WEIERSTRASS COEFFICIENTS OF THE CANONICAL LIFTING

LUÍS R. A. FINOTTI

Abstract. Given an ordinary elliptic curve

$$E/\mathbb{k} \;:\; y_0^2 = x_0^3 + a_0x_0 + b_0$$

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

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

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 $\mathrm{wgt}(B_i) = 6p^i$.

1. Introduction

Let $\mathbb{k}$ be a perfect field of characteristic $p > 0$. Associated to an *ordinary* elliptic curve E over $\mathbb{k}$, there exists a unique (up to isomorphisms) elliptic curve $\boldsymbol{E}$ over $\boldsymbol{W}(\mathbb{k})$, the ring of Witt vectors over $\mathbb{k}$, called the *canonical lifting* of E, and a map $\tau : E(\bar{\mathbb{k}}) \to \boldsymbol{E}(\boldsymbol{W}(\bar{\mathbb{k}}))$, 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 $\mathbb{k}$ and $\boldsymbol{W}(\mathbb{k})$, 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;

(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

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

2000 *Mathematics Subject Classification.* Primary 11G07; Secondary 11F03.

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

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 (as a Witt vector). 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 $\mathbb{k}$ is a field of characteristic different from 2 and 3, we refer to the elliptic curve given by the Weierstrass equation

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

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

We also need the following definition:

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

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

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

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

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

$$\boldsymbol{E}/\boldsymbol{W}(\mathbb{k}) \; : \; \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b}, \tag{1.3}$$

where $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$. Note that we are requiring that the reduction modulo p of $\boldsymbol{a}$ and $\boldsymbol{b}$ are a_0 and b_0 respectively, and therefore $\boldsymbol{E}$ reduces to E. 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

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

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

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

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 in [Fin13], is to describe these Witt vector components A_i and B_i of the Weierstrass coefficients of the canonical lifting as functions on a_0, b_0.

2. Choices of A_i and B_i

Clearly, since the functions A_i's and B_i's are not unique, our goal of describing them is not very precise. So, let's start with some observations about the possible choices that can be made.

First, suppose that we've obtained the canonical liftings with $\boldsymbol{a} = (a_0, a_1)$ and $\boldsymbol{b} = (b_0, b_1)$, with $a_1 = A_1(a_0, b_0)$ and $b_1 = B_1(a_0, b_0)$ for some choice of A_1 and B_1. Then, for any $\boldsymbol{\lambda} \in \boldsymbol{W}_2(\Bbbk)$, we have that the elliptic curve given by $(\boldsymbol{\lambda}^4 \cdot \boldsymbol{a}, \boldsymbol{\lambda}^6 \cdot \boldsymbol{b})$ is also the canonical lifting. To make sure the canonical lifting reduces to the original curve modulo p, we might take $\boldsymbol{\lambda} = (1, \lambda_1)$ for some $\lambda_1 \in \Bbbk$ (or in some extension of $\Bbbk$). In this case:

$$\begin{aligned} (1, \lambda_1)^4 \cdot (a_0, a_1) &= (a_0, a_1 + 4\lambda_1 a_0^p) \\ (1, \lambda_1)^6 \cdot (b_0, b_1) &= (b_0, b_1 + 6\lambda_1 b_0^p) \end{aligned}$$

Hence, if $a_0 \neq 0$ (i.e., $j_0 \neq 0$), then we can make $A_1(a_0, b_0)$ be *any* function, making then the choice of $B_1(a_0, b_0)$ uniquely determined. Or, similarly, if $b_0 \neq 0$ (i.e., $j_0 \neq 1728$), then we can choose $B_1(a_0, b_0)$ to be any function.

Here are some examples: let $p = 5$. Then, since an elliptic curve in characteristic 5 is supersingular if and only if $j_0 = 0$ (i.e., $a_0 = 0$), we must have $a_0 \neq 0$. As observed above, this allows us to choose $A_1(a_0, b_0)$ at will. The rows of Table 2.1 show the more or less arbitrary choices of $A_1 = 0$ and $A_1 = a_0$ with their corresponding functions B_1. (We will later described a method that allows us to compute these functions.)

On the other hand, when $p = 13$ we cannot guarantee that either a_0 or b_0 is different from zero, as $j_0 = 5 \neq 0, 1728$ is the only supersingular value, and hence $a_0 = 0$ and $b_0 = 0$

TABLE 2.1. Some possible functions A_1 and B_1 for $p = 5$.

A_1	B_1
0	$(4a_0^{12}b_0 + a_0^9b_0^3 + a_0^6b_0^5 + a_0^3b_0^7 + b_0^9)/a_0^6$
a_0	$(4a_0^{12}b_0 + a_0^9b_0^3 + a_0^6b_0^5 + a_0^3b_0^7 + 4a_0^2b_0^5 + b_0^9)/a_0^6$

TABLE 2.2. Some possible functions A_1 and B_1 for $p = 13$.

