WEIERSTRASS COEFFICIENTS OF THE CANONICAL LIFTING

LUÍS R. A. FINOTTI

Abstract. Given an ordinary elliptic curve

$$E/\Bbbk \ : \ y_0^2 = x_0^3 + a_0x_0 + b_0$$

over a field of characteristic $p \geq 5$, there are functions $A_i(a_0, b_0)$ and $B_i(a_0, b_0)$ such that the curve

$$\boldsymbol{E}/\boldsymbol{W}(\Bbbk) \ : \ \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b},$$

where $\boldsymbol{a} = (a_0, A_1(a_0, b_0), A_2(a_0, b_0), \ldots)$ and $\boldsymbol{b} = (b_0, B_1(a_0, b_0), B_2(a_0, b_0), \ldots)$ is the canonical lifting of E. Although these functions are not uniquely determined, we prove that they can be taken to be in $\mathbb{F}_p(a_0, b_0)$, defined for all ordinary elliptic curves of the given characteristic and modular, with $\mathrm{wgt}(A_i) = 4p^i$ and $\mathrm{wgt}(B_i) = 6p^i$.

Preliminary Version
Last revised: December 10, 2015.

1. Introduction

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) if σ denotes the Frobenius of both $\Bbbk$ and $\boldsymbol{W}(\Bbbk)$, then the canonical lifting of E^σ (the elliptic curve obtained by applying σ to the coefficients of the equation that defines E) is $\boldsymbol{E}^\sigma$;
(3) τ is an injective group homomorphism and a section of the reduction modulo p, which we denote by π;

2000 *Mathematics Subject Classification.* Primary 11G07; Secondary 11F11.

Key words and phrases. elliptic curves, canonical lifting, Weierstrass coefficients, modular functions.

(4) 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

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

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 [Deu41] and then generalized to Abelian varieties by Serre and Tate in [LST64]. 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 [Sat00], coding theory, as in Voloch and Walker's [VW00], and counting torsion points of curves of genus $g \geq 2$, as in Poonen's [Poo01] or Voloch's [Vol97].

In [Fin13] we've studied the j-invariant of the canonical lifting $\boldsymbol{E}$. More precisely, there are functions J_i, for $i \in \{1, 2, \ldots\}$, such that if j_0 is the j-invariant of an *ordinary* elliptic curve, then

$$\boldsymbol{j} = (j_0, J_1(j_0), J_2(j_0), \ldots),$$

is the j-invariant of its canonical lifting. We describe in the reference above many of the properties of these functions J_i.

Here we will answer a similar question, but with respect to the *Weierstrass coefficients* of the canonical lifting. Before we make this more precise, let us introduce some terminology to simplify the exposition.

Definition 1.1. If K is a field of characteristic different 2 and 3, we refer to the elliptic curve given by the Weierstrass equation

$$E/K \ : \ y^2 = x^3 + ax + b, \tag{1.1}$$

simply as *the curve given by* (a, b). We shall implicitly assume that $\Delta \stackrel{\text{def}}{=} 4a^3 + 27b^2 \neq 0$, i.e., that the curve is non-singular.

We also need the following definition:

Definition 1.2. Let $\Bbbk$ be a field with $\mathrm{char}(\Bbbk) = p \geq 5$. We define

$$\Bbbk^2_{\text{ord}} \stackrel{\text{def}}{=} \{(a_0, b_0) \in \Bbbk^2 \ : \ 4a_0^3 + 27b_0^2 \neq 0 \text{ and the curve given by } (a_0, b_0) \text{ is } \textit{ordinary}\}.$$

So, let's fix some field $\Bbbk$ with $\mathrm{char}(\Bbbk) = p \geq 5$ and $(a_0, b_0) \in \Bbbk^2_{\mathrm{ord}}$. Then, the ordinary elliptic curve

$$E/\Bbbk \ : \ y_0^2 = x_0^3 + a_0 x_0 + b_0 \tag{1.2}$$

has a canonical lifting, say $\boldsymbol{E}$, given by some pair $(\boldsymbol{a}, \boldsymbol{b}) \in \boldsymbol{W}(\Bbbk)^2$, i.e., by

$$\boldsymbol{E}/\boldsymbol{W}(\Bbbk) \ : \ \boldsymbol{y}^2 = \boldsymbol{x}^2 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b}, \tag{1.3}$$

where $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$. Unlike with the j-invariant, the pair of Weierstrass coefficients (a_0, b_0) of E does not uniquely determine $(\boldsymbol{a}, \boldsymbol{b})$, as the canonical lifting is unique only up to isomorphism. But certainly there are (non-unique) functions

$$A_i : \Bbbk^2_{\mathrm{ord}} \to \Bbbk, \qquad B_i : \Bbbk^2_{\mathrm{ord}} \to \Bbbk, \qquad \text{for } i \in \{1, 2, 3, \ldots\}$$

such that, if $(a_0, b_0) \in \Bbbk^2_{\mathrm{ord}}$, then the curve given by $(\boldsymbol{a}, \boldsymbol{b}) \in \boldsymbol{W}(\Bbbk)^2$, where

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

is the canonical lifting of the (ordinary) curve given by (a_0, b_0). Our goal here, similarly to what was done for the j-invariants, is to describe these coordinate functions A_i and B_i.

2. Initial Problems

Clearly, since the functions A_i's and B_i's are not unique, our goal of describing them is not very precise. But, for instance, one might ask if all functions giving the Weierstrass coefficients of the canonical lifting, independently of the choices involved, have the same "nature". Or, one might ask if there are particular choices that make these functions "better" in some sense.

The question about the nature of these functions was first raised by a reviewer for one of the author's proposals to the NSA. In particular, the reviewer seemed, as far at the author could tell, to assume that these A_i's and B_i's would be modular functions, and then asked about their weights.

Thus, let us give the following definition:

Definition 2.1. Let $p \geq 5$ and $\mathbb{K} \stackrel{\text{def}}{=} \mathbb{F}_p(a_0, b_0)$, where a_0 and b_0 are indeterminates. Define their weights as $\mathrm{wgt}(a_0) \stackrel{\text{def}}{=} 4$ and $\mathrm{wgt}(b_0) \stackrel{\text{def}}{=} 6$ and

$$\mathcal{S}_n = \left\{ \frac{f}{g} \in \mathbb{K} \ : \ f, g \in \mathbb{F}_p[a_0, b_0] \text{ homogeneous, and } \mathrm{wgt}(f) - \mathrm{wgt}(g) = n \right\} \cup \{0\}.$$

Hence, in our context, $\mathcal{S}_n$ is the space of modular functions of weight n.

