to construct non-binary error-correcting codes.

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 yield better results than the more usual Weierstrass form.

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. For the sake of simplicity we will here refer to twisted Edwards curves simply as Edwards curves, as these will be our sole focus.

In [3] the authors describe the construction of the canonical lifting and elliptic Teichmüller lift for Edwards curves, and our goal here is to study their minimal degree liftings, similarly to what was done in [8] for elliptic curves (given by Weierstrass equations). In particular, we prove that again the canonical lifting and elliptic Teichmüller lift give minimal degrees for the second coordinates (Theorem 5.1), we provide upper and lower bounds for these degrees of the coordinate functions for these lifts (Theorems 6.4 and 6.6, respectively), conditions necessary to achieve the lower bounds (in Theorem 6.6), and prove that the lower bounds can be achieved modulo p^3 (Theorem 8.1).

We now give a short description of the following sections. In Section 2 we give the precise definition of twisted Edwards curves and a review a few of their basic properties. In Section 3 we give the definition of the canonical lift and summarize the results about canonical liftings of Edwards curves from [3]. In Section 4 we define the Greenberg transform of curves over Witt vectors and give a basic description of its coordinates. In Section 5 we prove the result mentioned above that the elliptic Teichmüller lift has minimal possible degrees for the second coordinates. In Section 6 we give precise definitions of Edwards lifts, minimal and absolute minimal degree lifts, and find upper and lower bounds for minimal and absolute minimal degree lifts. In Section 7 we provide lemmas necessary for the proof of the next main result, which is presented on Section 8, namely that we can achieve the lower bound from Section 6 for the third coordinate.

2. Edwards Curves

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

Let $\Bbbk$ be a perfect field of characteristic $p > 2$. A *twisted Edwards curves* is a projective algebraic curve given by an equation of the form

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

(Plain *Edward curves* have $b = 1$, but this form 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

$$E_{a,b}/\Bbbk: \ b^2x^2 + y^2 = 1 + ax^2y^2. \tag{2.1}$$

The discriminant, which is assumed to be non-zero, is given by $\Delta \stackrel{\text{def}}{=} ab^2(a - b^2)$, and the corresponding *j-invariant* is given by

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

Recall that the projective model of $E_{a,b}$ above is given by

$$b^2X_1^2 + X_2^2 = X_0^2 + aX_3^2,$$
$$X_0X_3 = X_1X_2,$$

where $(x, y) \mapsto [1, x, y, xy]$, and thus $E_{a,b}$ has 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):

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

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

Furthermore, we have that

$$\mathrm{ord}_{\mathcal{O}^{\pm}}(x) = 0, \quad \mathrm{ord}_{\mathcal{O}^{\pm}}(y) = -1, \quad \mathrm{ord}_{\mathcal{Q}^{\pm}}(x) = -1, \quad \mathrm{ord}_{\mathcal{Q}^{\pm}}(y) = 0, \tag{2.2}$$

and

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

(Hence, since $(0, 1)$ is also on $E_{a,b}(\Bbbk)$, note that Edwards curves have at least four rational points.)

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

$$\kappa_0(x, y) \stackrel{\text{def}}{=} (-x, y), \quad \kappa_1(x, y) \stackrel{\text{def}}{=} (x, -y), \quad \kappa_2(x, y) \stackrel{\text{def}}{=} \left(\frac{y}{b}, bx\right). \tag{2.3}$$

These extend to the points at infinity as:

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

The group law (for affine points) is given by

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

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

Also,

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

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 y^{p-1} in $((1-y^2)(b^2-ay^2))^{(p-1)/2}$, or equivalently, the coefficient of x^{p-1} in $((b^2x^2-1)(ax^2-1))^{(p-1)/2}$.

Recall that $E_{a,b}$ is called *ordinary* if the p-torsion group of $E_{a,b}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and *supersingular* if it is isomorphic to 0, and the former occurs if and only we have $\mathfrak{h} \neq 0$.

Finally, we recall [3, Lemma 4.3]:

Lemma 2.1. *Let $f \in \Bbbk[E_{a,b}]$ (where $\Bbbk[E_{a,b}]$ denotes the affine coordinate ring of $E_{a,b}$). Then,*

$$f = f_1(x) + f_2(y) + yf_3(x) + xf_4(y),$$

for some $f_1, f_2, f_3, f_4 \in \Bbbk[t]$, with $f_2(0) = f_3(0) = f_4(0) = f_4'(0) = 0$. Moreover, this representation is unique in $\Bbbk[E_{a,b}]$.

We also have the following particular case:

Lemma 2.2. *Let $f \in \Bbbk[x, y]$. Then, there are $f_1, f_2 \in \Bbbk[t]$ such that*

$$f(x^2, y^2) = f_1(x^2) + f_2(y^2)$$

in $\Bbbk[E_{a,b}]$, with $\deg_t f_1 \leq \deg_x f$, $\deg_t f_2 \leq \deg_y f$, and $f_2(0) = 0$. By Lemma 2.1, this presentation is unique.

Proof. The result follows by inductively proving the result for monomials x^2y^2, $x^{2r}y^2$ for $r \geq 2$, and $x^{2r}y^{2s}$ for $s \geq 2$. $\square$

As an immediate consequence we have:

Proposition 2.3. *Let*

$$L(i,j) \stackrel{\text{def}}{=} \left\{ f(x^2, y^2) : f \in \Bbbk[x, y],\ \deg_x f \leq i,\ \deg_y f \leq j \right\} \subseteq \Bbbk[E_{a,b}].$$

Then, $L(i, j)$ is a $\Bbbk$-subspace of $\Bbbk[E_{a,b}]$ with $\dim_{\Bbbk} L(i, j) = i + j + 1$.

We also shall need the following result in Section 6:

Proposition 2.4. *Let $A \in L(i,j) \setminus L(i,j-1)$, $B \in L(m,n) \setminus L(m-1,n)$, and $C \in L(d,e)$, such that $(A,B) = (A) \cap (B)$, and let $r \stackrel{\text{def}}{=} \max\{d, m+i\}$, $s \stackrel{\text{def}}{=} \max\{e, n+j\}$. Then, there exists $u \in L(r-i,n)$ and $v \in L(i,s-n)$ such that*

$$Au + Bv = C.$$

Moreover, if $\hat{u} \in L(r-i,n)$ and $\hat{v} \in L(i,s-n)$ also give us $A\hat{u} + B\hat{v} = C$, then there is some $\lambda \in \Bbbk$ such that $\hat{u} = u + \lambda B$ and $\hat{v} = v - \lambda A$.

Proof. Let $\psi : L(r-i,n) \oplus L(i,s-n) \to L(r,s)$ defined as $\psi(u,v) = Au + Bv$. Thus, ψ is a linear transformation, and since $(A,B) = (A) \cap (B)$, we must have that $(u,v) \in \ker\psi$ if and only if $u = Bw$ and $v = -Aw$ for some $w \in \Bbbk[E_{a,b}]$. Note that since A, B, u, and v all only involve even powers, then so does w.

Using Lemma 2.2, let then

$$\begin{aligned} -A &= f_1(x^2) + f_2(y^2), \\ B &= g_1(x^2) + g_2(y^2), \\ w &= h_1(x^2) + h_2(y^2), \end{aligned}$$

which gives

$$\begin{aligned} u &= g_1(x^2)h_1(x^2) + g_1(x^2)h_2(y^2) + g_2(y^2)h_1(x^2) + g_2(y^2)h_2(y^2), \\ v &= f_1(x^2)h_1(x^2) + f_1(x^2)h_2(y^2) + f_2(y^2)h_1(x^2) + f_2(y^2)h_2(y^2). \end{aligned}$$

Then, $2n \geq \deg_y u = \deg_y g_2(y^2) + \deg_y h_2(y^2) = 2n + \deg_x h_2(y^2)$, and hence $h_2 \in \Bbbk$. Similarly, we have that $2i \geq \deg_x v = \deg_x f_1(x^2) + \deg_x h_1(x^2) = 2i + \deg_y h_1(x^2)$, and hence $h_1 \in \Bbbk$, and thus $w \in \Bbbk$.

Therefore, we have that $\ker\psi = \operatorname{span}\{(B,-A)\}$, and hence

$$\begin{aligned} \dim_\Bbbk \psi(L(r-i,n) \oplus L(i,s-n)) &= \dim_\Bbbk L(r-i,n) + \dim_\Bbbk L(i,s-n) - 1 \\ &= r + s + 1 \\ &= \dim_\Bbbk L(r,s), \end{aligned}$$

and ψ must be surjective.

Finally, the last statement immediately follows from the fact that $\ker\psi = \operatorname{span}\{(B, -A)\}$.
$\square$

3. Canonical Liftings of Edwards Curves

Let $\Bbbk$ be a perfect field of characteristic $p > 0$. Associated to an *ordinary* Edwards curve $E_{a,b}$ over $\Bbbk$ (or more generally, any ordinary curve of genus 1 with a rational point), there exists a unique (up to isomorphisms) Edwards curve $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ over $\boldsymbol{W}(\Bbbk)$, the ring of Witt vectors over $\Bbbk$, called the *canonical lifting* of $E_{a,b}$, and a map $\tau : E_{a,b}(\overline{\Bbbk}) \to \boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{W}(\overline{\Bbbk}))$, i.e., a *lift of points*, called the *elliptic Teichmüller lift*, characterized by the following properties:

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

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

commutes. (In other words, there exists a *lifting* $\boldsymbol{\phi}$ *of the Frobenius* ϕ. See, e.g., [13] and [4].)

This concept of canonical lifting of elliptic curves was first introduced by Deuring in [5] and then generalized to Abelian varieties by Serre and Tate in [13]. 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 [15], coding theory, as in Voloch and Walker's [17], and counting torsion points of curves of genus $g \geq 2$, as in Poonen's [14] or Voloch's [16].

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

$$E_{a_0,b_0}/\Bbbk : \; b_0^2 x_0^2 + y_0^2 = 1 + a_0 x^2 y^2 \tag{3.1}$$

be an ordinary (twisted) Edwards curve,

$$\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}(\Bbbk) : \; \boldsymbol{b}^2 \boldsymbol{x}^2 + \boldsymbol{y}^2 = 1 + \boldsymbol{a}\boldsymbol{x}^2 \boldsymbol{y}^2 \tag{3.2}$$

be its canonical lifting, and $\tau : E_{a_0,b_0}(\Bbbk) \to \boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{W}(\Bbbk))$ 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 $\Bbbk(E_{a_0,b_0})$.