A_1	B_1
0	$(4a_0^{33}b_0 + 5a_0^{30}b_0^3 + 11a_0^{27}b_0^5 + 4a_0^{24}b_0^7+$ $4a_0^{21}b_0^9 + 12a_0^{18}b_0^{11} + 4a_0^{15}b_0^{13} + 5a_0^{12}b_0^{15}+$ $5a_0^9b_0^{17} + 7a_0^6b_0^{19} + 7a_0^3b_0^{21} + 5b_0^{23})/(a_0^{15} + 4a_0^{12}b_0^2)$
$(6a_0^{34} + a_0^{31}b_0^2 + 10a_0^{28}b_0^4 + 6a_0^{25}b_0^6+$ $6a_0^{22}b_0^8 + 5a_0^{19}b_0^{10} + 6a_0^{16}b_0^{12} + a_0^{13}b_0^{14}+$ $a_0^{10}b_0^{16} + 4a_0^7b_0^{18} + 4a_0^4b_0^{20} + a_0b_0^{22})/(a_0^3b_0^{12} + 4b_0^{14})$	0

both give ordinary elliptic curves. One could still "force", using the algorithm we describe later on, that either $A_1 = 0$ or $B_1 = 0$ (or any other choice). The rows of Table 2.2 give the corresponding A_1 and B_1 for these particular choices.

But, this brings up a problem: the formula for B_1 in the first row of Table 2.2 (with $A_1 = 0$) does not work for the *ordinary* elliptic curve given by $(a_0, b_0) = (0, 1)$, while the formula for A_1 in the second row (with $B_1 = 0$) does now work for the *ordinary* elliptic curve given by $(a_0, b_0) = (1, 0)$. So, these formulas work in particular cases, but are not *universal*, i.e., they don't work (individually) for *all* $(a_0, b_0) \in \Bbbk^2_{\text{ord}}$.

This lead us to the following definition:

Definition 2.1. The functions A_i's and B_i's are called *universal* if they are defined for all $(a_0, b_0) \in \Bbbk^2_{\text{ord}}$.

Since we can compute the canonical liftings via the j-invariants (see [Fin13], for instance), another approach would be to use the fact that if $\boldsymbol{j}$ is the j-invariant of the canonical lifting, then, if $\boldsymbol{j} \neq 0, 1728$, we have that

$$\boldsymbol{y}^2 = \boldsymbol{x}^3 + \frac{27\boldsymbol{j}}{4(1728 - \boldsymbol{j})}\boldsymbol{x} + \frac{27\boldsymbol{j}}{4(1728 - \boldsymbol{j})} \tag{2.1}$$

is an equation for the canonical lifting. On the other hand, this equation does not reduce to $y_0^2 = x_0^3 + a_0x_0 + b_0$, and also has restrictions on the possible values of $\boldsymbol{j}$. The former problem can be easily resolved by setting:

$$\begin{aligned} \boldsymbol{a} &\overset{\text{def}}{=} \boldsymbol{\lambda}^4 \cdot \frac{27\boldsymbol{j}}{4(1728-\boldsymbol{j})} = (a_0, \cdots) \\ \boldsymbol{b} &\overset{\text{def}}{=} \boldsymbol{\lambda}^6 \cdot \frac{27\boldsymbol{j}}{4(1728-\boldsymbol{j})} = (b_0, \cdots), \end{aligned}$$

where

$$\boldsymbol{\lambda} \overset{\text{def}}{=} \left(\left(\frac{b_0}{a_0} \right)^{1/2}, 0, 0, \dots \right).$$

In the case of $p = 5$, this method gives

$$\begin{aligned} A_1 &= (2a_0^{12} + 3a_0^9 b_0^2 + 3a_0^6 b_0^4 + 3a_0^3 b_0^6 + 3b_0^8)/(a_0 b_0^4), \\ B_1 &= (2a_0^{12} b_0 + 3a_0^9 b_0^3 + 3a_0^6 b_0^5 + 3a_0^3 b_0^7 + 3b_0^9)/a_0^6. \end{aligned}$$

But again, in this case A_1 is not defined for the ordinary elliptic curve given by $(1, 0)$. So this method fails to provide universally defined formulas for A_1 and B_1. (Not surprisingly, due to the restrictions that $\boldsymbol{j} \neq 0, 1728$ in Eq. (2.1).)

On the other hand, observe that all the expressions we've obtained for A_1 and B_1, with exception of B_1 in the second row of Table 2.1, are *modular functions* of weight $4p$ and $6p$ respectively! (This particular B_1 fails because it comes from our choice to take $A_1 = a_0$, which has weight 4 and not $4p$.) To be more precise on our usage of the term *modular functions* in this context, we introduce the following defintion:

Definition 2.2. Let a_0 and b_0 be indeterminates in $\mathbb{F}_p[a_0, b_0]$, and assign them weights 4 and 6 respectively. Then, let

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

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

Note that the given weights make $\mathbb{F}_p[a_0, b_0]$ into a graded ring. Then, the sums of quotients (in $\mathbb{F}_p(a_0, b_0)$) of *homogeneous* polynomials in $\mathbb{F}_p[a_0, b_0]$ also form a graded ring $\mathcal{S}$. The set $\mathcal{S}_n$ is simply the homogeneous component of weight n of this graded ring.