The author had posted some computations of these functions (back in 2000), and at the time of writing, these can be found at `http://www.math.utk.edu/~finotti/can_lifts/`. Here are a few examples. For $p = 5$, we have:

$$A_1 = (a_0^3 b_0^2 + b_0^4)/a_0, \tag{2.1}$$

$$B_1 = 4a_0^6 b_0 + a_0^3 b_0^3 + b_0^5, \tag{2.2}$$

and

$$\begin{aligned} A_2 = (&2a_0^{36} + a_0^{33} b_0^2 + a_0^{30} b_0^4 + 3a_0^{27} b_0^6 + 2a_0^{24} b_0^8 + a_0^{18} b_0^{12} \\ &+ 4a_0^{12} b_0^{16} + 3a_0^9 b_0^{18} + 4a_0^6 b_0^{20} + 4a_0^3 b_0^{22} + 4b_0^{24})/a_0^{11}, \\ B_2 = &a_0^{36} b_0 + 4a_0^{33} b_0^3 + 3a_0^{27} b_0^7 + 4a_0^{21} b_0^{11} + 4a_0^{15} b_0^{15} + a_0^{12} b_0^{17} + 3a_0^6 b_0^{21} + b_0^{25}. \end{aligned}$$

For $p = 7$, one has:

$$\begin{aligned} A_1 &= 5a_0^7 + 4a_0^4 b_0^2 + 4a_0 b_0^4, \\ B1 &= (3a_0^{12} + a_0^9 b_0^2 + 3a_0^6 b_0^4 + 5a_0^3 b_0^6 + 4b_0^8)/b_0, \end{aligned}$$

and

$$\begin{aligned} A_2 = (&6a_0^{61} + 5a_0^{58} b_0^2 + 6a_0^{55} b_0^4 + 4a_0^{52} b_0^6 + 3a_0^{43} b_0^{12} + 6a_0^{40} b_0^{14} + a_0^{37} b_0^{16} \\ &+ a_0^{34} b_0^{18} + 4a_0^{31} b_0^{20} + 2a_0^{28} b_0^{22} + 3a_0^{25} b_0^{24} + 6a_0^{19} b_0^{28} + a_0^{16} b_0^{30} \\ &+ 3a_0^{13} b_0^{32} + 6a_0^{10} b_0^{34} + 2a_0^4 b_0^{38} + 2a_0 b_0^{40})/b_0^8, \\ B_2 = (&5a_0^{96} + 4a_0^{93} b_0^2 + 5a_0^{90} b_0^4 + 6a_0^{87} b_0^6 + 4a_0^{84} b_0^8 + 3a_0^{81} b_0^{10} + 6a_0^{72} b_0^{16} \\ &+ 5a_0^{69} b_0^{18} + 5a_0^{66} b_0^{20} + 2a_0^{60} b_0^{24} + 3a_0^{57} b_0^{26} + a_0^{54} b_0^{28} + 2a_0^{51} b_0^{30} + 6a_0^{48} b_0^{32} \\ &+ 2a_0^{45} b_0^{34} + 6a_0^{42} b_0^{36} + 2a_0^{39} b_0^{38} + a_0^{33} b_0^{42} + 4a_0^{30} b_0^{44} + 5a_0^{27} b_0^{46} + 4a_0^{24} b_0^{48} \\ &+ a_0^{21} b_0^{50} + 3a_0^{18} b_0^{52} + 5a_0^{15} b_0^{54} + 5a_0^{12} b_0^{56} + 5a_0^9 b_0^{58} + 6a_0^6 b_0^{60} + 6a_0^3 b_0^{62})/b_0^{15}. \end{aligned}$$

These computations, as well as others for $p = 11, 13$, seem to indicate that indeed, A_i and B_i are modular functions of weights $4p^i$ and $6p^i$ respectively, i.e., $A_i \in \mathcal{S}_{4p^i}$ and $B_i \in \mathcal{S}_{6p^i}$.

Notice that we do have denominators in those formulas. In particular, A_i and B_i, for $i = 1, 2$, are not determined for $(0, b_0)$ (i.e., $j_0 = 0$) when $p = 5$, and for $(a_0, 0)$ (i.e., $j_0 = 1728$) when $p = 7$. But this is not really a problem, as these curves are *supersingular* (i.e., those pairs are not in $\mathbb{k}^2_{\text{ord}}$) and hence do not have canonical liftings. In fact, these are the *only* supersingular curves for their corresponding characteristic! This was to be expected, as it is similar to the fact that the functions J_i (that give the coordinates of

the j-invariant of the canonical lifting, as mentioned above) have poles for supersingular j-invariants.

We then introduce some more terminology:

Definition 2.2. The functions A_i's and B_i's are called *universal* if they are defined for all $(a_0, b_0) \in \mathbb{k}^2_{\text{ord}}$.

Hence, the functions given above, as well as the ones found in the author's web page for $p = 11, 13$, are all universal modular functions.

On the other hand, it is not true that either will be the case in general. For instance, for $p = 5$, we have that

$$A_1 \stackrel{\text{def}}{=} (a_0 + b_0^2)/b_0, \tag{2.3}$$

$$B_1 \stackrel{\text{def}}{=} (4a_0^{12}b_0 + a_0^9 b_0^3 + a_0^6 b_0^5 + a_0^3 b_0^7 + 4a_0^2 b_0^4 + 4a_0 b_0^6 + b_0^9)/a_0^6, \tag{2.4}$$

do yield the canonical lifting (modulo p^2), but A_1 is neither universal (as it is not defined for the ordinary curve given by $(1, 0)$) nor a modular function (as the numerator is not homogeneous). So, it is not true that *all possible* functions A_i's and B_i's (giving the canonical lifting) are necessarily modular or universal.

This is easy to see in general. If we have any pair of functions A_1 and B_1 such that $((a_0, A_1), (b_0, B_1))$ gives the canonical lifting of the curve given by (a_0, b_0), then so does the pair

$$((1, \lambda_1)^4(a_0, A_1), (1, \lambda_1)^6(b_0, B_1)) = ((a_0, A_1 + 4\lambda_1 a_0^p), (b_0, B_1 + 6\lambda_1 b_0^p)),$$

and hence the new functions

$$A_1' \stackrel{\text{def}}{=} A_1 + 4\lambda_1 a_0^p,$$

$$B_1' \stackrel{\text{def}}{=} B_1 + 6\lambda_1 b_0^p,$$

also give the canonical lifting, *for any choice of* λ_1. In fact formulas (2.3) and (2.4) can be obtained from Eqs. (2.1) and (2.2) with

$$\lambda_1 = (a_0^3 b_0^3 + 4a_0^2 + 4a_0 b_0^2 + b_0^5)/(a_0^6 b_0).$$

It should be clear that one can, in fact, make *any* choice for either A_1 or B_1.

But, we can prove the following theorem, which is the main goal of this paper:

Theorem 2.3. *There are universal modular functions $A_i \in \mathcal{S}_{4p^i}$ and $B_i \in \mathcal{S}_{6p^i}$, for $i \in \{1, 2, 3, \ldots\}$, such that if (a_0, b_0) gives an ordinary elliptic curve, then*

$$((a_0, A_1(a_0, b_0), A_2(a_0, b_0), \ldots), (b_0, B_1(a_0, b_0), B_2(a_0, b_0), \ldots))$$

gives its canonical lifting.

Note that, in particular, A_i's and B_i's are rational functions on a_0 and b_0. As we shall see in Section 5, the coefficients are in the prime field $\mathbb{F}_p$. Moreover, we shall describe in Section 8 how *all* functions with the "good" properties above, i.e., universal and modular, can be obtained.

The proof of Theorem 2.3 is quite elementary and is obtained from a computation using Voloch's algorithm to compute canonical liftings, described in Section 5. We prove universality in Section 7 and modularity in Section 8.