Here are the main results of [3]:

Theorem 3.1. *With the notation above:*

(1) *We have that $\tau(\mathcal{O}^{\pm}) = \boldsymbol{\mathcal{O}}^{\pm}$ and $\tau(\mathcal{Q}^{\pm}) = \boldsymbol{\mathcal{Q}}^{\pm}$. Moreover, if κ_i, for $i = 0, 1, 2$, represent both the involutions of E_{a_0,b_0} and $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ (as in Eq. (2.3)), then we have that $\kappa_i \circ \tau = \tau \circ \kappa_i$. In particular, we have*

$$(x_0, F_1, F_2, \ldots) = \frac{1}{\boldsymbol{b}}(b_0 x_0, G_1(b_0 x_0), G_2(b_0 x_0), \ldots),$$
$$(y_0, G_1, G_2, \ldots) = \boldsymbol{b}(y_0/b_0, F_1(y_0/b_0), F_2(y_0/b_0), \ldots).$$

(2) *The functions F_i and G_i can be taken to be* odd *polynomials in $\Bbbk[x_0]$ and $\Bbbk[y_0]$, respectively.*

(3) *For all $n \geq 1$, we have*

$$\deg_{x_0} F_i = \deg_{y_0} G_i = (n+1)p^n - np^{n-1},$$

and

$$\frac{\mathrm{d}F_n}{\mathrm{d}x_0} = \mathfrak{h}^{(p^n-1)/(p-1)} (b_0^2 x_0^2 - 1)^{(p^n-1)/2} (a_0 x_0^2 - 1)^{(p^n-1)/2} - \sum_{k=0}^{n-1} F_k^{p^{n-k}-1} \frac{\mathrm{d}F_k}{\mathrm{d}x_0},$$
$$\frac{\mathrm{d}G_n}{\mathrm{d}y_0} = \mathfrak{h}^{(p^n-1)/(p-1)} (b_0^2 - a y_0^2)^{(p^n-1)/2} (1 - y_0^2)^{(p^n-1)/2} - \sum_{k=0}^{n-1} G_k^{p^{n-k}-1} \frac{\mathrm{d}G_k}{\mathrm{d}y_0}.$$

(Remember that $\mathfrak{h}$ denotes the Hasse invariant of $E_{a,b}$.)

4. The Greenberg Transform

It is often convenient to use the *Greenberg transform* when dealing with varieties over rings of Witt vectors, so here we review its definition and basic properties.

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

Definition 4.1. For $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\mathbf{x}, \mathbf{y}]$, we refer to $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}(R)$ 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.

In particular, E and $\boldsymbol{E}$ are Edwards curves, as in Eqs. (3.1) and (3.2), then the $(n+1)$-nth equation of $G(E)$ is given by

$$2(b_0^{p^n} - a_0^{p^n} y_0^{2p^n}) x_0^{p^n} x_n + 2(1 - a_0^{p^n} x_0^{2p^n}) y_0^{p^n} y_n + b_n x_0^{2p^n} - a_n x_0^{2p^n} y_0^{2p^n} = \cdots , \tag{4.1}$$

where no omitted term involves a_n, b_n, x_n, or y_n. Hence, if

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

is a lift of points, then

$$2(b_0^{p^n} - a_0^{p^n} y_0^{2p^n}) x_0^{p^n} F_n + 2(1 - a_0^{p^n} x_0^{2p^n}) y_0^{p^n} G_n + b_n x_0^{2p^n} - a_n x_0^{2p^n} y_0^{2p^n} = \cdots \tag{4.2}$$

(in the affine coordinate ring of the curve). See [11] for more general expressions for the coordinates of the Greenberg transform.

5. Minimal Degree Liftings Modulo p^2

Let, again, $\Bbbk$ be a field of characteristic $p > 0$. Voloch and Walker proved in [17, Proposition 4.2] that, when E is an ordinary elliptic curve *in Weierstrass form*, $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$ is an elliptic curve that reduces to E modulo p, and

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

is a lifting of points between the *affine parts* of the curves, then if the orders of poles at infinity of F_1 and G_1 are less than $3p$ and $4p$, respectively, then $\boldsymbol{E}$ is the canonical lifting of E and ν is the elliptic Teichmüller lift. This implies that the elliptic Teichmüller lift has minimal degrees (for the second coordinate functions) among all lifts of points, and that this minimal degree only occurs when $\boldsymbol{E}$ is the canonical lifting. We have the same result for Edwards curves:

Theorem 5.1. *Let $\Bbbk$ be a field of characteristic $p > 2$, $E_{a_0,b_0}/\Bbbk$ be an ordinary Edwards curve, $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}_2(\Bbbk)$ (remembering the $\boldsymbol{W}_r(\Bbbk)$ denotes the ring of Witt vectors of length r) be an Edwards curve that reduces to E_{a_0,b_0} module p, and $\nu : E_{a_0,b_0}(\overline{\Bbbk}) \to \boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{W}_2(\overline{\Bbbk}))$ be a lift of points given by $\nu(x_0, y_0) = ((x_0 F_1), (y_0, G_1))$. If $\operatorname{ord}_{\mathcal{O}^\pm}(F_1) < 2p$ and $\operatorname{ord}_{\mathcal{O}^\pm}(G_1) < 2p$, then $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ is the canonical lifting of $E_{a,b}$ (modulo p^2) and ν is the elliptic Teichmüller lift. In particular, this holds if F_1 and G_1 are polynomials of degree less than $2p$.*

Remark. Note that by Theorem 3.1, the Teichmüller lift is such that $\deg_{x_0} F_1 = \deg_{y_0} G_1 = 2p-1$.

Proof of Theorem 5.1. By [3, Corollary 7.2], it suffices to show that

$$\left(\frac{1}{(x_0, F_1)}\right)(\mathcal{Q}^{\pm}) = \left(\frac{1}{(x_0, G_1)}\right)(\mathcal{O}^{\pm}) = 0.$$

The result follows since

$$\frac{1}{(z_0, z_1)} = \left(\frac{1}{z_0}, -\frac{z_1}{z_0^{2p}}\right)$$

and

$$\operatorname{ord}_{\mathcal{Q}^{\pm}}(x_0) = -1, \quad \operatorname{ord}_{\mathcal{O}^{\pm}}(y_0) = -1.$$

$\square$

Thus, we can see that *if the curve is ordinary*, the elliptic Teichmüller lift is the lift of points with minimal degrees. In fact, supersingular curves always have larger degrees, but before we can prove it, we need the following lemma:

Lemma 5.2. *Let*

$$f(x_0, y_0) \stackrel{\text{def}}{=} b_0^2 x_0^2 + y_0^2 - \left(1 + a_0 x_0^2 y_0^2\right),$$

with $a_0, b_0 \neq 0$, and suppose we have

$$\left[(1-y_0^2)(b_0^2 - a_0 y_0^2)\right]^k h_1(x_0) = \left[(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1)\right]^k h_2(y_0) + g \cdot f \tag{5.1}$$

(in $\Bbbk[x_0, y_0]$) for some $k \geq 1$ and $g \in \Bbbk[x_0, y_0]$, $h_1 \in \Bbbk[x_0]$, $h_2 \in \Bbbk[y_0]$, and with $\deg_{x_0} h_1, \deg_{y_0} h_2 \leq 4k$*. Then,*

$$\left[(1-y_0^2)(b_0^2 - a_0 y_0^2)\right]^k \mid h_2(y_0),$$
$$\left[(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1)\right]^k \mid h_1(x_0).$$

In particular, we have $\deg_{x_0} h_1(x_0) = \deg_{y_0} h_2(y_0) = 4k$*.*

Proof. We prove by induction on k. The result is trivial if $k = 0$.

Evaluating Eq. (5.1) at $y_0 = \pm 1$, we get

$$\left[(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1)\right]^k h_2(\pm 1) = -g(x_0, \pm 1) \cdot (b_0^2 - a_0) x_0^2.$$

Since the right-hand side has no constant term, we must have that $h_2(\pm 1) = 0$, i.e., $(1 - y_0^2) \mid h_2(y_0)$.

Now, evaluating Eq. (5.1) at $y_0 = \beta \stackrel{\text{def}}{=} \pm b_0/a_0^{1/2}$ (extending $\Bbbk$, if necessary), and evaluating at $y_0 = \beta$, we get

$$\left[(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1)\right]^k h_2(\beta) = -g(x_0, \beta) \cdot (\beta^2 - 1).$$

This implies that if $h_2(\beta) \neq 0$, then we must have $\deg_{x_0} g \geq \deg_{x_0} g(x_0, \beta) = 4k$. But then, the degree on x_0 of the left side of Eq. (5.1) is less than or equal to $4k$, while the degree of the right side is at least $4k + 2$, a contradiction. Hence, we must have that $h_2(\beta) = 0$ and $(b_0^2 - a_0 y_0^2) \mid h_2$.

Thus, we have that $(1 - y_0^2)(b_0^2 - a_0 y_0^2) \mid h_2$, and a similar argument yields that $(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1) \mid h_1$. These also imply that $(1 - y_0^2)(b_0^2 - a_0 y_0^2)(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1) \mid g$. Hence we can divide Eq. (5.1) by $(1 - y_0^2)(b_0^2 - a_0 y_0^2)(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1)$, and the induction hypothesis yields the result. □

Theorem 5.3. *Let $E_{a_0,b_0}/\Bbbk$ be a supersingular curve, $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}_2(\Bbbk)$ be a lifting, and $\nu(x_0, y_0) = ((x_0 F_1), (y_0, G_1))$ a lift of points with $F_1 \in \Bbbk[x_0]$ and $G_1 \in \Bbbk[y_0]$. Then $\deg_{x_0} F_1, \deg_{y_0} G_1 > 2p - 1$.*

Proof. Let

$$\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}_2(\Bbbk) \ : \ \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\text{def}}{=} (b_0, b_1)^2 \boldsymbol{x}^2 + \boldsymbol{y}^2 - \left(1 + (a_0, a_1)\boldsymbol{x}^2 \boldsymbol{y}^2\right) = 0,$$

and $f(x_0, y_0) \stackrel{\text{def}}{=} b_0^2 x_0^2 + y_0^2 - (1 + a x_0^2 y_0^2)$, the reduction modulo p of $\boldsymbol{f}$, which gives the equation for E_{a_0,b_0}. Since ν is a lift of points, we must have that $\nu^* \boldsymbol{f} = 0$ in the function field $\Bbbk(E_{a_0,b_0})$. The second coordinate of this expression gives:

$$f_{x_0}^p F_1 + f_{y_0}^p G_1 + b_1 x_0^{2p} + a_1 x_0^{2p} y_0^{2p} + \psi_1(f) = 0,$$

where f_{x_0} and f_{y_0} are partial derivatives of f and $\psi_1(f)$ is as given in [10].

Note that although the definition of $\psi_1(f)$ is not straight-forward, its partial derivatives are rather simple:

$$\frac{\partial}{\partial x_0}\psi_1(f) = x_0^{p-1} f_{x_0}^p - f_{x_0} f^{p-1} = x_0^{p-1} f_{x_0}^p,$$
$$\frac{\partial}{\partial y_0}\psi_1(f) = y_0^{p-1} f_{y_0}^p - f_{y_0} f^{p-1} = y_0^{p-1} f_{y_0}^p.$$

Thus, taking the differential of the equation above, we get

$$f_{x_0}^p F_1' \mathrm{d}x_0 + f_{y_0}^p G_1' \mathrm{d}y_0 + x_0^{p-1} f_{x_0}^p \mathrm{d}x_0 + y_0^{p-1} f_{y_0}^p \mathrm{d}y_0 = 0.$$

Since $f_{x_0}\mathrm{d}x_0 = -f_{y_0}\mathrm{d}y_0$ (and $f_{x_0} \neq 0$), the above equation simplifies to

$$f_{x_0}^{p-1}\left(F_1' + x_0^{p-1}\right) = f_{y_0}^{p-1}\left(G_1' + y_0^{p-1}\right).$$

Note that since $x_0^2(b_0^2 - a_0 y_0^2) = 1 - y_0^2$ in $\Bbbk(E_{a_0,b_0})$, we have that

$$f_{x_0}^{p-1} = \left[4(1-y_0^2)(b_0^2 - a_0 y_0^2)\right]^{(p-1)/2},$$

and similarly

$$f_{y_0}^{p-1} = \left[4(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1)\right]^{(p-1)/2}.$$

Thus, we obtain

$$\left[(1-y_0^2)(b_0^2 - a_0 y_0^2)\right]^{(p-1)/2}\left(F_1' + x_0^{p-1}\right) = \\ \left[(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1)\right]^{(p-1)/2}\left(G_1' + y_0^{p-1}\right) + g \cdot f$$

in $\Bbbk[x_0, y_0]$, for some $g \in \Bbbk[x_0, y_0]$.