The fact that our examples above give $A_i \in \mathcal{S}_{4p^i}$ and $B_i \in \mathcal{S}_{6p^i}$ has an interesting implication: given $\lambda_0 \neq 0$, the elliptic curves over $\Bbbk$ given by (a_0, b_0) and $(\lambda_0^4 a_0, \lambda_0^6 b_0)$ are isomorphic and therefore the elliptic curves over $\boldsymbol{W}(\Bbbk)$ given by

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

and

$$((\lambda_0^4 a_0, A_1(\lambda_0^4 a_0, \lambda_0^6 b_0), A_2(\lambda_0^4 a_0, \lambda_0^6 b_0), \ldots), (\lambda_0^6 b_0, B_1(\lambda_0^4 a_0, \lambda_0^6 b_0), B_2(\lambda_0^4 a_0, \lambda_0^6 b_0), \ldots))$$

are isomorphic (by the uniqueness of the canonical lifting), so there must be some $\boldsymbol{\lambda}$ such that:

$$(\lambda_0^4 a_0, A_1(\lambda_0^4 a_0, \lambda_0^6 b_0), A_2(\lambda_0^4 a_0, \lambda_0^6 b_0), \ldots) = \boldsymbol{\lambda}^4 (a_0, A_1(a_0, b_0), A_2(a_0, b_0), \ldots), \tag{2.2}$$

$$(\lambda_0^6 b_0, B_1(\lambda_0^4 a_0, \lambda_0^6 b_0), B_2(\lambda_0^4 a_0, \lambda_0^6 b_0), \ldots) = \boldsymbol{\lambda}^6 (b_0, B_1(a_0, b_0), B_2(a_0, b_0), \ldots). \tag{2.3}$$

If A_i and B_i are modular function of weights $4p^i$ and $6p^i$ respectively, then we have that $\boldsymbol{\lambda} = (\lambda_0, 0, 0, \ldots)$, the simplest possible $\boldsymbol{\lambda}$. (Clearly, the converse also holds, i.e., if $\boldsymbol{\lambda} = (\lambda_0, 0, 0, \ldots)$ works in Eqs. (2.2) and (2.3), then $A_i \in \mathcal{S}_{4p^i}$ and $B_i \in \mathcal{S}_{6p^i}$.)

Also, observe that all A_i's and B_i's we found here are in $\mathbb{F}_p(a_0, b_0)$, so are rational functions with coefficient in $\mathbb{F}_p$.

So, ideally, we would be in search of A_i's and B_i's (giving the coordinates of the Weierstrass coefficients of the canonical lifting) that are both universal and in $\mathcal{S}_{4p^i}$ and $\mathcal{S}_{6p^i}$ respectively. Of course, at this point one must wonder if this is even possible. But, in fact, computations seem to indicate that it is indeed. The author has posted some computations of these functions at `https://github.com/lrfinotti/cl_examples`, and the MAGMA routines used in these computations can be found at `https://github.com/lrfinotti/witt`. Here are a few examples. For $p = 5$, we have:

$$\begin{aligned} A_1 &= (a_0^3 b_0^2 + b_0^4)/a_0, \\ B_1 &= 4a_0^6 b_0 + a_0^3 b_0^3 + b_0^5, \end{aligned}$$

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:

$$\begin{aligned} A_1 &= 5a_0^7 + 4a_0^4 b_0^2 + 4a_0 b_0^4, \\ B_1 &= (3a_0^{12} + a_0^9 b_0^2 + 3a_0^6 b_0^4 + 5a_0^3 b_0^6 + 4b_0^8)/b_0, \end{aligned}$$