3. Witt Vectors and the Greenberg Transform

In this section we will briefly review some of the basic facts about Witt vectors. More details, including motivation and proofs, can be found in [Ser79] or [Jac84]. Let p be a prime and and for each non-negative integer n consider

$$W^{(n)}(X_0,\dots,X_n) \stackrel{\text{def}}{=} X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^nX_n, \tag{3.1}$$

the corresponding *Witt polynomial*. Then, there exist polynomials $S_i, P_i \in \mathbb{Z}[X_0,\dots,X_i,Y_0,\dots,Y_i]$ satisfying:

$$W^{(n)}(S_0,\dots,S_n) = W^{(n)}(X_0,\dots,X_n) + W^{(n)}(Y_0,\dots,Y_n) \tag{3.2}$$

and

$$W^{(n)}(P_0,\dots,P_n) = W^{(n)}(X_0,\dots,X_n)\cdot W^{(n)}(Y_0,\dots,Y_n). \tag{3.3}$$

More explicitly, we have the following recursive formulas:

$$S_n = (X_n+Y_n) + \frac{1}{p}(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p) + \cdots + \frac{1}{p^n}(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}) \tag{3.4}$$

and

$$\begin{aligned} P_n &= \frac{1}{p^n}\Big[(X_0^{p^n} + \cdots + p^nX_n)(Y_0^{p^n} + \cdots + p^nY_n) - \\ &\qquad \Big(P_0^{p^n} + \cdots + p^{n-1}P_{n-1}^p\Big)\Big] \\ &= (X_0^{p^n}Y_n + X_1^{p^{n-1}}Y_{n-1}^p + \cdots + X_nY_0^{p^n}) \\ &\quad + \frac{1}{p}(X_0^{p^n}Y_{n-1}^p + \cdots + X_{n-1}^pY_0^{p^n}) \\ &\quad \vdots \\ &\quad + \frac{1}{p^n}(X_0^{p^n}Y_0^{p^n}) - \frac{1}{p^n}P_0^{p^n} - \cdots - \frac{1}{p}P_{n-1}^p \\ &\quad + p\left(X_1^{p^{n-1}}Y_n + X_2^{p^{n-2}}(Y_{n-1}^p + pY_n) + \dots\right). \end{aligned} \tag{3.5}$$

(Note that despite the denominators in the formulas, cancellations yield polynomials with coefficients in $\mathbb{Z}$.)

We can then define sums and products of infinite vectors in $A^{\mathbb{Z}_{\geq 0}}$, where A is a commutative ring (with 1), say $\boldsymbol{a} = (a_0, a_1, \dots)$ and $\boldsymbol{b} = (b_0, b_1, \dots)$, by

$$\boldsymbol{a} + \boldsymbol{b} \stackrel{\text{def}}{=} (S_0(a_0, b_0), S_1(a_0, a_1, b_0, b_1), \dots)$$

and

$$\boldsymbol{a} \cdot \boldsymbol{b} \stackrel{\text{def}}{=} (P_0(a_0, b_0), P_1(a_0, a_1, b_0, b_1), \dots).$$

These operations make $A^{\mathbb{Z}_{\geq 0}}$ into a commutative ring (with 1) called the *ring of Witt vectors over* A and denoted by $\boldsymbol{W}(A)$.

Since we will deal with Witt vectors over fields of characteristic p, we may use $\bar{S}_n, \bar{P}_n \in \mathbb{F}_p[X_0, \dots, X_n, Y_0, \dots, Y_n]$, defined to be the reductions modulo p of S_n, P_n respectively, to define the addition and the product of Witt vectors.

First, observe that, if we let $\operatorname{wgt}(X_i) = \operatorname{wgt}(Y_i) = p^i$, then both S_n and P_n are homogeneous of weight p^n. This gives the following trivial lemma:

Lemma 3.1. *Let $\pi_i : \boldsymbol{W}(\Bbbk) \to \Bbbk$ denote the map that gives the i-the coordinate of a Witt vector. Then, if $\pi_i(\boldsymbol{f}) \in \mathcal{S}_{rp^i}$ and $\pi_i(\boldsymbol{g}) \in \mathcal{S}_{sp^i}$, then $\pi_i(\boldsymbol{f} \cdot \boldsymbol{g}) \in \mathcal{S}_{(r+s)p^i}$. If further $r = s$, then $\pi_i(\boldsymbol{f} + \boldsymbol{g}) \in \mathcal{S}_{rp^i}$.*

We now briefly review the definition of the Greenberg transform for two variables. (See also [Lan52] and [Gre61].)

Definition 3.2. Let $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$. If $\boldsymbol{x}_0 = (x_0, x_1, \dots), \boldsymbol{y}_0 = (y_0, y_1, \dots) \in \boldsymbol{W}(\Bbbk[x_0, y_0, x_1, y_1, \dots])$, then $\boldsymbol{f}(\boldsymbol{x}_0, \boldsymbol{y}_0) = (f_0, f_1, \dots) \in \boldsymbol{W}(\Bbbk[x_0, y_0, x_1, y_1, \dots])$ is the *Greenberg transform* of $\boldsymbol{f}$ and will be denoted by $G(\boldsymbol{f})$. (Note that $f_n \in \Bbbk[x_0, \dots, x_n, y_0, \dots, y_n]$.)

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 $G(\boldsymbol{f})$.

Note that we clearly have

$$G(\boldsymbol{x} + \boldsymbol{y}) = (\bar{S}_0, \bar{S}_1, \dots) \qquad \text{and} \qquad G(\boldsymbol{x} \cdot \boldsymbol{y}) = (\bar{P}_0, \bar{P}_1, \dots).$$

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

4. Properties of the Elliptic Teichmüller Lift

The most usual way to compute the canonical lifting is using the modular polynomial, as the lifting of the Frobenius gives an isogeny of degree p. On the other hand, Voloch developed and algorithm, later extended by the author, which computes the canonical lifting via its Weierstrass coefficients, and hence is a better approach to our problem.

The algorithm computes also the elliptic Teichmüller lift (described in Section 1), and uses the following results:

Theorem 4.1. *If τ is the elliptic Teichmüller lift for an ordinary elliptic curve over a field $\Bbbk$ of characteristic $p \geq 5$, then,*

$$\tau(x_0, y_0) = ((x_0, F_1, F_2, \ldots), (y_0, y_0H_1, y_0H_2, \ldots))$$

where $F_i, H_i \in \Bbbk[x_0]$,

$$\deg F_i \leq ((i+2)p^i - ip^{i-1})/2,$$
$$\deg H_i \leq ((i+3)p^i - ip^{i-1} - 3)/2,$$

and

$$F_i' = \mathfrak{H}^{-(p^i-1)/(p-1)}(x_0^3 + a_0x_0 + b_0)^{(p^i-1)/2} - x_0^{p^i-1} - \sum_{j=1}^{i-1} F_j^{p^{i-j}-1}F_j',$$

where $\mathfrak{H}$ is the Hasse Invariant *of the curve.*

The bounds for the degrees were proved in [Fin02] and the formula for the derivative was proved in [Fin04].

Remember that if

$$E/\Bbbk \ : \ y_0^2 = f(x_0) \stackrel{\text{def}}{=} x_0^3 + a_0x_0 + b_0,$$

then the Hasse invariant $\mathfrak{H}$ in the formula above is simply the coefficient of x_0^{p-1} from $f^{(p-1)/2}$, and the curve is ordinary if and only if $\mathfrak{H} \neq 0$. Hence, if we see a_0 and b_0 as the unknowns of the polynomial ring $\mathbb{F}_p[a_0, b_0]$, with $\operatorname{wgt}(a_0) = 4$ and $\operatorname{wgt}(b_0) = 6$ as before, then $\mathfrak{H}$ is a homogeneous polynomial of weight $(p-1)$.

Before we proceed to describe the algorithm, it is worth noting that when dealing with Witt vectors, we usually assume that the base field $\Bbbk$ is perfect. So, in principle, the coordinates of the Weierstrass coefficients of the canonical lifting, as well as the coefficients of elliptic Teichüller lift τ, might not be in $\mathbb{F}_p(a_0, b_0)$, but in its perfect closure. On the other hand, as observed in [Fin12], the algorithm we are about to describe proves that these can actually be taken in $\mathbb{F}_p(a_0, b_0)$ itself. We will also observe this consequence in our description of the algorithm below.