Now, if we assume that $\deg_{x_0} F_1, \deg_{y_0} G_1 \leq 2p-1$, and hence $\deg_{x_0} F_1' + x_0^{p-1}, \deg_{y_0} G_1' + y_0^{p-1} \leq 2p-2$, then we can apply Lemma 5.2, which gives us that $\left[(1-y_0^2)(b_0^2 - a_0 y_0^2)\right]^{(p-1)/2} \mid \left(G_1' + y_0^{p-1}\right)$ and $\left[(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1)\right]^{(p-1)/2} \mid \left(F_1' + x_0^{p-1}\right)$. But this implies that $\deg_{x_0} F_1, \deg_{y_0} G_1 \geq 2p-1$, and since then the equality must occur, we have that

$$F_1' = k_1 \cdot \left[(b_0^2 x_0^2 - 1)(a_0 x_0^2 - 1)\right]^{(p-1)/2} - x_0^{p-1},$$
$$G_1' = k_2 \cdot \left[(1-y_0^2)(b_0^2 - a_0 y_0^2)\right]^{(p-1)/2} - y_0^{p-1},$$

for some $k_1, k_2 \in \mathbb{k}^\times$. But this is impossible since the Hasse invariant is zero by assumption, and hence the right sides have terms in x_0^{p-1} and y_0^{p-1}, respectively, and therefore cannot be derivatives. □

Thus, we have that among all Edwards curves, to obtain lifts of points having the smallest possible degrees for the second coordinate, we must start with an ordinary Edwards curve, take its lifting to be the corresponding canonical lifting, and take the lift of points to be the elliptic Teichmüller lift. If any of these three conditions is not satisfied, then we necessarily have larger degrees.

6. Minimal Degee Liftings

As previously observed, Voloch and Walker used liftings of curves to construct error-correcting codes, and smaller degrees yield better bounds for the parameters of the resulting codes. Therefore, it makes sense to look for minimal degrees, which motivates the definitions introduced below.

We will have two difference scenarios:

(1) We start with Edwards curves $E_{a_0,b_0}/\mathbb{k}$ and $\boldsymbol{E_{a,b}}/\boldsymbol{W}(\mathbb{k})$, with the latter reducing to the former modulo p, and find a lift of points $\nu : E_{a_0,b_0}(\overline{\mathbb{k}}) \to \boldsymbol{E_{a,b}}(\boldsymbol{W}(\overline{\mathbb{k}}))$ with coordinate functions having degrees as small as possible. (We will refer to these as *minimal degree lifts*, properly defined in Definition 6.2 below.)

(2) We start with only an Edwards curve $E_{a_0,b_0}/\mathbb{k}$, and find both a lift $\boldsymbol{E_{a,b}}$ to $\boldsymbol{W}(\mathbb{k})$ and a lift of points $\nu : E_{a_0,b_0}(\overline{\mathbb{k}}) \to \boldsymbol{E_{a,b}}(\boldsymbol{W}(\overline{\mathbb{k}}))$ with coordinate functions having degrees as small as possible. (We will refer to these as *absolute minimal degree lifts*, properly defined in Definition 6.3 below.)

After imposing some restrictions on the kind of lift of points ν we will study, in this section we will also find upper bounds (in Theorem 6.4) and lower bounds (in Theorem 6.6) for these lifts of points. (In Section 8 we investigate some cases in which the lower bound can be achieved.)

Throughout this section, we let E_{a_0,b_0} be a twisted Edwards Curve over a perfect field $\mathbb{k}$ of characteristic $p \geq 3$ given by

$$E_{a_0,b_0}/\mathbb{k} : \; b_0^2 x_0^2 + y_0^2 = 1 + a_0 x^2 y^2 \tag{6.1}$$

and $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ be a lifting of E_{a_0,b_0} given by

$$\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}(\mathbb{k}) : \; \boldsymbol{b}^2\boldsymbol{x}^2 + \boldsymbol{y}^2 = 1 + \boldsymbol{a}\boldsymbol{x}^2\boldsymbol{y}^2,$$

(and thus $\boldsymbol{a}$ and $\boldsymbol{b}$ reduce to a_0 and b_0 modulo p, respectively). We shall also denote by U and $\boldsymbol{U}$ the *affine parts* of E_{a_0,b_0} and $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ respectively. Finally, we let $\nu : U(\bar{\mathbb{k}}) \to \boldsymbol{U}(\boldsymbol{W}(\bar{\mathbb{k}}))$ be a lifting of points (between the affine parts only) given by

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

with $F_i, G_i \in \mathbb{k}(E_{a_0,b_0})$.

Note that requiring that the image of $U(\bar{\mathbb{k}})$ via ν is contained $\boldsymbol{U}(\boldsymbol{W}(\bar{\mathbb{k}}))$ is not sufficient to guarantee that the coordinate functions are polynomial, as denominators involving, for instance, $b_0^2 - a_0 y_0^2$ could still appear. But, although we will mostly consider the affine parts of the curves, we will consider lifts of points that have properties that allow them to perhaps be extended to the points at infinity. Moreover, we will require that ν also has the extra properties of the elliptic Teichmüller lift τ, namely, that they commute with the involutions κ_i, for $i = 1, 2, 3$.

By [3, Proposition 4.4], these requirements force ν to have a restricted form, quite similar to τ and motivates the following definition:

Definition 6.1. A lift of points ν as above is called an *Edwards lift* if $F_i \in \mathbb{k}[x_0]$, $G_i \in \mathbb{k}[y_0]$, both odd, and satisfying

$$\begin{aligned}(x_0, F_1, F_2, \ldots) &= \frac{1}{\boldsymbol{b}}(b_0 x_0, G_1(b_0 x_0), G_2(b_0 x_0), \ldots),\\ (y_0, G_1, G_2, \ldots) &= \boldsymbol{b}(y_0/b_0, F_1(y_0/b_0), F_2(y_0/b_0), \ldots).\end{aligned}$$

Hence we must have $\deg F_i = \deg G_i$.

Note that Edwards lifts do not necessarily extend to points at infinity. For that we would also need that

$$\nu^* \frac{1}{\boldsymbol{x}}(\mathcal{O}^{\pm}) = \pm \boldsymbol{a}^{1/2}, \qquad \nu^* \frac{1}{\boldsymbol{x}}(\mathcal{Q}^{\pm}) = 0,$$

$$\nu^* \frac{1}{\boldsymbol{y}}(\mathcal{O}^{\pm}) = \pm 0, \qquad \nu^* \frac{1}{\boldsymbol{y}}(\mathcal{Q}^{\pm}) = \frac{\boldsymbol{a}^{1/2}}{\boldsymbol{b}}.$$

We now give the precise definition of a *minimal degree lift (of points)*, which is done recursively:

Definition 6.2 (Minimal Degree Edwards Lift)**.** Let E_{a_0,b_0} and $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ be Edwards curves as above. A *minimal degree Edwards lift modulo* p^2 *from* E_{a_0,b_0} *to* $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}_2(\mathbb{k})$ is an Edwards lift

$$\nu(x_0, y_0) = ((x_0, F_1), (y_0, G_1))$$

where $\deg(F_1)$ and $\deg(G_1)$ are minimal.

Inductively, a *minimal degree Edwards lift modulo* p^{n+1} *from* E_{a_0,b_0} *to* $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}_{n+1}(\mathbb{k})$ is an Edwards lift

$$\nu(x_0, y_0) = ((x_0, F_1, \dots, F_n), (y_0, G_1, \dots, G_n))$$

whose reduction modulo p^n is a minimal degree lift modulo p^n and $\deg(F_n)$ and $\deg(G_n)$ are minimal.

Note that with these minimal degree liftings, the lifting $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ of E_{a_0,b_0} is *fixed*, and we look for lifting of points between these two curves with minimal degrees. The next definition deals with the case when we want to chose a lifting of E_{a_0,b_0} that yields minimal degrees among all possible liftings.

Definition 6.3 (Absolute Minimal Degree Curve)**.** Let E_{a_0,b_0} be as above. We define an *absolute minimal degree curve modulo* p^2 over E_{a_0,b_0} to be a curve $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}_2(\mathbb{k})$ that reduces to E_{a_0,b_0} modulo p satisfying the following property: if

$$\nu(x_0, y_0) = ((x_0, F_1), (y_0, G_1))$$

is a minimal degree Edwards lift from E_{a_0,b_0} to $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ and $\tilde{\boldsymbol{E}}_{\boldsymbol{a},\boldsymbol{b}}$ is any curve that reduces to E_{a_0,b_0} modulo p, then any minimal degree Edwards lift

$$\tilde{\nu}(x_0, y_0) = ((x_0, \tilde{F}_1), (y_0, \tilde{G}_1))$$

from E_{a_0,b_0} to $\tilde{\boldsymbol{E}}_{\boldsymbol{a},\boldsymbol{b}}$ satisfies $\deg F_1 \leq \deg \tilde{F}_1$ (and hence also $\deg G_1 \leq \deg \tilde{G}_1$). In this case we call ν an *absolute minimal degree lift (of points) modulo* p^2.

Inductively, an *absolute minimal degree curve modulo* p^{n+1} is a curve $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}_{n+1}(\mathbb{k})$ whose reduction modulo p^n is an absolute minimal degree curve modulo p^n over E_{a_0,b_0}, satisfying the following property: if

$$\nu(x_0, y_0) = ((x_0, F_1, \ldots, F_n), (y_0, G_1, \ldots, G_n))$$

is a minimal degree Edwards lift from E_{a_0,b_0} to $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ and $\tilde{\mathbf{E}}_{\boldsymbol{a},\boldsymbol{b}}/\boldsymbol{W}_{n+1}(\mathbb{k})$ is any curve whose reduction modulo p^n is equal to the reduction modulo p^n of $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$, then any minimal degree lift

$$\tilde{\nu}(x_0, y_0) = ((x_0, \tilde{F}_1, \ldots, \tilde{F}_n), (y_0, \tilde{G}_1, \ldots, \tilde{G}_n))$$

from E_{a_0,b_0} to $\tilde{\boldsymbol{E}}_{\boldsymbol{a},\boldsymbol{b}}$ is such that $\deg F_n \leq \deg \tilde{F}_n$ (and hence also $\deg G_n \leq \deg \tilde{G}_n$). In this case we call ν an *absolute minimal degree lift (of points) modulo* p^{n+1}.