and

$$\begin{aligned}
A_2 = {} & (6a_0^{61} + 5a_0^{58}b_0^2 + 6a_0^{55}b_0^4 + 4a_0^{52}b_0^6 + 3a_0^{43}b_0^{12} + 6a_0^{40}b_0^{14} + a_0^{37}b_0^{16} \\
& + a_0^{34}b_0^{18} + 4a_0^{31}b_0^{20} + 2a_0^{28}b_0^{22} + 3a_0^{25}b_0^{24} + 6a_0^{19}b_0^{28} + a_0^{16}b_0^{30} \\
& + 3a_0^{13}b_0^{32} + 6a_0^{10}b_0^{34} + 2a_0^{4}b_0^{38} + 2a_0b_0^{40})/b_0^8, \\
B_2 = {} & (5a_0^{96} + 4a_0^{93}b_0^2 + 5a_0^{90}b_0^4 + 6a_0^{87}b_0^6 + 4a_0^{84}b_0^8 + 3a_0^{81}b_0^{10} + 6a_0^{72}b_0^{16} \\
& + 5a_0^{69}b_0^{18} + 5a_0^{66}b_0^{20} + 2a_0^{60}b_0^{24} + 3a_0^{57}b_0^{26} + a_0^{54}b_0^{28} + 2a_0^{51}b_0^{30} + 6a_0^{48}b_0^{32} \\
& + 2a_0^{45}b_0^{34} + 6a_0^{42}b_0^{36} + 2a_0^{39}b_0^{38} + a_0^{33}b_0^{42} + 4a_0^{30}b_0^{44} + 5a_0^{27}b_0^{46} + 4a_0^{24}b_0^{48} \\
& + a_0^{21}b_0^{50} + 3a_0^{18}b_0^{52} + 5a_0^{15}b_0^{54} + 5a_0^{12}b_0^{56} + 5a_0^{9}b_0^{58} + 6a_0^{6}b_0^{60} + 6a_0^{3}b_0^{62})/b_0^{15}.
\end{aligned}$$

These computations, as well as others for $p = 11, 13$ (and others not posted in the site above), seem to indicate that indeed, A_i and B_i *can* be universal modular functions in $\mathcal{S}_{4p^i}$ and $\mathcal{S}_{6p^i}$ respectively.

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 $\Bbbk^2_{\text{ord}}$) and hence do not have canonical liftings. In fact, these are the *only* supersingular curves for their corresponding characteristic!

This 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. (See Theorem 1.1 in [Fin13].)

Thus, our main goal here is to prove:

Theorem 2.3. *There are universal modular functions $A_i \in \mathcal{S}_{4p^i}$ and $B_i \in \mathcal{S}_{6p^i}$ (and, in particular, are rational functions with coefficients in $\mathbb{F}_p$), for $i \in \{1, 2, 3, \ldots\}$, such that if $(a_0, b_0) \in \Bbbk^2_{\text{ord}}$ 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.

Moreover, we shall also 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 requires only linear algebra and an algorithm developed by Voloch and Walker (and later extended by the author), to compute canonical liftings. (This algorithm is described in Section 5, and it was shown to the author by Voloch. It can be derived after Proposition 4.2 from [VW00], but it does not explicitly appear in this or any other reference besides some of the author's previous papers.) On the other hand, the author believes that the proof itself, although simple, is far from trivial.

The universality part of Theorem 2.3 is proved in Section 7, while the modularity part is proved in Section 8.

It should be mentioned that 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 as the author could tell, to assume that these A_i's and B_i's would be modular functions, perhaps due to some previously posted computations, and then asked about their weights.

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 many sources such as Hazewinkel's [Haz09] and Borger's [Bor11]. A more friendly introduction can be found in Rabinoff's notes [Rab14].

Let p be a prime and for each non-negative integer n consider

$$W^{(n)}(X_0, \ldots, X_n) \overset{\text{def}}{=} X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^n X_n,$$

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

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

and

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

More explicitly, we have the following recursive formulas:

$$S_n = (X_n + Y_n) + \frac{1}{p}(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p) + \cdots + \frac{1}{p^n}(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}) \tag{3.1}$$

and

$$\begin{aligned}
P_n &= \frac{1}{p^n}\Big[(X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - \\
&\qquad \Big(P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^{p}\Big)\Big] \\
&= (X_0^{p^n} Y_n + X_1^{p^{n-1}} Y_{n-1}^{p} + \cdots + X_n Y_0^{p^n}) \\
&\quad + \frac{1}{p}(X_0^{p^n} Y_{n-1}^{p} + \cdots + X_{n-1}^{p} Y_0^{p^n}) \qquad (3.2)\\
&\quad \vdots \\
&\quad + \frac{1}{p^n}(X_0^{p^n} Y_0^{p^n}) - \frac{1}{p^n} P_0^{p^n} - \cdots - \frac{1}{p} P_{n-1}^{p} \\
&\quad + p\left(X_1^{p^{n-1}} Y_n + X_2^{p^{n-2}}(Y_{n-1}^{p} + pY_n) + \ldots\right).
\end{aligned}$$

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 $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$, by

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

and

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

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 $\bar{S}_n, \bar{P}_n \in \mathbb{F}_p[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$, 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 introduce a grading on $\mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$ by defining $\operatorname{wgt}(X_i) = \operatorname{wgt}(Y_i) = p^i$, then both S_n and P_n are homogeneous of weights p^n and $2p^n$ respectively in this graded ring. This gives the following trivial lemma:

Lemma 3.1. *Let $\pi_i : \boldsymbol{W}(\Bbbk) \to \Bbbk$ denote the map that gives the i-th 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 polynomials in two variables. For our mainly computational purposes, the definition is quite simple. For more details, refer to [Lan52] and [Gre61], or, for a more advanced reference using the scheme language, [Bui96] and [LS03] give a good introduction.