5. Voloch's Algorithm for Computing the Canonical Lifting

Let then $\Bbbk$ be a field, not necessarily perfect, of characteristic $p \geq 5$ and E be an ordinary elliptic curve given by $(a_0, b_0) \in \Bbbk^2_{\text{ord}}$, i.e., given by Eq. (1.2), and suppose its canonical lifting $\boldsymbol{E}$ is given by $(\boldsymbol{a}, \boldsymbol{b})$, i.e., given by Eq. (1.3), with $\boldsymbol{a} = (a_0, a_1, a_2, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, b_2, \ldots)$. Suppose we have computed the first n coordinates of $\boldsymbol{a}$, $\boldsymbol{b}$ and of the elliptic Teichmüller τ, and further that they are all defined over $\mathbb{F}_p(a_0, b_0)$. We then want to compute their $(n+1)$-th coordinates, i.e., we want a_n, b_n, F_n and H_n (with the notation of Theorem 4.1) and show that they are also defined over $\mathbb{F}_p(a_0, b_0)$. Since we don't require the field $\Bbbk$ to be perfect, we might as well assume that $\Bbbk = \mathbb{F}_p(a_0, b_0)$ through out this section. (In the proof of Theorem 2.3 we will take a_0 and b_0 to be *indeterminates*.)

Since $\tau(x_0, y_0)$ is a point of $\boldsymbol{E}$, it must satisfy the equation given by the $(n+1)$-th coordinate of the Greenberg transform. For simplicity, let again f denote the cubic from the Weierstrass equation of E, i.e., let $f \stackrel{\text{def}}{=} x_0^3 + a_0 x_0 + b_0$. Thus, this equation gives us:

$$2y_0^{p^n+1} H_n + \cdots = (f')^{p^n} F_n + a_n x_0^{p^n} + b_n + \cdots \tag{5.1}$$

where omitted terms do not involve any of the terms we are trying to compute, namely, a_n, b_n, F_n and H_n. This can be seen directly from the formulas for sums and products of Witt vectors in Section 3 or from the formula for the Greenberg transform given in Theorem 6.4 of [Fin14]. Clearly, by the induction hypothesis, the right hand side of is a polynomial in $\Bbbk[x_0]$. Also, observing that $y_0^2 = f(x_0)$ and using Lemma 5.1 from [Fin04], we have that Eq. (5.1) becomes

$$2f^{(p^n+1)/2} H_n + \cdots = (f')^{p^n} F_n + a_n x_0^{p^n} + b_n + \cdots \tag{5.2}$$

where *all* the omitted terms are in $\Bbbk[x_0]$. (The cited lemma guarantees that the powers of y_0 appearing on the left hand side are all even, and thus can be replaced by polynomials in x_0.)

Since we know F_n', we know some of the coefficients of F_n. Hence, if we let $\hat{F}_n$ be the formal integral of F_n, with no term having a zero derivative added, and

$$M \stackrel{\text{def}}{=} \begin{cases} ((n+2)p^{n-1} - np^{n-2})/2, & \text{if } n \geq 2, \\ 1, & \text{if } n = 1, \end{cases}$$

then

$$F_n = \hat{F}_n + \sum_{i=0}^{M} c_i x_0^{ip},$$

where the c_i's are unknown. Also, we shall let $N \stackrel{\text{def}}{=} ((n+3)p^n - np^{n-1} - 3)/2$ and

$$H_n = \sum_{i=0}^{N} d_i x_0^i,$$

where the d_i's are also unknown. (Note that, by Theorem 4.1, we have that $\deg F_n \leq pM$, if $n > 1$, and $\deg H_n \leq N$.) Collecting all the known terms of Eq. (5.2), all of which are in $\Bbbk[x_0]$, we get

$$2f^{(p^n+1)/2}\left(\sum_{i=0}^{N} d_i x_0^i\right) = (f')^{p^n}\left(\sum_{i=0}^{M} c_i x_0^{ip}\right) + a_n x_0^{p^n} + b_n + \cdots. \tag{5.3}$$

Now, comparing the coefficients of same degree (in x_0) in the equation above gives a *linear* system in the unknowns a_n, b_n, c_i's and d_i's, which we know has a solution, namely, the one given by the canonical lifting and the elliptic Teichmüller lift.

On the other hand, it is not true that any solution will give you the canonical lifting and the elliptic Teichmüller lift. A solution would guarantee only that we have *some* lifting of the elliptic curve with *some* lift of points, but nothing else.

To narrow the solution to the one we seek, we need one extra condition: we need that $\tau^*(\boldsymbol{x}/\boldsymbol{y})(O) = 0$, were O is the origin of E. (See the proof of Proposition 4.2 of [VW00].)

Hence we need the following lemma:

Lemma 5.1. *Let $\boldsymbol{x} = (x_0, x_1, \ldots), \boldsymbol{y} = (y_0, y_1, \ldots) \in \mathbb{F}_p(x_0, y_0, x_1, y_1, \ldots)$. Then, the $(n+1)$-th coordinate of $\boldsymbol{x}/\boldsymbol{y}$ as a Witt vector is of the form $z/y_0^{(n+1)p^n}$, where $z \in \mathbb{F}_p[x_0, \ldots, x_n y_0, \ldots, y_n]$.*

Proof. Firstly, observe that the group of units $\boldsymbol{W}(R)^\times$ of $\boldsymbol{W}(R)$, for some ring R, is simply the vectors with first entry in $R^\times$, and it is easy to check that the denominators of the coordinates of $\boldsymbol{y}^{-1}$ are powers of y_0.

By the formula for products of Witt vectors, i.e., Eq. (3.5), it suffices to show that the denominator for the $(n+1)$-th coordinate of $\boldsymbol{y}^{-1}$ is $y_0^{(n+1)p^n}$. Clearly, the first coordinate is $1/y_0$, and so we inductively assume that this is true up to the n-th coordinate. Write then:

$$\boldsymbol{y}^{-1} \equiv \left(\frac{Y_0}{y_0}, \frac{Y_1}{y_0^{2p}}, \frac{Y_2}{y_0^{3p^2}}, \ldots, \frac{Y_{n-1}}{y_0^{np^{n-1}}}, Z_n\right) \pmod{p^{n+1}},$$

where $Y_i \in \mathbb{F}_p[y_0, \ldots, y_i]$. Since

$$\boldsymbol{y} \cdot \boldsymbol{y}^{-1} = 1 = (1, 0, 0, \ldots),$$

comparing the $(n+1)$-th coordinates we get

$$Z_n y_0^{p^n} + \frac{Y_{n-1}^p}{y_0^{np^n}} + \cdots + \frac{Y_0^{p^n}}{y_0^{p^n}} y_n + \cdots = 0,$$

where the omitted terms have a denominator of at most $y_0^{(n-1)p^n}$, by the induction hypothesis and Eq. (3.5). Then, solving for Z_n in the above equation gives that its denominator is $y_0^{(n+1)p^n}$, as we wished to prove. □

So, still assuming that we have a_i, b_i, F_i and H_i for $i = 1, \ldots, (n-1)$ giving us the canonical lifting and elliptic Teichmüller lift (modulo p^n), we look at the $(n+1)$-th coordinate of $\tau^*(\boldsymbol{x}/\boldsymbol{y})$. By Lemma 5.1 above, we have that it is

$$\frac{F_n}{y_0^{p^n}} - \frac{y_0 H_n \cdot x_0^{p^n}}{y_0^{2p^n}} + \frac{1}{y_0^{(n+1)p^n}} \cdot [\cdots],$$

where the omitted terms are known and in $\Bbbk[x_0, y_0]$ (still assuming $\Bbbk = \mathbb{F}_p(a_0, b_0)$). Also, since τ is a lift of points, we have (by looking at the pull-back of the $(n+1)$-th coordinate of the Greenberg transform of $\boldsymbol{E}$ by τ)

$$2y_0^{p^n} y_0 H_n = (f')^{p^n} F_n + a_n x_0^{p^n} + b_n + \cdots$$

where, again, the omitted terms are known and in $\Bbbk[x_0, y_0]$. Hence, combining these two equations we have that $(n+1)$-the coordinate of $\tau^*(\boldsymbol{x}/\boldsymbol{y})$ is equal to

$$\left(\frac{1}{y_0^{p^n}} - \frac{x_0^{p^n}}{2y_0^{3p^n}} (f')^{p^n} \right) F_n - \frac{a_n x_0^{2p^n}}{2y_0^{3p^n}} - \frac{b_n}{2y_0^{3p^n}} + \frac{1}{y_0^{(n+1)p^n}} \cdot [\cdots]. \tag{5.4}$$

Remember that we are imposing the condition that $\tau^*(\boldsymbol{x}/\boldsymbol{y})(O) = 0$, and hence the expression above must have value 0 at O. What we need to do now is study how the choice of a_n, b_n and (the unknown coefficients of) F_n could make this happen. But, since the terms with a_n and b_n already have value 0 at O, this new condition won't give us any information about them directly.