We start by finding an upper bound for the degree of a minimal degree lifting (independent of the choice of the curve $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$):

Theorem 6.4. *Let E_{a_0,b_0} be an Edwards curve over a perfect field $\mathbb{k}$ of characteristic $p \geq 3$, U be the affine part of E_{a_0,b_0}, $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ be an Edwards curve over $\boldsymbol{W}(\mathbb{k})$ that reduces to E_{a_0,b_0} modulo p, and $\boldsymbol{U}$ be its affine part. Then there is an Edwards lifting of points $\nu : U \to \boldsymbol{U}$ given by*

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

such that for all n

$$\deg F_n, \deg G_n \leq (n+1)p^n + np^{n-1}.$$

To prove this, we first introduce some notation from [7] and [8].

Definition 6.5. Let $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation of the field K. For $e \geq 0$, define:

$$U_r(e) \stackrel{\text{def}}{=} \{\boldsymbol{s} = (s_0, s_1, \ldots) \in \boldsymbol{W}(K)^\times : v(s_n) \geq p^n(v(s_0) - ne), \text{ for } 0 \leq n \leq r\},$$

and $U(e) = \bigcap_{r \geq 1} U_r(e)$.

Lemma 2.2 of [8] shows that $U_r(e)$ and $U(e)$ are groups.

Proof of Theorem 6.4. Throughout we use the valuation $v := \mathrm{ord}_{\mathcal{Q}+}$, and hence $v(x_0) = -1$ and $v(y_0) = 0$.

Again we prove this by induction. By Theorem 5.1, the statement clearly holds for $n = 1$, so we assume $n \geq 2$. Consider the $(n+1)$-nth coordinate of the $\nu^* G(\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}})$, which, by Eq. 4.2, is given by:

$$2(b_0 - a_0 y_0^2)^{p^n} x_0^{p^n} F_n + 2(1 - a_0 x_0^2)^{p^n} y_0^{p^n} G_n + b_n x_0^{2p^n} - a_n x_0^{2p^n} y_0^{2p^n} = \cdots , \tag{6.2}$$

where we regard F_n and G_n as unknowns.

By the induction hypothesis we have that

$$(x_0, F_1, \ldots, F_n), (y_0, G_1, \ldots, G_n) \in U_{n-1}((p+1)/p),$$

and by [8, Lemma 3.2], we have that all the omitted terms have valuation greater than or equal to $p^n\,(-2 - n(p+1)/p)$, i.e., of degree in x_0 less than or equal to $(n+2)p^n + np^{n-1}$. A similar argument using $v \stackrel{\text{def}}{=} \mathrm{ord}_{\mathcal{O}+}$ instead gives the omitted terms have degree in y_0 less than or equal to $(n+2)p^n + np^{n-1}$.

Note since F_i and G_i are odd, [8, Lemma 5.1] tell us that the coordinates of

$$(x_0, F_1, F_2, \ldots)^2 \quad \text{and} \quad (y_0, G_1, G_2, \ldots)^2$$

only contain even powers of x_0 and y_0, and hence the same must be true for the omitted terms in Eq. (6.2) above.

Let now $F_n = x_0 u$ and $G_n = y_0 v$, regarding now u and v as unknown even polynomials in $\Bbbk[x_0]$ and $\Bbbk[y_0]$ respectively. (We will show that there are such F_n and G_n of form by finding u and v, so for now this is taken as an assumption.) Observing that

$$(b_0^2 - a_0 y_0^2) x_0^2 = (1 - y_0^2) \quad \text{and} \quad (1 - a_0 x_0^2) y_0^2 = (1 - b_0^2 x_0^2),$$

Eq. (6.2) above becomes

$$Au + Bv = C, \tag{6.3}$$

where

$$\begin{aligned} A &\stackrel{\text{def}}{=} 2(b_0^2 - a_0 y_0^2)^{p^n} x_0^{p^n+1} \\ &= 2(1-y_0^2)^{\frac{p^n+1}{2}} (b_0^2 - a_0 y_0^2)^{\frac{p^n-1}{2}}, \\ B &\stackrel{\text{def}}{=} 2(1 - a_0 x_0^2)^{p^n} y_0^{p^n+1} \\ &= 2(1-b_0^2 x_0^2)^{\frac{p^n+1}{2}} (1 - a_0 x_0^2)^{\frac{p^n-1}{2}}, \end{aligned}$$

and C be the omitted terms from Eq. (6.2). Then, we have that

$$\left(\frac{x_0^{p^n-1}}{2}\right) A + \left(\frac{y_0^{p^n-1}(b_0^2 - a_0 y_0^2)^{p^n}}{2(b_0^2 - a_0)^{p^n}}\right) B = \left(1 - y_0^2\right)^{p^n} + \left(y_0^2\right)^{p^n} = 1, \tag{6.4}$$

and thus $(A) \cap (B) = (AB)$. Therefore, by Proposition 2.4, we have that there are $u \in L((n+2)p^n + np^{n-1}, 0)$ and $v \in L(0, (n+2)p^n + np^{n-1})$ such that $Au + Bv = C$.

Now, let $A^* \stackrel{\text{def}}{=} 2(b_0^2 - a_0 y_0^2)^{p^n}$ and $B^* \stackrel{\text{def}}{=} 2(1 - a_0 x_0^2)^{p^n}$. Noting that $(A^*) \cap (B^*) = (A^* B^*)$ by Eq. (6.4) and since $A = x_0^{p^n+1} A^*$ and $B^* = y_0^{p^n+1} B^*$, Proposition 2.4 now gives us that there are $u^* \in L((n+2)p^n + np^{n-1}, 0)$ and $v^* \in L(0, (n+2)p^n + np^{n-1})$ such that $A^* u^* + B^* v^* = C$.

Since also $A^* x_0^{p^n+1} u + B^* y_0^{p^n+1} v = C$, by Proposition 2.4 we have that there is $\lambda \in \Bbbk$ such that

$$\begin{aligned} u^* &= x_0^{p^n+1} u + \lambda B^*, \\ v^* &= y_0^{p^n+1} v - \lambda A^*, \end{aligned}$$

and hence $(p^n+1) \deg_x u = \deg_x u^* \leq (n+2)p^n + np^{n-1}$, i.e., $\deg_x u \leq (n+1)p^n + np^{n-1} - 1$, and similarly, $\deg_y v \leq (n+1)p^n + np^{n-1} - 1$.

Hence, letting $F_n \stackrel{\text{def}}{=} x_0 \cdot u$ and $G_n \stackrel{\text{def}}{=} y_0 v$, we obtain the desired bounds.

On the other hand, at this point we cannot guarantee that these F_n and G_n give an Edwards lift, as the resulting lift of points might not commute with the involution κ_2. But, by the induction hypothesis

$$\begin{aligned} \frac{1}{\boldsymbol{b}} (b_0 x_0, G_1(b_0 x_0), \ldots, G_n(b_0 x_0)) &= (x_0, F_1(x_0), \ldots, F_{n-1}(x_0), H_n(x_0)) \\ \boldsymbol{b} (y_0/b_0, F_1(y_0/b_0), \ldots, F_n(y_0/b_0)) &= (y_0, G_1(y_0), \ldots, G_{n-1}(y_0), I_n(y_0)), \end{aligned}$$

for some polynomials H_n and I_n. By [8, Lemma 5.1] again, we have that these polynomials are also odd, and hence $H_n = x_0\hat{u}$, $I_n = y_0\hat{v}$, with $\hat{u}$ and $\hat{v}$ even polynomials in $\Bbbk[x_0]$ and $\Bbbk[y_0]$ respectively. Evaluating the equation of $\boldsymbol{E_{a,b}}$ at this pair of polynomials give us that $(\hat{u}, \hat{v})$ is another solution of Eq. (6.3), and by Proposition 2.4 we have that $\hat{u} = u + \lambda B$ and $\hat{v} = v - \lambda A$ for some $\lambda \in \Bbbk$.

Now, we try to modify our original u and v so that the resulting lift is an Edwards lift. Let $\tilde{u} \stackrel{\text{def}}{=} u + \frac{\lambda}{2}B$ and $\tilde{v} = v - \frac{\lambda}{2}A$. Then, $(\tilde{u}, \tilde{v})$ is another solution of Eq. (6.3) and thus $\tilde{F}_n \stackrel{\text{def}}{=} x_0\tilde{u} = F_n + \frac{\lambda}{2}x_0B$ and $\tilde{G}_n \stackrel{\text{def}}{=} y_0\tilde{v} = G_n - \frac{\lambda}{2}y_0A$ are odd polynomials that define another lift of same degrees. Then, observing that

$$\frac{1}{b_0^{p^n-1}}A(b_0x_0) = B(x_0), \quad \text{and} \quad b_0^{p^n-1}B\left(\frac{y_0}{b_0}\right) = A(y_0),$$

we get

$$\begin{aligned}
&\frac{1}{\boldsymbol{b}}\left(b_0x_0, G_1(b_0x_0), \dots, G_{n-1}(b_0x_0), \tilde{G}_n(b_0x_0)\right) \\
&\quad = \frac{1}{\boldsymbol{b}}\left(b_0x_0, G_1(b_0x_0), \dots, G_{n-1}(b_0x_0), G_n(b_0x_0) - \frac{\lambda}{2}b_0x_0A(b_0x_0)\right) \\
&\quad = \left(x_0, F_1(x_0), \dots, F_{n-1}(x_0), H_n(x_0) - \frac{1}{b_0^{p^n}}\frac{\lambda}{2}b_0x_0A(b_0x_0)\right) \\
&\quad = \left(x_0, F_1(x_0), \dots, F_{n-1}(x_0), H_n(x_0) - \frac{\lambda}{2}x_0B\right).
\end{aligned}$$

But

$$H_n - \frac{\lambda}{2}x_0B = x_0\hat{u} - \frac{\lambda}{2}x_0B = x_0\left(u + \lambda B\right) - \frac{\lambda}{2}x_0B = x_0\left(u + \frac{\lambda}{2}B\right) = x_0\tilde{u} = \tilde{F}_n,$$

and thus

$$\frac{1}{\boldsymbol{b}}\left(b_0x_0, G_1(b_0x_0), \dots, G_{n-1}(b_0x_0), \tilde{G}_n(b_0x_0)\right) = \left(x_0, F_1(x_0), \dots, F_{n-1}(x_0), \tilde{F}_n(x_0)\right).$$

A similar computation yields

$$\boldsymbol{b}\left(y_0/b_0, F_1(y_0/b_0), \dots, F_{n-1}(y_0/b_0), \tilde{F}_n(y_0/b_0)\right) = \left(y_0, G_1(y_0), \dots, G_{n-1}(y_0), \tilde{G}_n(y_0)\right),$$

and hence the lift of points

$$(x_0, y_0) \mapsto ((x_0, F_1, \dots, F_{n-1}, \tilde{F}_n), (y_0, G_1, \dots, G_{n-1}, \tilde{G}_n))$$

is an Edwards lift with the degrees bounded as in the statement. □

We can now give general lower bounds for the degrees of the coordinate functions of lifting of points for Edwards curves, that apply to Edwards lift, as well as a necessary condition to attain them in this case:

Theorem 6.6. *Let* $\nu((x_0,y_0)) = ((x_0,F_1,\dots,F_n),(y_0,G_1,\dots,G_n))$ *(for* $n\geq 1$*) be a lifting of points (not necessarily an Edwards lift) from the affine part* U *of an Edwards curve* E_{a_0,b_0} *to the affine part* $\boldsymbol{U}$ *of a lift* $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$*, where* $F_i \in k[x_0]$, $G_i\in k[y_0]$ *and*

$$\deg(F_i) = \deg(G_i) = 2p^i - 1$$

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

$$\frac{\mathrm{d}F_n}{\mathrm{d}x_0} = \mathfrak{h}^{-(p^n-1)/(p-1)}(b_0^2x_0^2-1)^{\frac{p^n-1}{2}}(a_0x_0^2-1)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} F_k^{p^{n-k}-1}\frac{\mathrm{d}F_k}{\mathrm{d}x_0},$$
$$\frac{\mathrm{d}G_n}{\mathrm{d}y_0} = \mathfrak{h}^{-(p^n-1)/(p-1)}(b_0^2-a_0y_0^2)^{\frac{p^n-1}{2}}(1-y_0^2)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} G_k^{p^{n-k}-1}\frac{\mathrm{d}G_k}{\mathrm{d}y_0}.$$

where $\mathfrak{h}$ *is the (necessarily non-zero) Hasse invariant of* E_{a_0,b_0}*.*

Proof. Firstly, as in [8, Theorem 4.1], we have that

$$(\boldsymbol{x},\boldsymbol{y}) \mapsto \left(\boldsymbol{x}^{p^n} + p\boldsymbol{F}_1^{p^{n-1}} + \cdots + p^n\boldsymbol{F}_n, \boldsymbol{y}^{p^n} + p\boldsymbol{G}_1^{p^{n-1}} + \cdots + p^n\boldsymbol{G}_n\right),$$

where $\boldsymbol{F}_i$ and $\boldsymbol{G}_i$ are lifts of F_i and G_i to $\boldsymbol{W}(\Bbbk)[\boldsymbol{x}]$ and $\boldsymbol{W}(\Bbbk)[\boldsymbol{y}]$ respectively, gives a lift of the p^n-th power Frobenius $\phi^n : U \to U^{\sigma^n}$, which we denote by $\boldsymbol{\phi}^n$.

Now let

$$\boldsymbol{\omega} \stackrel{\text{def}}{=} \frac{2\boldsymbol{y}\mathrm{d}\boldsymbol{x}}{\boldsymbol{b}^{2p^n}\boldsymbol{x}^2 - 1} = \frac{2\boldsymbol{x}\mathrm{d}\boldsymbol{y}}{1-\boldsymbol{y}^2}$$

be the invariant differential of $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$, and ω_0 be its reduction modulo p, i.e., the invariant differential of E_{a_0,b_0}. Then the reduction modulo p of $\left(\frac{1}{p^n}\boldsymbol{\phi}^n\right)^*(\boldsymbol{\omega}^{\sigma^n})$ is given by

$$\omega \stackrel{\text{def}}{=} \frac{2y_0^{p^n}\left(\sum_{i=0}^n F_i^{p^{n-i}-1}\frac{\mathrm{d}F_i}{\mathrm{d}x_0}\right)}{(b_0^2x_0^2-1)^{p^n}}\mathrm{d}x_0 = \frac{2x_0^{p^n}\left(\sum_{i=0}^n G_i^{p^{n-i}-1}\frac{\mathrm{d}G_i}{\mathrm{d}y_0}\right)}{(1-y_0^2)^{p^n}}\mathrm{d}y_0,$$

which can be also represented as

$$\omega = \frac{y_0^{p^n-1}\left(\sum_{i=0}^n F_i^{p^{n-i}-1}\frac{\mathrm{d}F_i}{\mathrm{d}x_0}\right)}{(b_0^2x_0^2-1)^{p^n-1}}\omega_0 = \frac{x_0^{p^n-1}\left(\sum_{i=0}^n G_i^{p^{n-i}-1}\frac{\mathrm{d}G_i}{\mathrm{d}y_0}\right)}{(1-y_0^2)^{p^n-1}}\omega_0.$$

Since the invariant differential is regular on $\boldsymbol{U}^{\sigma^n}$, the reduction modulo p of its pullback by $\boldsymbol{\phi}^n$ must also be, and hence we have that $\omega = \lambda_n \omega_0$, for some λ_n in the affine coordinate ring $\Bbbk[E_{a_0,b_0}]$. From the representations of ω above, we then obtain

$$\begin{aligned} y_0^{p^n-1} \sum_{i=0}^{n} F_i^{p^{n-i}-1} \frac{\mathrm{d}F_i}{\mathrm{d}x_0} &= \lambda_n \left(b_0^2 x_0^2 - 1\right)^{p^n-1} \\ x_0^{p^n-1} \sum_{i=0}^{n} G_i^{p^{n-i}-1} \frac{\mathrm{d}G_i}{\mathrm{d}y_0} &= \lambda_n \left(1 - y_0^2\right)^{p^n-1}. \end{aligned}$$

Now, since

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

we get

$$\begin{aligned} \frac{\mathrm{d}F_n}{\mathrm{d}x_0} &= \lambda_n (b_0^2 x_0^2 - 1)^{\frac{p^n-1}{2}} (a_0 x_0^2 - 1)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} F_k^{p^{n-k}-1} \frac{\mathrm{d}F_k}{\mathrm{d}x_0}, \\ \frac{\mathrm{d}G_n}{\mathrm{d}y_0} &= \lambda_n (b_0^2 - a_0 y_0^2)^{\frac{p^n-1}{2}} (1 - y_0^2)^{\frac{p^n-1}{2}} - \sum_{k=0}^{n-1} G_k^{p^{n-k}-1} \frac{\mathrm{d}G_k}{\mathrm{d}y_0}. \end{aligned}$$

This implies that $\lambda_n (b_0^2 x_0^2 - 1)^{\frac{p^n-1}{2}} (a_0 x_0^2 - 1)^{\frac{p^n-1}{2}}$ must be equal to a polynomial in x_0 in $\Bbbk[E_{a_0,b_0}]$. We then have

$$\begin{aligned} \deg_{x_0} \left(\lambda_n (b_0^2 x_0^2 - 1)^{\frac{p^n-1}{2}} (a_0 x_0^2 - 1)^{\frac{p^n-1}{2}} \right) &= -\operatorname{ord}_{\mathcal{Q}^{\pm}} \left(\lambda_n (b_0^2 x_0^2 - 1)^{\frac{p^n-1}{2}} (a_0 x_0^2 - 1)^{\frac{p^n-1}{2}} \right) \\ &= (2p^n - 2) - \operatorname{ord}_{\mathcal{Q}^{\pm}}(\lambda_n) \geq 2p^n - 2, \end{aligned}$$

and therefore, since for $k < n$ we have that

$$\deg_{x_0} \left(F_k^{p^{n-k}-1} \frac{\mathrm{d}F_k}{\mathrm{d}x_0} \right) = 2^{p^n} - 1 - p^{n-k}$$

by the induction hypothesis, we have that $\deg_{x_0} F_n \geq 2p^n - 1$. Similarly, $\deg_{y_0} G_n \geq 2p^n - 1$.

Now if the equality occurs in both cases, then $\operatorname{ord}_{\mathcal{O}^{\pm}} \lambda_n = \operatorname{ord}_{\mathcal{Q}^{\pm}} \lambda_n = 0$, and since $\lambda_n \in \Bbbk[E_{a_0,b_0}]$, we must have that $\lambda_n \in \Bbbk$.

We now must show that in this case we must have $\lambda_n = \mathfrak{h}^{-(p^n-1)/(p-1)}$, which we also do by induction. For $n = 1$, the formula for the derivative is

$$\frac{\mathrm{d}F_1}{\mathrm{d}x_0} = \lambda_1 (b_0 x_0^2 - 1)^{\frac{p-1}{2}} (a_0 x_0^2 - 1)^{\frac{p-1}{2}} - x_0^{p-1}.$$

But for the terms on the left-side to be a derivative, it must contain no term in x_0^{p-1}, and hence λ_1 is the inverse of the coefficient of x_0^{p-1} of $(b_0 x_0^2 - 1)^{\frac{p-1}{2}} (a_0 x_0^2 - 1)^{\frac{p-1}{2}}$, i.e., the inverse of the Hasse invariant $\mathfrak{h}$, which therefore must be non-zero. Hence, we have that $\lambda_1 = \mathfrak{h}^{-1}$, as needed.

Now, by the induction hypothesis, we have

$$\mathfrak{h}^{-(p^{n-1}-1)/(p-1)} = \frac{y_0^{p^{n-1}-1} \sum_{i=0}^{n-1} F_i^{p^{n-1-i}-1} \frac{\mathrm{d}F_i}{\mathrm{d}x_0}}{(b_0^2 x_0^2 - 1)^{p^{n-1}-1}}.$$

Then, if $\mathcal{C}$ denotes the *Cartier operator*, we have

$$\begin{aligned}
\mathcal{C}(\omega) &= \mathcal{C}\left(\frac{2 y_0^{p^n} \left(\sum_{i=0}^{n} F_i^{p^{n-i}-1} \frac{\mathrm{d}F_i}{\mathrm{d}x_0} \right)}{(b_0^2 x_0^2 - 1)^{p^n-1}} \, \mathrm{d}x_0 \right) \\
&= \frac{2 y_0^{p^{n-1}} \left(\sum_{i=0}^{n-1} F_i^{p^{n-1-i}-1} \frac{\mathrm{d}F_i}{\mathrm{d}x_0} \right)}{(b_0^2 x_0^2 - 1)^{p^{n-1}}} \, \mathrm{d}x_0 \\
&= \frac{y_0^{p^{n-1}-1} \left(\sum_{i=0}^{n-1} F_i^{p^{n-1-i}-1} \frac{\mathrm{d}F_i}{\mathrm{d}x_0} \right)}{(b_0^2 x_0^2 - 1)^{p^{n-1}-1}} \, \omega_0 \\
&= \mathfrak{h}^{-(p^{n-1}-1)/(p-1)} \omega_0.
\end{aligned}$$

But since we also have $\omega = \lambda_n \omega_0$, we obtain $\mathcal{C}(\omega) = \lambda_n^{1/p} \mathcal{C}(\omega_0) = \lambda_n^{1/p} \mathfrak{h}^{1/p} \omega_0$. Comparing these two expressions for $\mathcal{C}(\omega)$, we obtain the desired expression for λ_n. □

7. Technical Lemmas

Our next goal is to prove that we can achieve the lower bound for ordinary elliptic curves up to the third coordinated, stated as Theorem 8.1 below. Its proof requires many involved computations, and thus we shall use this section to introduce some lemmas with the intent of simplifying the exposition. Although notation-heavy, most of these lemmas are quite simple, with one exception (namely, item 2 of Lemma 7.2), which shall take most of this section.

We shall assume in this section that E_{a_0,b_0} is an ordinary elliptic curve, $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ is its canonical lifting, and

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

is the elliptic Teichmüller lift.