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

Definition 3.2. For $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$, we refer to $\boldsymbol{f}(\boldsymbol{x}_0, \boldsymbol{y}_0) \in \boldsymbol{W}(R)$ as above as the *Greenberg transform* of $\boldsymbol{f}$, and denote it by $G(\boldsymbol{f})$.

Moreover, if

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

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

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

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

Also observe that we clearly have

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

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.

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. So, if j_0 is the j-invariant of an ordinary elliptic curve and $\boldsymbol{j} = (j_0, j_1, \ldots)$ is the j-invariant of its canonical lifting, then

$$\Phi_p((j_0, j_1, \ldots), (j_0^p, j_1^p, \ldots)) = 0,$$

where $\Phi_p(X, Y)$ is the modular polynomial. This allows us to successively find j_1, j_2, etc. (See, for instance, Theorem 3 of [LST64].)

On the other hand, Voloch and Walker developed an 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 author is not aware of the complexity calculations of either algorithm, but computations in practice make it clear that, if one uses known formulas for the modular polynomial Φ_p, the former method is considerably more efficient. Also, it is clear that the former method requires considerably less memory, as for the Voloch-Walker algorithm we have to work with Witt vectors over rings of polynomials in several variables, which yield polynomials with a huge number of terms.

On the other hand, the Voloch-Walker algorithm not only computes the canonical lifting (via its Weierstrass coefficients, instead of j-invariant), but also the elliptic Teichmüller lift (described in Section 1), which also gives us the lifting of the Frobenius. (To see how the computation of the lifting of the Frobenius and the elliptic Teichmüller lift are related, refer to [Bui96] or [VW00].)

Since this algorithm yields the Weierstrass coefficients, even though is less efficient in practice, it suits us better for the task at hand.

Remember that if

$$E/\mathbb{k} \ : \ y_0^2 = f(x_0) \overset{\text{def}}{=} x_0^3 + a_0 x_0 + b_0,$$

then the *Hasse invariant* $\mathfrak{H}$ of E for 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 $\mathrm{wgt}(a_0) = 4$ and $\mathrm{wgt}(b_0) = 6$ as before, then $\mathfrak{H}$ is a homogeneous polynomial of weight $(p-1)$.

Before we can describe the Voloch-Walker algorithm, we need the following results:

Theorem 4.1. *Let $\mathbb{k}$ be a field of characteristic $p \geq 5$, $E/\mathbb{k}$ be an ordinary elliptic curve given by Eq.* (1.2)*, $\boldsymbol{E}/\boldsymbol{W}(\mathbb{k})$ be its canonical lifting (given by a short Weierstrass equation as in Eq.* (1.3)*) and $\tau : E(\mathbb{k}) \to \boldsymbol{E}(\boldsymbol{W}(\mathbb{k}))$ be the elliptic Teichmüller lift. Then, there are $F_i, H_i \in \mathbb{k}[x_0]$ such that*

$$\tau(x_0, y_0) = ((x_0, F_1, F_2, \ldots), (y_0, y_0 H_1, y_0 H_2, \ldots))$$

with

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

where deg *denotes the degree of polynomials in* $\Bbbk[x_0]$*, 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 F_k' *denotes the derivative of* F_k*.*

The bounds for the degrees are given by Theorem 1.1 from [Fin02] and the formula for the derivative is Theorem 2.1 from [Fin04].

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 that $\boldsymbol{W}(\Bbbk)$ is a *strict p-ring* (as defined in Chapter II of [Ser79]). Moreover, in [LST64] the canonical lifting is defined for ordinary curves over *perfect* fields of positive characteristic. 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 fact in our description of the algorithm below.

5. Voloch and Walker's Algorithm for Computing the Canonical Lifting

5.1. **The Setup.** In order to obtain general formulas, we consider in this section $\mathbb{K} = \mathbb{F}_p(a, b)$ where a and b are *indeterminates* and $p \geq 5$. (So, clearly $\mathbb{K}$ is not perfect.) Then the elliptic curve given by (a, b) (i.e., given by Eq. (1.2) with $a_0 = a$ and $b_0 = b$) is ordinary. Suppose its canonical lifting $\boldsymbol{E}$ is given by $(\boldsymbol{a}, \boldsymbol{b})$, i.e., given by Eq. (1.3), with $\boldsymbol{a} = (a, a_1, a_2, \ldots)$ and $\boldsymbol{b} = (b, b_1, b_2, \ldots)$. Also, suppose that the elliptic Teichmüller (with the notation of Theorem 4.1) is given by

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

where F_i and H_i are polynomials in x_0. (So, in principle, a_i, b_i, and the coefficients of F_i and H_i, all belong to the perfect closure of $\mathbb{K}$.)

We will derive an algorithm to compute, one coordinate at a time, the a_i's, b_i's, F_i's and H_i's, and show that $a_i, b_i \in \mathbb{K}$ and $F_i, H_i \in \mathbb{K}[x_0]$, i.e., we do not need the perfect closure of $\mathbb{K}$.