Also, if we split $F_n = F_{n,1} + F_{n,2}$, where $F_{n,1}$ has all the terms of F_n with degrees greater than or equal to $(3p^n+1)/2$ and $F_{n,2}$ has all the terms of F_n with degrees less than or equal to $(3p^n-1)/2$, then the terms

$$\left(\frac{1}{y_0^{p^n}} - \frac{x_0^{p^n}}{2y_0^{3p^n}} (f')^{p^n} \right) F_{n,2}$$

also evaluate to 0 at O. Note that if $n = 1$, then $F_{n,1} = 0$, and we have that Eq. (5.4) already evaluates to 0 at O, and hence, we shall assume in what follows that $n \geq 2$. Remembering

that

$$F_n = \hat{F}_n + \sum_{i=0}^{M} c_i x_0^{ip},$$

where $\deg \hat{F}_n = (3p^n - 1)/2$, we have that

$$F_{n,1} = \sum_{i=M'+1}^{M} c_i x_0^{ip},$$

$$F_{n,2} = \hat{F}_n + \sum_{i=0}^{M'} c_i x_0^{ip},$$

where $M' \stackrel{\text{def}}{=} (3p^{n-1} - 1)/2$, and hence one can see that the only values that are determined by the extra condition are the c_i's for $i \geq M'$.

Now, using again that $y_0^2 = f(x_0)$, we can rewrite the Eq. (5.4) above as

$$\frac{1}{y_0^{(n+1)p^n}} \left[y_0^{(n-2)p^n} \left(f^{p^n} - \frac{x_0^{p^n}}{2} (f')^{p^n} \right) F_{n,1} + \mathcal{F} + y_0 \mathcal{G} \right] + \cdots, \tag{5.5}$$

where $\mathcal{F}, \mathcal{G} \in \Bbbk[x_0]$ and the omitted terms contain terms which already evaluate to 0 at O, such as the ones we've discussed above. The condition then imposes that the terms inside the bracket must have a pole of order less than $\left| \text{ord}_O \left(y_0^{(n+1)p^n} \right) \right| = 3(n+1)p^n$.

If n is even, let

$$\mathcal{H} \stackrel{\text{def}}{=} f^{(n-2)p^n/2} \left(f^{p^n} - \frac{x_0^{p^n}}{2} (f')^{p^n} \right),$$

and then Eq. (5.5) becomes

$$\frac{1}{y_0^{(n+1)p^n}} \left[\mathcal{H} F_{n,1} + \mathcal{F} + y_0 \mathcal{G} \right] + \cdots.$$

Since only $y_0\mathcal{G}$ involves y_0, its terms cannot cancel with any other terms inside the brackets, and hence we must have that $\text{ord}_O(y_0\mathcal{G}), \text{ord}_O(\mathcal{H}F_{n,1} + \mathcal{F}) > -3(n+1)p^n$, in particular the degree of $\mathcal{H}F_{n,1} + \mathcal{F}$, as a polynomial in x_0, must be less than $3(n+1)p^n/2$. Since $\deg \mathcal{H} = 3np^n/2$, this restriction on the degree $\mathcal{H}F_{n,1} + \mathcal{F}$ determines c_i for $i \in \{(3p^n + 3)/2, (3p^n + 5)/2, \ldots, M\}$. Therefore, in this case when n is even, the imposition that the solution must yield the canonical lifting and elliptic Teichmüller lift uniquely determines these coefficients, all of which can be found from the known previous coordinates, which appear in $\mathcal{F}$, and the restriction $\deg(\mathcal{H}F_{n,1} + \mathcal{F}) < 3(n+1)p^n/2$.

The case when n is odd is similar: let now

$$\mathcal{H} \stackrel{\text{def}}{=} f^{((n-2)p^n - 1)/2} \left(f^{p^n} - \frac{x_0^{p^n}}{2} (f')^{p^n} \right).$$

Then, Eq. (5.5) becomes

$$\frac{1}{y_0^{(n+1)p^n}}\left[y_0\mathcal{H}F_{n,1}+\mathcal{F}+y_0\mathcal{G}\right].$$

A similar analysis as the one above gives again c_i for $i\in\{(3p^n+3)/2,(3p^n+5)/2,\dots,M\}$ from the fact we need $\deg(\mathcal{H}F_{n,1}+\mathcal{G})<(3(n+1)p^n-3)/2$.

Therefore, the first step of the algorithm should be to determine these c_i's, which by our induction hypothesis will be in $\Bbbk=\mathbb{F}_p(a_0,b_0)$. Then, the system given by Eq. (5.3) has these terms determined, which then would also determine the d_i's for $i\in\{(4p^n-p-1)/2,(4p^n-p+1)/2,\dots,N\}$. So, we can collect these newly known terms with the other known terms, simplifying Eq. (5.3) to

$$2f^{(p^n+1)/2}\left(\sum_{i=0}^{N'}d_ix_0^i\right)=(f')^{p^n}\left(\sum_{i=0}^{M'}c_ix_0^{ip}\right)+a_nx_0^{p^n}+b_n+\cdots, \tag{5.6}$$

with $M'=(3p^{n-1}-1)/2$ (as above) and $N'\stackrel{\text{def}}{=}(4p^n-p-3)/2$ and all omitted terms known. Again this gives us a linear systems on the still unknown c_i's, d_i's, a_n and b_n.

Rather than solving this system directly, it seems computationally more efficient to impose that $2f^{(p^n+1)/2}$ divides the right hand side: performing the long division gives a remainder in terms of the c_i's, a_n and b_n and imposing that this remainder is zero gives a linear system on these unknowns. The system does not have a unique solution (as, again, the Weierstrass coefficients are not unique), but *any* solution indeed gives us Weierstrass coefficients of the canonical lifting. (And, of course, it also gives us the elliptic Teichmüller.)

On the other hand, for our theoretical purposes here, we will not take this approach and simply look at the system directly given by Eq. (5.6), to which we will often refer below.

Note that we know that the system has a solution, and since, by the induction hypothesis, the coefficients of the linear system are in $\Bbbk=\mathbb{F}_p(a_0,b_0)$, we have that there is a solution also in $\mathbb{F}_p(a_0,b_0)$.

6. Solutions of the System

In this section we study the solutions of the system given by Eq. (5.6), under the same assumptions as before: we assume a_i's, b_i's, F_i's and H_i's are known for $i<n$ and give the canonical lifting and elliptic Teichmüller lift (modulo p^n) and that c_i, for $i\in\{M'+1,\dots,M\}$, and d_i's, for $i\in\{N'+1,\dots,N\}$, were determine in order to guarantee that every solution gives Weierstrass coefficients of the canonical lifting and its associate elliptic Teichmüller lift.