Note that if $\boldsymbol{b} \equiv \tilde{\boldsymbol{b}} \pmod{p}$, we have that the Edwards curves give by

$$\boldsymbol{b}^2\boldsymbol{x}^2 + \boldsymbol{y}^2 = 1 - \boldsymbol{a}\boldsymbol{x}^2\boldsymbol{y}^2$$

and

$$\tilde{\boldsymbol{b}}^2\boldsymbol{x}^2 + \boldsymbol{y}^2 = 1 - \frac{\tilde{\boldsymbol{b}}^2}{\boldsymbol{b}^2}\boldsymbol{a}\boldsymbol{x}^2\boldsymbol{y}^2$$

are isomorphic, with isomorphism $(\boldsymbol{x}, \boldsymbol{y}) \mapsto \left(\frac{\boldsymbol{b}}{\tilde{\boldsymbol{b}}}\boldsymbol{x}, \boldsymbol{y}\right)$, and hence we can assume, without loss of generality that $\boldsymbol{b} = (b_0, 0, 0)$, and we will assume that this is the case for the canonical lifting $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$.

We start with some notation and simple results about representations in the affine coordinate ring $\Bbbk[E_{a_0,b_0}]$:

Lemma 7.1. *Let*

$$A_1(y_0) \stackrel{\text{def}}{=} y_0 - 1, \qquad A_2(y_0) \stackrel{\text{def}}{=} a_0y_0 - b_0^2, \qquad A_3(y_0) \stackrel{\text{def}}{=} a_0y_0^2 - 2b_0^2y_0 + b_0^2$$
$$B_1(x_0) \stackrel{\text{def}}{=} b_0^2x_0 - 1, \qquad B_2(x_0) \stackrel{\text{def}}{=} a_0x_0 - 1, \qquad B_3(x_0) \stackrel{\text{def}}{=} a_0b_0^2x_0^2 - 2b_0^2x_0 + 1.$$

We then have:

(1)

$$B_3(x_0^2)A_2(y_0^2) = (b_0^2 - a_0)(b_0^2x_0^2 - y_0^2),$$
$$A_3(y_0^2)B_2(x_0^2) = -(b_0^2 - a_0)(b_0^2x_0^2 - y_0^2).$$

(2)

$$B_2(x_0^2)y_0^2 = B_1(x_0^2),$$
$$A_2(y_0^2)x_0^2 = A_1(y_0^2).$$

(3) $A_2(y_0^2)B_2(x_0^2) = b_0^2 - a_0$.

(4) *For $i, t \in \mathbb{Z}_{>0}$ and $t \geq i$, we have*

$$(b_0^2 - a_0)^i B_1(x_0^2)^{t-i} = y_0^{2(t-i)} A_2(y_0)^i B_2(x_0^2)^t.$$

(5)

$$\begin{aligned}
A_1(b_0^2 x_0^2) &= B_1(x_0^2),\\
A_2(b_0^2 x_0^2) &= b_0^2 B_2(x_0^2),\\
A_3(b_0^2 x_0^2) &= b_0^2 B_3(x_0^2).
\end{aligned}$$

Proof. The proof is completely elementary and can be easily checked. □

The next lemma, which deals with the second coordinates of the elliptic Teichmüller lift (i.e., F_1 and G_1), is also relatively simple, except for item 2, which is a key step for the proof of Theorem 8.1, and will take most of this section.

Lemma 7.2. *Assume that $p > 7$ and let*

$$\begin{aligned}
d_1(t) &\stackrel{\text{def}}{=} t^{\frac{p+1}{2}} B_1(t)^{\frac{p+1}{2}} B_2(t) B_3(t),\\
d_2(t) &\stackrel{\text{def}}{=} t^{\frac{p+1}{2}} A_1(t)^{\frac{p+1}{2}} A_2(t) A_3(t).
\end{aligned}$$

(1) *There are polynomials $q_1, q_2, r_1, r_2 \in \Bbbk[t]$ such that*

$$\begin{aligned}
F_1(x_0)^2 &= d_1(x_0^2) q_1(x_0^2) + r_1(x_0^2),\\
G_1(y_0)^2 &= d_2(y_0^2) q_2(y_0^2) + r_2(y_0^2),
\end{aligned}$$

with $\deg q_i = p - 5$ and $\deg r_i \leq p + 3$. (Hence, the equations above give the long divisions of F_1^2 and G_1^2 by $d_1(x_0^2)$ and $d_2(y_0^2)$, respectively.)

(2) *There are $\alpha_i \in \Bbbk$, for $i \in \{0, 1, \ldots, (p-5)/2\}$ and $\tilde{q}_j \in \Bbbk[t]$ with $\deg \tilde{q}_j \leq (p-9)/2$, for $j \in \{1, 2\}$, such that*

$$\begin{aligned}
q_1(t) &= \tilde{q}_1(t) + \sum_{i=0}^{(p-5)/2} \alpha_i [t \cdot B_1(t)]^{\frac{p-5}{2} - i} B_2(t)^i,\\
q_2(t) &= \tilde{q}_2(t) + \sum_{i=0}^{(p-5)/2} \alpha_i [t \cdot A_1(t)]^{\frac{p-5}{2} - i} A_2(t)^i.
\end{aligned}$$

(3) *Let* $f_i(t) \stackrel{\text{def}}{=} q_i(t) - \tilde{q}_i(t)$*, and hence given by the summations above. We then have*

$$f_1(x_0^2) A_2(y_0^2)^{\frac{p-5}{2}} = f_2(y_0^2) B_2(x_0^2)^{\frac{p-5}{2}}.$$

(4) *We have*

$$f_2(b_0^2 x_0^2) = b_0^{p-5} f_1(x_0^2).$$

Proof. For the first item, remember that $F_1(x_0) = x_0 \hat{F}_1(x_0^2)$, and $G_1(y_0) = y_0 \hat{G}_1(y_0^2)$. Then, we divide $\hat{F}(t)^2$ and $\hat{G}(t)^2$ by $d_1(t)$ and $d_2(t)$:

$$\begin{aligned} \hat{F}_1(t)^2 &= \frac{d_1(t)}{t} q_1(t) + \hat{r}_1(t), \\ \hat{G}_1(t)^2 &= \frac{d_2(t)}{t} q_2(t) + \hat{r}_2(t), \end{aligned}$$

with $\deg \hat{r}_i \leq p+2$. Letting $r_i(t) \stackrel{\text{def}}{=} t\, \hat{r}_i(t)$, the above equations give us the desired result.

Assuming that item 2 holds and using item 2 of Lemma 7.1, we get

$$\begin{aligned} f_1(x_0^2) A_2(y_0^2)^{\frac{p-5}{2}} &= \sum_{i=0}^{(p-5)/2} \alpha_i \left[x_0^2 B_1(x_0^2) A_2(y_0^2) \right]^{\frac{p-5}{2}-i} B_2(x_0^2)^i A_2(y_0^2)^i \\ &= B_2(x_0^2)^{\frac{p-5}{2}} \sum_{i=0}^{(p-5)/2} \alpha_i \left[x_0^2 \frac{B_1(x_0^2)}{B_2(x_0^2)} A_2(y_0^2) \right]^{\frac{p-5}{2}-i} A_2(y_0^2)^i \\ &= B_2(x_0^2)^{\frac{p-5}{2}} \sum_{i=0}^{(p-5)/2} \alpha_i \left[x_0^2 y_0^2 A_2(y_0^2) \right]^{\frac{p-5}{2}-i} A_2(y_0^2)^i \\ &= f_2(y_0^2) B_2(x_0^2)^{\frac{p-5}{2}}, \end{aligned}$$

and hence item 3 also must hold.

Moreover, still assuming item 2 holds, and using item 5 of Lemma 7.1, we have

$$\begin{aligned} f_2(b_0^2 x_0^2) &= \sum_{i=0}^{(p-5)/2} \alpha_i \left[b_0^2 x_0^2 A_1(b_0^2 x_0^2) \right]^{\frac{p-5}{2}-i} A_2(b_0^2 x_0^2)^i \\ &= \sum_{i=0}^{(p-5)/2} \alpha_i \left[b_0^2 x_0^2 B_1(x_0^2) \right]^{\frac{p-5}{2}-i} b_0^{2i} B_2(x_0^2)^i \\ &= b_0^{p-5} f_1(x_0^2), \end{aligned}$$

which proves item 4.

Thus, it only remains to prove item 2. First note that since

$$\deg\left([t\cdot B_1(t)]^{\frac{p-5}{2}-i}B_2(t)^i\right)=p-5-i,$$

there are *unique* $\alpha_i\in\Bbbk$ and $\tilde{q}_1\in\Bbbk[t]$ such that

$$q_1(t)=\tilde{q}_1(t)+\sum_{i=0}^{(p-5)/2}\alpha_i[t\cdot B_1(t)]^{\frac{p-5}{2}-i}B_2(t)^i,$$

with $\deg\tilde{q}_1\leq(p-7)/2$.

Similarly, we have that there are uniquely determined $\beta_i\in\Bbbk$ and $\tilde{q}_2\in\Bbbk[t]$ with $\deg\tilde{q}_2\leq(p-7)/2$ such that

$$q_2(t)=\tilde{q}_2(t)+\sum_{i=0}^{(p-5)/2}\beta_i[t\cdot A_1(t)]^{\frac{p-5}{2}-i}A_2(t)^i.$$

Hence, we must show that $\alpha_i=\beta_i$ for all i, and that $\deg\tilde{q}_j\leq(p-9)/2$.

For the first part, note that since τ is an Edwards lift, and $\boldsymbol{b}=(b_0,0,0)$, we have that $G_1(b_0x_0)=b_0^pF_1(x_0)$. Also, item 5 of Lemma 7.1 and a simple computation shows that $d_2(b_0^2x_0^2)=b_0^{p+5}d_1(x_0^2)$. Therefore we have

$$\begin{aligned}F_1(x_0)^2&=\frac{1}{b_0^{2p}}G_1(b_0x_0)\\&=\frac{1}{b_0^{2p}}d_2(b_0^2x_0^2)q_2(b_0^{p^2}x_0^2)+r_2(b_0^2x_0^2)\\&=d_1(x_0^2)\left[b_0^{-(p-5)}q_2(x_0^2)\right]+\left[b_0^{-2p}r_2(b_0^2x_0^2)\right].\end{aligned}$$

Thus, by the uniqueness of the quotient and remainder, we have $q_1(x_0^2)=b_0^{-(p-5)}q_2(x_0^2)$ and $r_1(x_0^2)=b_0^{-2p}r_2(b_0^2x_0^2)$. This gives us that

$$\begin{aligned}q_1(x_0^2)&=b_0^{-(p-5)}\tilde{q}_2(b_0^2x_0^2)+b_0^{-(p-5)}\sum_{i=0}^{(p-5)/2}\beta_i\left[b_0^2x_0^2A_1(b_0^2x_0^2)\right]^{(p-5)/2-i}A_2(b_0^2x_0^2)^i\\&=b_0^{-(p-5)}\tilde{q}_2(b_0^2x_0^2)+\sum_{i=0}^{(p-5)/2}\beta_i\left[x_0^2B_1(x_0^2)\right]^{(p-5)/2-i}B_2(x_0^2)^i.\end{aligned}$$

Hence, by the uniqueness of the construction, we must have that $\alpha_i=\beta_i$ for all i and $\tilde{q}_1(x_0^2)=b_0^{-(p-5)}\tilde{q}_2(b_0^2x_0^2)$.