We shall proceed by induction: so assume that we have computed the first n coordinates, i.e., a_i, b_i, F_i, and H_i for $i < n$, and that $a_i, b_i \in \mathbb{K}$ and $F_i, H_i \in \mathbb{K}[x_0]$ for all $i < n$. We then want to compute the $(n+1)$-st coordinates, i.e., a_n, b_n, F_n and H_n, and show that also $a_n, b_n \in \mathbb{K}$ and $F_n, H_n \in \mathbb{K}[x_0]$.

Summarizing:

- **We know (induction hypothesis):** a_i, b_i, F_i, and H_i for $i < n$, and that $a_i, b_i \in \mathbb{K}$ and $F_i, H_i \in \mathbb{K}[x_0]$ for all $i < n$.
- **We need:** to find a_n, b_n, F_n and H_n with $a_n, b_n \in \mathbb{K}$ and $F_n, H_n \in \mathbb{K}[x_0]$.

As it will become clear from the procedure below, we observe that we can later apply the same formulas obtained form $\mathbb{K} = \mathbb{F}_p(a, b)$ for the canonical lifting and elliptic Teichmüller lift with $a = a_0$ and $b = b_0$, where $(a_0, b_0) \in \Bbbk^2_{\text{ord}}$, for any (not necessarily perfect) field $\Bbbk$ of characteristic p, as long as (a_0, b_0) yields no poles for the formulas obtained.

5.2. **The Affine Part.** Since $\tau(x_0, y_0)$ is a point of $\boldsymbol{E}$, it must satisfy the equation given by the $(n+1)$-st coordinate of the Greenberg transform. For simplicity, let again f denote the cubic from the Weierstrass equation of E, i.e., let $f \stackrel{\text{def}}{=} x_0^3 + ax_0 + b$. Thus, with our induction hypothesis, the $(n+1)$-st coordinate of the Greenberg transform gives us:

$$2y_0^{p^n+1} H_n \equiv (f')^{p^n} F_n + a_n x_0^{p^n} + b_n \pmod{\mathbb{K}[x_0, y_0]}, \tag{5.1}$$

where we use the congruence notation in the usual way for abelian groups, i.e., $a \equiv b \pmod{H}$ if $(a - b) \in H$. Observe that the terms in $\mathbb{K}[x_0, y_0]$ in this $(n+1)$-st coordinate of the Greenberg transform correspond to terms we have previously computed, and therefore are all known, while the terms a_n, b_n, F_n and H_n are the terms we need compute in this step. (Note that we use the prime, as in f', to denote derivatives with respect to x_0.) This congruence 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, we have that omitted terms on the right hand side of Eq. (5.1) form a polynomial in $\mathbb{K}[x_0]$. Also, observing that $y_0^2 = f(x_0)$ and using Lemma 5.1 from [Fin04], we have that Eq. (5.1) becomes

$$2f^{(p^n+1)/2} H_n \equiv (f')^{p^n} F_n + a_n x_0^{p^n} + b_n \pmod{\mathbb{K}[x_0]}. \tag{5.2}$$

(The cited lemma guarantees that the powers of y_0 appearing on the coordinates of $(y_0, y_0H_1, y_0H_2, \ldots)^2$ are all even, and thus can be replaced by polynomials in x_0.)

Now, finding the polynomials F_n, H_n means finding their coefficients. Since we know F_n' (from Theorem 4.1), 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 (but $\hat{F}_n$ is known). Note, moreover, that by Theorem 4.1 and our induction hypothesis, we have that $\hat{F}_n \in \mathbb{K}[x_0]$.

Also, we shall let $N \overset{\text{def}}{=} ((n+3)p^n - np^{n-1} - 3)/2$ 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 $\deg H_n \leq N$.)

So, now we will replace F_n and H_n in Eq. (5.2) by their expressions given above (in terms of their coefficients). This way we introduce the c_i's and d_i's are unknowns, and our goal becomes to compute a_n, b_n, the c_i's and d_i's, and prove that they are all in $\mathbb{K} = \mathbb{F}_p(a, b)$.

Then, this gives us

$$2f^{(p^n+1)/2} \left(\sum_{i=0}^{N} d_i x_0^i \right) \equiv (f')^{p^n} \left(\sum_{i=0}^{M} c_i x_0^{ip} \right) + a_n x_0^{p^n} + b_n \pmod{\mathbb{K}[x_0]}, \tag{5.3}$$

or

$$2f^{(p^n+1)/2} \left(\sum_{i=0}^{N} d_i x_0^i \right) = (f')^{p^n} \left(\sum_{i=0}^{M} c_i x_0^{ip} \right) + a_n x_0^{p^n} + b_n + g \tag{5.4}$$

for some $g \in \mathbb{K}[x_0]$ which has all of its terms known by the induction hypothesis (i.e., the computations of the previous coordinates).