Suppose then that we have two solutions, say

$$(a_n, b_n, c_0, \ldots, c_{M'}, d_0, \ldots, d_{N'}) \quad \text{and} \quad (a'_n, b'_n, c'_0, \ldots, c'_{M'}, d'_0, \ldots, d'_{N'}).$$

Then, since both solutions give the canonical lifting, there is $\boldsymbol{\lambda} \in \boldsymbol{W}_{n+1}(\Bbbk)$, where $\boldsymbol{W}_k$ denote the ring of Witt vectors of length k (i.e., the reduction modulo p^k of the ring of Witt vectors), such that:

$$(a_0, \ldots, a_{n-1}, a'_n) = \boldsymbol{\lambda}^4(a_0, \ldots, a_{n-1}, a_n),$$
$$(b_0, \ldots, b_{n-1}, b'_n) = \boldsymbol{\lambda}^6(b_0, \ldots, b_{n-1}, b_n).$$

Since

$$\boldsymbol{\lambda}^4 \equiv \boldsymbol{\lambda}^6 \equiv 1 \pmod{p^n},$$

we have that $\boldsymbol{\lambda} \equiv \pm 1 \pmod{p^n}$. We can assume that $\boldsymbol{\lambda} \equiv 1 \pmod{p^n}$, i.e.,

$$\boldsymbol{\lambda} = (1, 0, \ldots, 0, \lambda)$$

for some λ in $\Bbbk$ (or in some extension of $\Bbbk$). Hence, this gives us that

$$a'_n = a_n + 4\lambda a_0^{p^n},$$
$$b'_n = b_n + 6\lambda b_0^{p^n}.$$

If we subtract Eq. (5.6) from the same equation for the second solution (i.e., $(a'_n, b'_n, \ldots)$), we get

$$2f^{(p^n+1)/2}\left(\sum_{i=0}^{N'}(d'_i - d_i)x_0^i\right) = (3x_0^2 + a_0)^{p^n}\left(\sum_{i=0}^{M'}(c'_i - c_i)x_0^{ip}\right) + 4\lambda a_0^{p^n}x_0^{p^n} + 6\lambda b_0^{p^n}. \quad (6.1)$$

Since the elliptic Teichmüller is uniquely determined by the Weierstrass coefficients, there is a unique solution for c'_i's and d'_i's in terms of the c_i's, d_i's and λ.

By taking:

$$c'_i = \begin{cases} c_i, & \text{if } i \neq p^{n-1}, \\ 2\lambda + c_i, & \text{if } i = p^{n-1}, \end{cases}$$

Eq. (6.1) becomes

$$2f^{(p^n+1)/2}\left(\sum_{i=0}^{N'}(d'_i - d_i)x_0^i\right) = 6\lambda f^{p^n}.$$

Hence, if we define d'_i via:

$$\sum_{i=0}^{N'} d'_i x_0^i = \left(\sum_{i=0}^{N'} d_i x_0^i\right) + 3\lambda f^{(p^n-1)/2}$$

we find the these choices for the c'_i's and d'_i's satisfy Eq. (6.1), and so, by uniqueness, these give the elliptic Teichmüller lifts for the curve given by $a'_n = a_n + 4\lambda a_0^{p^n}$ and $b'_n = b_n + 6\lambda b_0^{p^n}$.

This shows that the nullspace of the coefficient matrix of the system given by Eq (5.6) has dimension 1, generated by $(4a_0^{p^n}, 6b_0^{p^n}, 0, \ldots, 0, 2, 0, \ldots, 0, 3, \ldots)$, where 2 appears in the coordinate corresponding to $c_{p^{n-1}}$. In particular, *all c_i's, for $i \neq p^{n-1}$, are the same for every choice a_n and b_n (that gives the canonical lifting)*!

Note that this means that the "choice" we have when finding the canonical lifting and elliptic Teichmüller lift, is a choice of the value for either $c_{p^{n-1}}$, a_n or b_n.

7. Universality

In this section we will prove that there are universally defined functions A_i's and B_i's. So, we are back in the situation where we want general formulas, and hence we shall take $\Bbbk \stackrel{\text{def}}{=} \mathbb{F}_p(a_0, b_0)$, where a_0 and b_0 are indeterminates. In order for our solutions to be universal, the denominators cannot vanish for any ordinary elliptic curve, i.e., they have to be products of powers of factors of the discriminant Δ or of the Hasse invariant $\mathfrak{H}$. So, we want $A_i, B_i \in R$, where R is the localization of $\mathbb{F}_p[a_0, b_0]$ at $\{(\Delta \cdot \mathfrak{H})^i \,:\, i \in \{0, 1, 2, \ldots\}\}$.

We will, again, proceed by induction. We assume then that we have computed the canonical lifting and elliptic Teichmüller lift of

$$E/\Bbbk \,:\, y_0^2 = x_0^3 + a_0 x_0 + b_0$$

up to the n-the coordinate, with $a_i, b_i \in R$ and $F_i, H_i \in R[x_0]$. Note that, since we are taking a_0 and b_0 as indeterminates, we clearly have $a_i = A_i$ and $b_i = B_i$. We need then to prove that there are $a_n, b_n \in R$ which give the canonical lifting modulo p^{n+1}.

First, observe that all the omitted terms of Eq. (5.6) are in R. For most of them this follows from the induction hypothesis. But also the terms in $\hat{F}_n$ are in R by the induction hypothesis and the formula for F'_n (in Theorem 4.1). Moreover, the c_i's, for $i \in \{M' + 1, \ldots, M\}$ are in R, by the induction hypothesis and the algorithm described in Section 5, as they are chosen so that $\deg(\mathcal{H}F_n + \mathcal{F}) < 3(n+1)p^n/2$ (for some polynomials in $\mathcal{F}, \mathcal{H} \in R[x_0]$) when n is even, or $\deg(\mathcal{H}F_n + \mathcal{G}) < (3(n+1)p^n - 3)/2$ (for some polynomials $\mathcal{G}, \mathcal{H} \in R[x_0]$) if n is odd, and in both cases the leading coefficient of $\mathcal{H}$ is in $\mathbb{F}_p$. Finally, the d_i's for $i \in \{N' + 1, \ldots, N\}$ are also in R by Eq. (5.3). (Note that the only new denominator

introduced is in fact a power of $\mathfrak{H}$ in $\hat{F}_n$. No power of Δ is directly introduced in the denominator.)

Now, from our analysis of the solutions of the system given by Eq. (5.6) in Section 6, we know that all c_i's, for $i \leq M'$, expect for $c_{p^{n-1}}$ are universal, so they are all in R. (Here is where the denominator Δ could conceivably appear.) Also, as then observed, we may choose the value of $c_{p^{n-1}}$, and *we will now choose it to be zero*, and hence also in R. Since the general solution to the system had only one free parameter (also observed in Section 6), with this choice the solution is unique.

Now, by comparing the terms of degrees (in x_0) from $(7p^n - p)/2$ down to $(3p^n + 3)/2$ in Eq. (5.6), we get a system of the form:

$$\begin{array}{c} \begin{array}{ccccccccccc} d_{N'} & d_{N'-1} & d_{N'-2} & \cdots & d_0 & c_{M'} & \cdots & c_0 & a_n & b_n & \end{array} \\ \begin{pmatrix} 3 & 0 & 0 & \cdots & 0 & * & \cdots & * & 0 & 0 \\ * & 3 & 0 & \cdots & 0 & * & \cdots & * & 0 & 0 \\ * & * & 3 & \cdots & 0 & * & \cdots & * & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ * & * & * & \cdots & 3 & * & \cdots & * & 0 & 0 \end{pmatrix} \end{array} = \begin{pmatrix} * \\ * \\ * \\ \vdots \\ * \end{pmatrix}$$

where all "$*$" entries are in R. So, also $d_i \in R$ for all i.