Since this last statement shows that $\deg \tilde{q}_1 = \deg \tilde{q}_2$, it now suffices to show that $\deg \tilde{q}_1 \leq (p-9)/2$ to finish the proof of item 2. Thus, if we let c be the coefficient of $x_0^{(p-7)/2}$ in $\tilde{q}_1$, we must show that $c = 0$. For that we look at the derivative

$$\begin{aligned}\frac{\mathrm{d}(F_1)^3}{\mathrm{d}x_0} &= 3F_1^2 \frac{\mathrm{d}F_1}{\mathrm{d}x_0} \\ &= 3[d_1(x_0^2)q_1(x_0^2) + r_1(x_0^2)]\frac{\mathrm{d}F_1}{\mathrm{d}x_0} \\ &= 3[d_1(x_0^2)\tilde{q}_1(x_0^2) + d_1(x_0^2)f_1(x_0^2) + r_1(x_0^2)]\frac{\mathrm{d}F_1}{\mathrm{d}x_0}.\end{aligned}$$

Since this expression is a derivative, the coefficient of x_0^{5p-1} must be zero. Note that by Theorem 3.1

$$\frac{\mathrm{d}F_1}{\mathrm{d}x_0} = \mathfrak{h}^{-1} B_1(x_0^2)^{(p-1)/2} B_2(x_0^2)^{(p-1)/2} - x_0^{p-1}, \tag{7.1}$$

and thus the coefficient of x_0^{5p-1} in $3d_1(x_0^2)\tilde{q}_1(x_0^2)\mathrm{d}F_1/\mathrm{d}x_0$ is $3\mathfrak{h}^{-1} a_0^{\frac{p+3}{2}} b_0^{2p+2} c$. Hence, to show that $c = 0$, it now suffices to prove that the other two terms yield no term in x_0^{5p-1}.

Since $\deg r_1 \leq p-3$ and $\deg \mathrm{d}F_1/\mathrm{d}x_0 = 2p-2$, the last term yields no term in x_0^{5p-1}.

Finally, we look at

$$d_1(x_0^2)f_1(x_0^2)\frac{\mathrm{d}F_1}{\mathrm{d}x_0} = d_1(x_0^2)f_1(x_0^2)\left[\mathfrak{h}^{-1} B_1(x_0^2)^{(p-1)/2} B_2(x_0^2)^{(p-1)/2} - x_0^{p-1}\right]. \tag{7.2}$$

Since

$$\deg\left(d_1(x_0^2)f_1(x_0^2)x_0^{p-1}\right) = 5p-3 < 5p-1,$$

the coefficient of x_0^{5p-1} from Eq. (7.2) must come from

$$d_1(x_0^2)f_1(x_0^2)B_1(x_0^2)^{(p-1)/2}B_2(x_0^2)^{(p-1)/2} = x_0^{p+1}B_1(x_0^2)^p B_2(x_0^2)^{\frac{p+1}{2}} B_3(x_0^2)f_1(x_0^2),$$

and it is the same as the coefficient of t^{p-1} in

$$\begin{aligned}&B_2(t)^{\frac{p+1}{2}} B_3(t) f_1(t) \\ &\qquad = \sum_{i=0}^{(p-5)/2} \alpha_i (a_0 b_0^2 t^2 - 2b_0^2 t + 1) t^{(p-5)/2-i} (b_0^2 t - 1)^{(p-5)/2-i} (a_0 t - 1)^{(p+1)/2+i}.\end{aligned}$$

Therefore, to conclude the proof, we now show that this coefficient must be zero. To simplify our notation, let $r \stackrel{\text{def}}{=} (p-5)/2$, so that the above equation becomes

$$B_2(t)^{r+3} B_3(t) f_1(t) = \sum_{i=0}^{r} \alpha_i (a_0 b_0^2 t^2 - 2b_0^2 t + 1) t^{r-i} (b_0^2 t - 1)^{r-i} (a_0 t - 1)^{r+3+i}. \tag{7.3}$$

Then, for $0 \leq i \leq r-1$, expanding the powers we get that the summand for index i on the right-side of Eq. (7.3) is α_i times

$$
\begin{aligned}
(a_0 b_0^2 t^2 - 2b_0^2 t + 1) \cdot & \sum_{l=0}^{r+3+i} \sum_{k=0}^{r-i} (-1)^{l+k} \cdot \binom{r+3+i}{l}\binom{r-i}{k} a_0^{r+3+i-l} b_0^{2(r-i-k)} t^{3r+3-i-k-l} \\
&= \sum_{l=0}^{r+3+i} \sum_{k=0}^{r-i} (-1)^{l+k} \cdot \binom{r+3+i}{l}\binom{r-i}{k} a_0^{r+4+i-l} b_0^{2(r+1-i-k)} t^{3r+5-i-k-l} \\
&\quad + 2 \cdot \sum_{l=0}^{r+3+i} \sum_{k=0}^{r-i} (-1)^{l+k+1} \cdot \binom{r+3+i}{l}\binom{r-i}{k} a_0^{r+3+i-l} b_0^{2(r+1-i-k)} t^{3r+4-i-k-l} \\
&\quad + \sum_{l=0}^{r+3+i} \sum_{k=0}^{r-i} (-1)^{l+k} \cdot \binom{r+3+i}{l}\binom{r-i}{k} a_0^{r+3+i-l} b_0^{2(r-i-k)} t^{3r+3-i-k-l}.
\end{aligned}
$$

Thus, the coefficient of t^{p-1} in the expression above is equal to

$$
\begin{aligned}
& \sum_{k=0}^{r-i} (-1)^{r+1-i} \cdot \binom{r+3+i}{r+1-i-k}\binom{r-i}{k} a_0^{3+2i+k} b_0^{2(r-i-k)} \\
&\quad + 2 \cdot \sum_{k=0}^{r-i} (-1)^{r+1-i} \cdot \binom{r+3+i}{r-i-k}\binom{r-i}{k} a_0^{3+2i+k} b_0^{2(r+1-i-k)} \\
&\quad + \sum_{k=0}^{r-1-i} (-1)^{r-1-i} \cdot \binom{r+3+i}{r-1-k-i}\binom{r-i}{k} a_0^{2i+k+4} b_0^{2(r-i-k)} \\
&= (-1)^{r+1} a_0^{2i+3} b_0^{2r+2-2i} \cdot \left[\sum_{k=0}^{r-i} \binom{r+3+i}{r+1-i-k}\binom{r-i}{k} a_0^k b_0^{-2k} \right. \\
&\quad + 2 \cdot \sum_{k=0}^{r-i} \binom{r+3+i}{r-i-k}\binom{r-i}{k} a_0^k b_0^{-2k} \\
&\quad \left. + \sum_{k=0}^{r-1-i} \binom{r+3+i}{r-1-k-i}\binom{r-i}{k} a_0^{k+1} b_0^{-2(k+1)} \right].
\end{aligned}
$$

Now, dropping the non-zero constant isolated above, we can rewrite the above expression, by isolation the terms in $k=0$ in the first two summations and reparameterizing, as

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

We then first observe that, since $0 \leq i \leq r-1 = (p-7)/2$, we have

$$\binom{r+3+i}{r+1-i} + 2\binom{r+3+i}{r-i} = \frac{(r+3+i)!}{(r-i)!(2+2i)!} \cdot \frac{p}{(r+1-i)(3+2i)} = 0.$$

Moreover, since $k \leq r-1-i$ and $0 \leq i \leq r-1$, we have that $2i+k+4 \leq 2r+2 = p-3$, and thus, by Pascal's identity, we similarly have

$$\begin{aligned}\binom{r-i}{k+1}\binom{r+3+i}{r-k-i} + 2\binom{r-i}{k+1}\binom{r+3+i}{r-1-k-i} + \binom{r-i}{k}\binom{r+3+i}{r-1-k-i}&\\ = \binom{r-i}{k+1}\binom{r+4+i}{r-k-i} + \binom{r+1-i}{k+1}\binom{r+3+i}{r-1-k-i}&\\ = \frac{(r-i)!(r+3+i)!}{(k+1)!(r-i-k)!(r-1--k)!(2i+k+4)!} \cdot p = 0.&\end{aligned}$$

Therefore, all terms in t^{p-1} from Eq. (7.3) coming from summands corresponding to index i between 0 and $r-1$ are zero.

Finally, for index $i = r$, the corresponding summand from Eq. (7.3) is

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

Thus, the coefficient of t^{p-1} is

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

which conclude the proof. $\square$

The final lemma of this section is a simple result relating the second and third coordinates of the elliptic Teichmüller lift:

Lemma 7.3. *Let*

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

Then, we have that $\deg_{x_0}\left(x_0^{p^2} F_2 - F_1^{2p}\right), \deg_{y_0}\left(y_0^{p^2} G_2 - G_1^{2p}\right) \leq 3p^2 - 1.$

Proof. By [3, Corollary 7.2], we have that $\tau^*(1/\boldsymbol{x})(\mathcal{Q}^{\pm}) = \tau^*(1/\boldsymbol{y})(\mathcal{O}^{\pm}) = 0$. Now, since

$$\frac{1}{(t_0, t_1, t_2)} = \left(\frac{1}{t_0}, -\frac{t_1}{t_0^{2p}}, \frac{t_1^{2p} - t_0^{p^2} t_2}{t_0^{3p^2}}\right),$$

the result follows from Eq (2.2).

□

8. Minimal Degree Liftings Modulo p^3

In this section we prove that we can achieve the lower bound for ordinary elliptic curves given by Theorem 6.6 up to the third coordinated. (Again, the motivation here comes from the construction of error-correcting codes, where smaller degrees yield better parameters for the resulting codes.) More precisely, we will show that given an ordinary Edwards curve, we can obtain a lift of points $(x_0, y_0) \mapsto ((x_0, F_1, F_2), (y_0, G_1, G_2))$ with $\deg F_i = \deg G_i = 2p^i - 1$. Note that by Theorem 5.1, we know we can achieve get $\deg F_1 = \deg G_1 = 2p - 1$ when $(x_0, y_0) \mapsto ((x_0, F_1), (y_0, G_1))$ is the elliptic Teichmüller (up to the second coordinate) itself. But, by Theorem 3.1, we know that F_2 and G_2 cannot be given by the elliptic Teichmüller, so a different lift is needed.

Theorem 8.1. *Let E_{a_0,b_0} be an ordinary elliptic curve, $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ be its canonical lifting, and*

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

be the elliptic Teichmüller lift. Then, there is a Edwards lift of points

$$\nu = ((x_0, F_1, \tilde{F}_2), (y_0, G_1, \tilde{G}_2))$$

between E_{a_0,b_0} and the canonical lifting $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$ with $\deg_{x_0} \tilde{F}_2 = \deg_{y_0} \tilde{G}_2 = 2p^2 - 1.$

Remark. The canonical lifting and associated elliptic Teichmüller lift give the lower bound for the second coordinates. But note that when adding the third coordinate, although the curve that gives the lower bound is still the canonical lifting, the lift of points *cannot* be the elliptic Teichmüller lift anymore.

It is natural to ask if it remains true that the lower bound of Theorem 6.6 can always be achieve and the corresponding curve is always the canonical lifting. We do not have an answer to this general question, or even computational evidence, as computations are quite demanding. But in the case of *elliptic curves*, we could always get the lower bound for the fourth coordinate in any concrete example we tried, although we could not prove it in general, but the curves obtained were *not* the corresponding canonical liftings anymore. We expect something similar would occur for Edwards curves.