Now, comparing the coefficients of same degree (in x_0) in the equation above gives a *linear* system (with coefficients in $\mathbb{K}$) in the unknowns a_n, b_n, c_i's and d_i's. Note that we know that this system 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 for the *affine parts*, but nothing else. (Basically, we are still missing regularity at infinity.)

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

5.3. **Regularity at Infinity.**

The fact that $\tau^*(\boldsymbol{x}/\boldsymbol{y})(O) = 0$ will allow us to compute a few of the c_i's and d_i's, while at the same time guarantee that any solution after that will give precisely the canonical lifting and elliptic Teichmüller lift.

We shall denote by $\mathfrak{m}_O$ the elements h of the function field of function field of E such that $\mathrm{ord}_O(h) \geq 1$, i.e., the maximal ideal of the ring of regular functions at O, and so we have the all coordinates of $\tau^*(\boldsymbol{x}/\boldsymbol{y})$ must be in $\mathfrak{m}_O$.

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

We will need the following result:

Lemma 5.2. *The monomials* $\prod X_i^{a_i} \prod Y_j^{b_j}$ *occurring on* $\bar{P}_n$ *satisfies*

$$\sum a_i p^i = \sum b_j p^j = p^n \quad \text{and} \quad \sum i a_i p^i + \sum j b_j p^j \leq n p^n.$$

Moreover,

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

where $\bar{Q}_n \in \mathbb{F}_p[X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}]$ *and has its monomials (as above) satisfying* $\sum i a_i p^i + \sum j b_j p^j \leq (n-1)p^n$.

Proof. The lemma is Lemma 2.1 from [Fin02]. Although the lemma states

$$\sum i a_i p^i + \sum j b_j p^j < n p^n$$

for the second part, its proof actually shows the result stated above. □

Proof of Lemma 5.1. 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. (3.2), it suffices to show that the denominator for the $(n+1)$-st 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:

$$\boldsymbol{y}^{-1} = \left(\frac{\alpha_0}{y_0}, \frac{\alpha_1}{y_0^{2p}}, \frac{\alpha_2}{y_0^{3p^2}}, \ldots, \frac{\alpha_{n-1}}{y_0^{np^{n-1}}}, \beta_n, \ldots \right),$$

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

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

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

$$\beta_n y_0^{p^n} + \sum_{i=1}^{n} \frac{\alpha_{n-i}^{p^i}}{y_0^{(n-i+1)p^n}} y_i^{p^{n-i}} + \bar{Q}_n(y_0, \ldots, y_{n-1}, \alpha_0/y_0, \ldots, \alpha_{n-1}/y_0^{np^{n-1}}) = 0.$$

By Lemma 5.2, a term from $\bar{Q}_n$ coming from a monomial $\prod X_i^{a_i} \prod Y_j^{b_j}$ has the power of y_0 in its denominator given by

$$\sum b_j(j+1)p^j = \sum b_j p^j + \sum j b_j p^j \leq p^n + (n-1)p^n = np^n.$$

Then, solving for β_n in the above equation gives that its denominator is $y_0^{(n+1)p^n}$. □

So, still assuming that we have a_i, b_i, F_i and H_i for $i = 1, \ldots, (n-1)$ giving us the first n coordinates of the canonical lifting and elliptic Teichmüller lift, we look at the $(n+1)$-st coordinate of $\tau^*(\boldsymbol{x}/\boldsymbol{y})$, which we shall denote by τ_n. By Lemma 5.1 above, we have that

$$\tau_n = \frac{F_n}{y_0^{p^n}} - \frac{y_0 H_n \cdot x_0^{p^n}}{y_0^{2p^n}} + \frac{\epsilon_1}{y_0^{(n+1)p^n}},$$

for some $\epsilon_1 \in \mathbb{K}[x_0, y_0]$. Replacing H_n in the equation above by the expression for it given by Eq. (5.1), we get

$$\tau_n = \left(\frac{1}{y_0^{p^n}} - \frac{x_0^{p^n}}{2y_0^{3p^n}} (f')^{p^n} \right) F_n - \frac{a_n x_0^{2p^n}}{2y_0^{3p^n}} - \frac{b_n}{2y_0^{3p^n}} + \frac{\epsilon_2}{y_0^{(n+1)p^n}}, \tag{5.5}$$

for some $\epsilon_2 \in \mathbb{K}[x_0, y_0]$.

Remember that we are imposing the condition that $\tau^*(\boldsymbol{x}/\boldsymbol{y})(O) = 0$, and hence we must have that $\tau_n \in \mathfrak{m}_O$. 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 in $\mathfrak{m}_O$, 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

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

are also in $\mathfrak{m}_O$. Note that if $n = 1$, then $F_{n,1} = 0$, and we have that Eq. (5.5) is already in $\mathfrak{m}_O$ (i.e., we have that $\tau_1 \in \mathfrak{m}_O$). This is simple computation that can be done directly or one can refer to proof of Proposition 4.2 in [VW00]. 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 (that $\tau_n \in \mathfrak{m}_O$) are the c_i's for $i \geq M'$.