Finally, now looking at terms of degrees p^n and 0 in Eq. (5.6), we can see that also $a_n, b_n \in R$, proving the universality of A_n and B_n when choosing $c_{p^{n-1}} = 0$.

8. Modularity

In this section we prove that, with the choice of $c_{p^{n-1}} = 0$ as above, that the functions obtained satisfy $A_n \in \mathcal{S}_{4p^n}$ and $B_n \in \mathcal{S}_{6p^n}$. For the sake of exposition, we shall extended the definition of $\mathcal{S}_n$. First, let $\operatorname{wgt}(x_0) \stackrel{\text{def}}{=} 2$ and $\operatorname{wgt}(y_0) \stackrel{\text{def}}{=} 3$, while still assuming that $\operatorname{wgt}(a_0) = 4$ and $\operatorname{wgt}(b_0) = 6$, so that y_0^2 and $x_0^2 + a_0x_0 + b_0$ are both homogeneous of weight 6. Then, define:

$$\mathcal{S}_n = \left\{ \frac{f}{g} \in \Bbbk \ : \ f, g \in \mathbb{F}_p[a_0, b_0, x_0, y_0] \text{ homogeneous and } \operatorname{wgt}(f) - \operatorname{wgt}(g) = n \right\} \cup \{0\}.$$

We again use induction assuming that, for $i < n$, we have that $F_i \in \mathcal{S}_{2p^i}$, $y_0H_i \in \mathcal{S}_{3p^i}$, $A_i \in \mathcal{S}_{4p^i}$ and $B_i \in \mathcal{S}_{6p^i}$.

By Lemma 3.1, we have that the omitted terms in Eq. (5.1) (or Eq. (5.2)) are all in $\mathcal{S}_{6p^n}$. It's also easy to check that $\hat{F}_n = F_n - \sum_{i=0}^{M} c_i x_0^{ip}$ (i.e., the formal integral for the formula of the derivative of F_n) is in $\mathcal{S}_{2p^n}$, by Theorem 4.1. Thus, all omitted terms of Eq. (5.3) are also in $\mathcal{S}_{6p^n}$.

Also, again by Lemma 3.1, we have that all the terms in the n-th coordinate of $\tau^*(\boldsymbol{x}/\boldsymbol{y})$, except for those involving F_n, are in $\mathcal{S}_{-p^n}$, and hence the terms $\mathcal{F}+y_0\mathcal{G}$ inside the brackets in Eq. (5.5) are in $\mathcal{S}_{(3n+2)p^n}$. This implies that $F_{n,1} = \sum_{i=M'+1}^{M} c_i x_0^{ip} \in \mathcal{S}_{2p^n}$. Then, Eq. (5.3), by equating degrees, gives us that $\sum_{i=N'+1}^{N} d_i x_0^i \in \mathcal{S}_{3p^n}$. So, all of the omitted terms of Eq. (5.6) are in $\mathcal{S}_{6p^n}$.

Remember we have chosen $c_{p^{n-1}} = 0$, and hence the solution for the system given by Eq (5.6) is unique. Moreover, as observed in the Section 6, the denominators of c_i's, d_i's, a_n and b_n that give the solution can be taken as powers of $\Delta \cdot \mathfrak{H}$, and hence are *homogeneous* polynomials on a_0, b_0. So, we can split the terms of the solution, by splitting the numerator in its homogeneous terms, as:

$$\begin{aligned} a_n &= a_{n,0} + a_{n,1} \\ b_n &= b_{n,0} + b_{n,1} \\ c_i &= c_{i,0} + c_{i,1} \\ d_i &= d_{i,0} + d_{i,1} \end{aligned}$$

where

$$\begin{aligned} a_{n,0} &\in \mathcal{S}_{4p^n}, \text{ and no term on } a_{n,1} \text{ is in } \mathcal{S}_{4p^n}, \\ b_{n,0} &\in \mathcal{S}_{6p^n}, \text{ and no term on } b_{n,1} \text{ is in } \mathcal{S}_{6p^n}, \\ c_{i,0} &\in \mathcal{S}_{4p^n-2ip}, \text{ and no term on } c_{i,1} \text{ is in } \mathcal{S}_{4p^n-2ip}, \\ d_{i,0} &\in \mathcal{S}_{3p^n-2i-3}, \text{ and no term on } d_{i,1} \text{ is in } \mathcal{S}_{3p^n-2i-3}. \end{aligned}$$

This way, we have, by Eq. (5.6), that

$$2f^{(p^n+1)/2}\left(\sum_{i=0}^{N'} d_{i,0}x_0^i\right) = (f')^{p^n}\left(\sum_{i=0}^{M'} c_{i,0}x_0^{ip}\right) + a_{n,0}x_0^{p^n} + b_{n,0} + \cdots, \tag{8.1}$$

with the same omitted terms as in Eq. (5.6), and that

$$2f^{(p^n+1)/2}\left(\sum_{i=0}^{N'} d_{i,1}x_0^i\right) = (f')^{p^n}\left(\sum_{i=0}^{M'} c_{i,1}x_0^{ip}\right) + a_{n,1}x_0^{p^n} + b_{n,1}. \tag{8.2}$$

Thus, the $a_{n,0}$, $b_{n,0}$, $c_{i,0}$'s and $d_{i,0}$'s give a solution of Eq. (5.6), but since the solution is unique (since we are taking $c_{p^{n-1}} = 0$), we must have that $a_n = a_{n,0}$, $b_n = b_{n.0}$, $c_i = c_{i,0}$ and $d_i = d_{i,0}$. Hence, $F_n \in \mathcal{S}_{2p^n}$, $y_0H_n \in \mathcal{S}_{3p^n}$, $A_n = a_n \in \mathcal{S}_{4p^n}$ and $B_i = b_n \in \mathcal{S}_{6p^n}$, which is what we needed to prove.

Finally, recall from Section 6 that any other solution is given by

$$A'_n = A_n + 4\lambda a_0^{p^n}, \tag{8.3}$$

$$B'_n = B_n + 6\lambda b_0^{p^n}. \tag{8.4}$$

Thus, if we want to preserve the weights, we must choose $\lambda \in \mathcal{S}_0$. If we want to keep it universal, we must choose $\lambda \in R$, and hence all possible A_n's and B_n's satisfying Theorem 2.3 come from choosing $\lambda \in R \cap \mathcal{S}_0$ in Eqs. (8.3) and (8.4) (with A_n and B_n the ones obtained with $c_{p^{n-1}} = 0$), or, equivalently, from choosing $c_{p^{n-1}} \in R \cap \mathcal{S}_0$ when solving the system given by Eq. (5.6).

9. Final Observations

First, we would like to observe that if the A_i's and B_i's are modular functions, then they must be of weights $4p^i$ and $6p^i$, respectively. If $4a_0^{p^n} B_n \neq 6b_0^{p^n} A_n$, where A_n and B_n are the modular functions obtained when $c_{p^{n-1}}$ is chosen to be zero as above, then one can use Eqs. (8.3) and (8.4) to prove that every other pair of modular functions A'_n and B'_n (also giving the canonical lifting) would have weights $4p^n$ and $6p^n$ respectively. But, this restriction (that $4a_0^{p^n} B_n \neq 6b_0^{p^n} A_n$) is not necessary, as we shall see below.