Proof of Theorem 8.1. As before, note that we can assume, without loss of generality, that $\boldsymbol{b} = (b_0, 0, 0)$. Note that if $\deg_{t_0} T_1(t_0) = 2p-1$, $\deg_{t_0} T_2(t_0) = 2p^2-1$ and if $\boldsymbol{c} = (c_0, c_1, c_2)$, with $c_i \in \Bbbk$ and $c_0 \neq 0$, then the second and third coordinates of

$$(c_0, c_1, c_2) \cdot (t_0, T_1(t_0), T_2(t_0))$$

have degrees $2p-1$ and $2p^2-1$ respectively. This follows since the second coordinate is given by

$$c_0^p T_1(t_0) + c_1 t_0,$$

and the third coordinate is given by

$$c_0^{p^2} T_2(t_0) + c_1^p T_1(t_0)^p + c_2 t_0^{p^2} - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} c_0^{pi} c_1^{p-i} t_0^{p(p-i)} T_1(t_0)^i.$$

Thus, we shall assume that $\boldsymbol{b} = (b_0, 0, 0)$, and if we can achieve the lower bound in this particular case, we can achieve in any case using an isomorphism.

Moreover, we shall assume that $p > 7$. The cases for $p = 5$ and $p = 7$ can be computed directly with the algorithms in `https://github.com/lrfinotti/witt`, but unfortunately, the formulas are too long to be added here.

Similar to the proof of Theorem 6.4, on the third coordinate of $\tau^* G(\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}})$ we have

$$2(b_0 - a_0 y_0^2)^{p^2} x_0^{p^2} F_2 + 2(1 - a_0 x_0^2)^{p^2} y_0^{p^2} G_2 = \cdots, \tag{8.1}$$

where the omitted terms do not involve F_2 or G_2. By [3, Proposition 4.4], we can write $F_2(x_0) = x_0\hat{F}_2(x_0^2)$ and $G_2(y_0) = y_0\hat{G}_2(y_0^2)$. Then, again, as done in the proof of Theorem 6.4, the equation of E_{a_0,b_0} allows us to rewrite the equation above as

$$A(y_0^2)\hat{F}_2(x_0^2) + B(x_0^2)\hat{G}_2(y_0^2) = \cdots,$$

where

$$A(y_0) \stackrel{\text{def}}{=} 2A_1(y_0)^{\frac{p^2+1}{2}} A_2(y_0)^{\frac{p^2-1}{2}},$$
$$B(x_0) \stackrel{\text{def}}{=} 2B_1(x_0)^{\frac{p^2+1}{2}} B_2(x_0)^{\frac{p^2-1}{2}},$$

with A_i and B_i as in Lemma 7.1 and with the omitted terms equal to the ones from Eq. (8.1).

Now, with the notation from Lemmas 7.1 and 7.2, and letting

$$\tilde{r}_1(t) \stackrel{\text{def}}{=} r_1(t) + d_1(t)\tilde{q}_1(t),$$
$$\tilde{r}_2(t) \stackrel{\text{def}}{=} r_1(t) + d_2(t)\tilde{q}_2(t),$$

we can write

$$F_1(x_0)^2 = d_1(x_0^2)f_1(x_0^2) + \tilde{r}_1(x_0^2),$$
$$G_1(y_0)^2 = d_2(y_0^2)f_2(y_0^2) + \tilde{r}_2(y_0^2),$$

with $\deg \tilde{r}_i \leq (3p-1)/2$.

Now, let

$$\delta_1(x_0) \stackrel{\text{def}}{=} x_0^{p^2} F_2 - F_1^{2p},$$
$$\delta_2(x_0) \stackrel{\text{def}}{=} y_0^{p^2} G_2 - G_1^{2p}.$$

Then, by Lemma 7.3, we have that $\deg \delta_i \leq 3p^2 - 1$. We then have

$$x_0^{p^2} F_2 = d_1(x_0^2)^p f_1(x_0^2)^p + \left[\tilde{r}_1(x_0^2)^p + \delta_1(x_0)\right], \tag{8.2}$$
$$y_0^{p^2} G_2 = d_2(y_0^2)^p f_2(y_0^2)^p + \left[\tilde{r}_2(y_0^2)^p + \delta_2(y_0)\right], \tag{8.3}$$

This implies that $x_0^{p^2} \mid d_1(x_0^2)^p$ and $y_0^{p^2} \mid d_2(y_0^2)^p$, and so let now

$$\tilde{F}_2(x_0) \stackrel{\text{def}}{=} \frac{\tilde{r}_1(x_0^2)^p + \delta_1(x_0)}{x_0^{p^2}},$$
$$\tilde{G}_2(y_0) \stackrel{\text{def}}{=} \frac{\tilde{r}_2(y_0^2)^p + \delta_2(y_0)}{y_0^{p^2}}.$$

Then, $\tilde{F}_2$ and $\tilde{G}_2$ are polynomials of degree less than or equal to $2p^2-1$, and we now proceed to show that they give the desired minimal degree lifting.

To prove that

$$\nu(x_0, y_0) \stackrel{\text{def}}{=} ((x_0, F_1, \tilde{F}_2), (y_0, G_1, \tilde{G}_2))$$

defines a lift of points between E_{a_0,b_0} and its canonical lifting $\boldsymbol{E}_{\boldsymbol{a},\boldsymbol{b}}$, it suffices to show that

$$-2A_2(y_0^2)^{p^2} x_0^{p^2} \tilde{F}_2 - 2B_2(x_0^2)^{p^2} y_0^{p^2} \tilde{G}_2 = \cdots\,, \tag{8.4}$$

with the same omitted terms as Eq. (8.1), or equivalently, that

$$A_2(y_0^2)^{p^2} x_0^{p^2} F_2 + B_2(x_0^2)^{p^2} y_0^{p^2} G_2 = A_2(y_0^2)^{p^2} x_0^{p^2} \tilde{F}_2 + B_2(x_0^2)^{p^2} y_0^{p^2} \tilde{G}_2.$$

By Eqs. (8.2) and (8.3), it suffices to show that

$$A_2(y_0^2)^{p^2} d_1(x_0^2)^p f_1(x_0^2)^p = -B_2(x_0^2)^{p^2} d_2(y_0^2)^p f_2(y_0^2)^p. \tag{8.5}$$

By definition of d_1, given in Lemma 7.2, we have

$$A_2(y_0^2)^{p^2} d_1(x_0^2)^p f_1(x_0^2)^p = A_2(y_0^2)^{p^2} x_0^{p^2+p} B_1(x_0^2)^{\frac{p^2+p}{2}} B_2(x_0^2)^p B_3(x_0^2)^p f_1(x_0^2)^p.$$

Then, by item 1 of Lemma 7.1, we have

$$\begin{aligned} &A_2(y_0^2)^{p^2} d_1(x_0^2)^p f_1(x_0^2)^p \\ &\qquad = (b_0^2 - a_0)^p x_0^{p^2+p} A_2(y_0^2)^{p^2-p} B_1(x_0^2)^{\frac{p^2+p}{2}} B_2(x_0^2)^p f_1(x_0^2)^p (b_0^2 x_0^2 - y_0^2)^p. \end{aligned}$$

Now, by item 2 of the same lemma, we obtain

$$\begin{aligned} &A_2(y_0^2)^{p^2} d_1(x_0^2)^p f_1(x_0^2)^p \\ &\qquad = (b_0^2 - a_0)^p x_0^{p^2+p} y_0^{p^2+p} A_2(y_0^2)^{p^2-p} B_2(x_0^2)^{\frac{p^2+3p}{2}} f_1(x_0^2)^p (b_0^2 x_0^2 - y_0^2)^p. \end{aligned}$$

Then, by item 3 of the same lemma,

$$A_2(y_0^2)^{p^2} d_1(x_0^2)^p f_1(x_0^2)^p = (b_0^2 - a_0)^{\frac{p^2+5p}{2}} x_0^{p^2+p} y_0^{p^2+p} \left[f_1(x_0^2) A_2(y_0^2)^{\frac{p-5}{2}} \right]^p (b_0^2 x_0^2 - y_0^2)^p.$$

An analogous argument yields

$$B_2(x_0^2)^{p^2} d_2(y_0^2)^p f_2(y_0^2)^p = -(b_0^2 - a_0)^{\frac{p^2+5p}{2}} x_0^{p^2+p} y_0^{p^2+p} \left[f_2(y_0^2) B_2(x_0^2)^{\frac{p-5}{2}} \right]^p (b_0^2 x_0^2 - y_0^2)^p.$$

Now, by item 3 of Lemma 7.2, these last two equations give us the desired result, namely, that Eq. (8.5) holds.

Now, to finish the proof we must show that ν (as defined above) is an Edwards lift. Since ν is the same τ modulo p^2, and since $\boldsymbol{b} = (b_0, 0, 0)$, it suffices to show that

$$\tilde{G}_2(b_0 x_0) = b_0^{p^2} \tilde{F}(x_0), \quad \tilde{F}_2(y_0/b_0) = \frac{\tilde{G}_2(y_0)}{b_0^{p^2}}.$$

Clearly, it suffices to prove the former. But since τ is an Edwards lift, we have $G_2(b_0x_0) = b_0^2 F_2(x_0)$. Then, by item 4 of Lemma 7.2 and item 5 of Lemma 7.1, we get

$$\begin{aligned}
\tilde{G}_2(b_0 x_0) &= G_2(b_0 x_0) - b_0^p x_0^p A_1(b_0^2 x_0^2)^{\frac{p^2+p}{2}} A_2(b_0^2 x_0^2)^p A_3(b_0^2 x_0^2)^p \left[b_0^{p-5} f_1(x_0^2) \right]^p \\
&= b_0^{p^2} \tilde{F}_2(x_0) - b_0^p x_0^p B_1(x_0^2)^{\frac{p^2+p}{2}} \left[b_0^2 B_2(x_0^2) \right]^p \left[b_0^2 B_3(x_0^2) \right]^p \left[b_0^{p-5} f_1(x_0^2) \right]^p \\
&= b_0^{p^2} \left[F_2(x_0) - x_0^p B_1(x_0^2)^{\frac{p^2+p}{2}} B_2(x_0^2)^p B_3(x_0^2)^p f_1(x_0^2)^p \right] \\
&= b_0^{p^2} \tilde{F}_2(x_0),
\end{aligned}$$

which concludes the proof. □

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] L. Bitting and L. R. A. Finotti. Canonical liftings of edwards curves. To appear at the Acta Arithmetica. Available at `http://www.math.utk.edu/~finotti`, 2026.

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

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

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

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

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

[9] L. R. A. Finotti. Minimal degree liftings in characteristic 2. *J. Pure Appl. Algebra*, 207(3):631–673, 2006.

[10] L. R. A. Finotti. Computations with Witt vectors of length 3. *J. Théor. Nombres Bordeaux*, 23(2):417–454, 2011.

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

[12] J. Groves. *An Exploration of Absolute Minimal Degree Lifts of Hyperelliptic Curves*. PhD thesis, University of Tennessee, 2023.

[13] 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`.

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

[15] 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.

[16] 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`.

[17] 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