Before we proceed, though, observe that if the functions $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ are chosen (giving the canonical lifting), then given $\lambda_0 \in \Bbbk$, there must be some $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_n) \in \boldsymbol{W}_{n+1}(\Bbbk)$ such that:

$$(\lambda_0^4 a_0, A_1(\lambda_0^4 a_0, \lambda_0^6 b_0), \ldots, A_n(\lambda_0^4 a_0, \lambda_0^6 b_0)) = \boldsymbol{\lambda}^4(a_0, A_1(a_0, b_0), \ldots, A_n(a_0, b_0)) \tag{9.1}$$

$$(\lambda_0^6 b_0, B_1(\lambda_0^4 a_0, \lambda_0^6 b_0), \ldots, B_n(\lambda_0^4 a_0, \lambda_0^6 b_0)) = \boldsymbol{\lambda}^6(b_0, B_1(a_0, b_0), \ldots, B_n(a_0, b_0)), \tag{9.2}$$

since the canonical liftings of isomorphic elliptic curves are isomorphic. Clearly, $\lambda_1, \ldots, \lambda_n$ are functions of λ_0. We shall prove, at the same time, that if the A_i's and B_i's are modular, then their weights are $4p^n$ and $6p^n$, respectively, and in this case we also must have $\lambda_i = 0$ for $i > 0$, and hence $\boldsymbol{\lambda}$ is simply the Teichmüller lift of λ_0.

Once more, we proceed by induction. So, assume that for $i < n$ we have $A_i \in \mathcal{S}_{4p^i}$, $B_i \in \mathcal{S}_{6p^i}$ and $\lambda_1 = \cdots = \lambda_{n-1} = 0$, and suppose that A_n and B_n are modular. Say, $A_n \in \mathcal{S}_k$, for some k.

We have, from Eq. (9.1), with $\lambda_1 = \cdots = \lambda_{n-1} = 0$, that

$$\lambda_0^k A_n(a_0, b_0) = A_n(\lambda_0^4 a_0, \lambda_0^6 b_0) = \lambda_0^{4p^n} A_n(a_0, b_0) + 4\lambda_0^{3p^n} \lambda_n a_0^{p^n},$$

and so

$$4\lambda_0^{3p^n} \lambda_n a_0^{p^n} = (\lambda_0^k - \lambda_0^{4p^n}) A_n(a_0, b_0).$$

Since the left hand side is in $\mathcal{S}_{4p^n}$ and the right hand side is in $\mathcal{S}_k$, we must have $k = 4p^n$, unless either side is zero. In any case, the right hand side must be zero and so $\lambda_n = 0$, which also gives that either $k = 4p^n$ or $A_n = 0$, and so $A_n \in \mathcal{S}_{4p^n}$.

Also, again since $\lambda_n = 0$, Eq. (9.2) now gives us

$$B_n(\lambda_0^4 a_0, \lambda_0^6 b_0) = \lambda_0^{6p^n} B_n(a_0, b_0),$$

and hence $B_n \in \mathcal{S}_{6p^n}$.

It is also worth mentioning that, although we stated that the universal functions A_i's and B_i's, obtained by setting $c_{p^n-1} = 0$, as done above, might have powers of factors of the discriminant Δ in their denominator, this has not happened for any concrete example computed so far. The formula for F_n' clearly shows where powers of the Hasse invariant are introduced, but we never introduce a denominator of Δ directly. On the other hand, when solving the system given by Eq. (5.6), the determinant of the coefficient matrix can introduce new denominators, and indeed, in some cases it does introduce extra powers of $\mathfrak{H}$. Since the data is limited, as the computations involved are quite demanding, it is hard to know for sure. Although I have not been able to see an easy proof that only $\mathfrak{H}$ appears in the denominator, that would be my guess, but I would be reluctant to call it a conjecture at this point.

Finally, one might ask what powers of $\mathfrak{H}$ appear in the denominators. Again the difficulty with our current approach is understanding the determinant of the coefficient matrix of our system. By making connections with the lifting of the j-invariant (which was discussed in [Fin10], [Fin12] and [Fin13]), it seems that one could prove that either A_n or B_n has a power of $\hat{\mathfrak{H}}$ of at least $np^{n-1} + (n-1)p^{n-2}$, where $\hat{\mathfrak{H}}$ is $\mathfrak{H}$ divided by the largest powers of a_0 and b_0 that divide it. But this doesn't seem to be very useful, as in all examples so far, $\mathfrak{H}$ itself appears, not $\hat{\mathfrak{H}}$, and the power can be larger that this bound. E.g., for $p = 5$, we have that the denominator of A_3 is $\mathfrak{H}^{100} = a_0^{100}$, while $3 \cdot 5^2 + 2 \cdot 5 = 85$. So, one power of $\hat{\mathfrak{H}}$ (or $\mathfrak{H}$ itself) in the denominator of either A_n or B_n has a lower bound, but we have no upper bound for it, nor any bound whatever for the power appearing on the other denominator.

This fact that $\mathfrak{H}$ itself appears instead of $\hat{\mathfrak{H}}$ is a contrast with the lifts of the j-invariant, where *pseudo-canonical liftings* can occur. (See [Fin12].) For example, the formula for the j-invariant of the canonical lifting in characteristic 5 is

$$\boldsymbol{j} = \left(j_0, 3j_0^3 + j_0^4, \ldots\right).$$

So, modulo p^2, there is no denominator in the formula for the second coordinate, and hence it is defined even for the supersingular elliptic curve given by $j_0 = 0$. (The same is true for

the third coordinate, but not for the fourth.) Hence, one might expect that, in similar way, with some choice of A_1 and B_1, again for $p = 5$, these would be defined for $a_0 = 0$, even though it yields a supersingular elliptic curve. But, from our analysis above, this is not the case. So, while for $p = 5$ the formulas for the j-invariant can yield pseudo-canonical liftings, i.e., liftings of supersingular elliptic curves given by the formulas that give the canonical lifting, the formulas for the Weierstrass coefficients do *not*.

Competing Interests. The author declares that he has no competing interests.

Acknowledgment. The author would like to thank F. Voloch and S. Mulay for the invaluable discussions on the subject of this paper. Also, the computations mentioned were done with MAGMA.

References

[Deu41] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenköper. *Abh. Math. Sem. Univ. Hamburg*, 14:197–272, 1941.

[Fin02] L. R. A. Finotti. Degrees of the elliptic Teichmüller lift. *J. Number Theory*, 95(2):123–141, 2002.

[Fin04] L. R. A. Finotti. Minimal degree liftings of hyperelliptic curves. *J. Math. Sci. Univ. Tokyo*, 11(1):1–47, 2004.

[Fin10] L. R. A. Finotti. Lifting the j-invariant: Questions of Mazur and Tate. *J. Number Theory*, 130(3):620 – 638, 2010.

[Fin12] L. R. A. Finotti. Nonexistence of pseudo-canonical liftings. *Int. J. Number Theory*, 8(1):31–51, 2012.

[Fin13] L. R. A. Finotti. Coordinates of the j-invariant of the canonical lifting. *Funct. Approx. Comment. Math.*, 49(1):57–72, 2013.

[Fin14] L. R. A. Finotti. Computations with Witt vectors and the Greenberg transform. *Int. J. Number Theory*, 10(6):1431–1458, 2014.

[Gre61] M. J. Greenberg. Schemata over local rings. *Ann. of Math. (2)*, 73:624–648, 1961.

[Jac84] N. Jacobson. *Basic Algebra*, volume 2. W. H. Freeman and Company, second edition, 1984.

[Lan52] S. Lang. On quasi algebraic closure. *Ann. of Math. (2)*, 55:373–390, 1952.

[LST64] 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`.

[Poo01] B. Poonen. Computing torsion points on curves. *Experiment. Math.*, 10(3):449–465, 2001.

[Sat00] 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.

[Ser79] J-P. Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

[Vol97] 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`.

[VW00] 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
E-mail address: finotti@math.utk.edu