So, using again that $y_0^2 = f(x_0)$, and remembering that we need $\tau_n \in \mathfrak{m}_O$, Eq. (5.5) gives us

$$\tau_n \equiv \frac{1}{y_0^{(n+1)p^n}} \left[y_0^{(n-2)p^n} \left(f^{p^n} - \frac{x_0^{p^n}}{2} (f')^{p^n} \right) F_{n,1} + \mathcal{F} + y_0 \mathcal{G} \right] \equiv 0 \pmod{\mathfrak{m}_O}, \tag{5.6}$$

where $\mathcal{F}, \mathcal{G} \in \mathbb{K}[x_0]$ are such that $\epsilon_2 = \mathcal{F} + y_0\mathcal{G}$. (Note that the terms of ϵ_2 are all known, i.e., have been computed with previous coordinates.) This congruence then imposes that the terms inside the brackets must have a pole of order less than $\left| \mathrm{ord}_O \left(y_0^{(n+1)p^n} \right) \right| = 3(n+1)p^n$.

If n is even, let

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

and then Eq. (5.6) becomes

$$\tau_n \equiv \frac{1}{y_0^{(n+1)p^n}} \left[\mathcal{H} F_{n,1} + \mathcal{F} + y_0 \mathcal{G} \right] \equiv 0 \pmod{\mathfrak{m}_O}.$$

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 $\mathrm{ord}_O\left(y_0\mathcal{G}\right), \mathrm{ord}_O\left(\mathcal{H}F_{n,1} + \mathcal{F}\right) > -3(n+1)p^n$, 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 $i \in \{(3p^{n-1} + 1)/2, (3p^{n-1} + 3)/2, \ldots, M\}$. 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. (5.6) becomes

$$\tau_n \equiv \frac{1}{y_0^{(n+1)p^n}} \left[y_0 \mathcal{H} F_{n,1} + \mathcal{F} + y_0 \mathcal{G} \right] \equiv 0 \pmod{\mathfrak{m}_O}.$$

A similar analysis as the one above gives again c_i for $i \in \{(3p^{n-1}+1)/2, (3p^{n-1}+3)/2, \ldots, M\}$ 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 $\mathbb{K} = \mathbb{F}_p(a, b)$. Then, the system given by Eq. (5.4) has these terms determined, which then would also determine the d_i's for $i \in \{(4p^n - p - 1)/2, (4p^n - p + 1)/2, \ldots, N\}$.

So, with $M' = (3p^{n-1} - 1)/2$ (as above) and $N' \stackrel{\text{def}}{=} (4p^n - p - 3)/2$, the terms c_i for $i = M + 1, \ldots, M'$ and d_i for $i = N + 1, \ldots, N'$ are now known, and hence we can collect these with the other already known terms, simplifying Eq. (5.4) to

$$2f^{(p^n+1)/2} \left(\sum_{i=0}^{N'} d_i x_0^i \right) = (f')^{p^n} \left(\sum_{i=0}^{M'} c_i x_0^{ip} \right) + a_n x_0^{p^n} + b_n + g_2, \tag{5.7}$$

with $g_2 \in \mathbb{K}[x_0]$ having all its terms known. Again this gives us a linear systems on the still unknown a_n, b_n, $c_0, \ldots, c_{M'}$, $d_0, \ldots, d_{N'}$ with coefficients in $\mathbb{K}$.

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 a_n, b_n, $c_0, \ldots, c_{M'}$, and imposing that this remainder is zero gives a linear system on these unknowns, and thus does not involve the d_i's. 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. (5.7), 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 $\mathbb{K} = \mathbb{F}_p(a, b)$, we have that there is a solution also in $\mathbb{F}_p(a, b)$.

6. Solutions of the System

In this section we study the solutions of the system given by Eq. (5.7), under the same assumptions as in the previous section, which we review below:

- $\mathbb{K} = \mathbb{F}_p(a, b)$, with $p \geq 5$ prime, and a, b indeterminates;

- we have already computed $a_1, \ldots, a_{n-1}, b_1, \ldots, b_{n-1} \in \mathbb{K}$ such that $(a, a_1, \ldots, a_{n-1})$ and $(b, b_1, \ldots, b_{n-1})$ give the first n-coordinates of the Weierstrass coefficients of the canonical lifting (of the curve given by (a, b));
- we have already computed $F_1, \ldots, F_{n-1}, H_1, \ldots, H_{n-1} \in \mathbb{K}[x_0]$ such that the first n-coordinates of the elliptic Teichmüller lift is given by
$$\tau(x_0, y_0) = ((x_0, F_1, \ldots, F_{n-1}), (y_0, y_0 H_1, \ldots, y_0 H_{n-1}));$$
- we have
$$F_n = \sum_{i=0}^{M'} c_i x_0^{ip} + \cdots \quad \text{and} \quad H_n = \sum_{i=0}^{N'} d_i x_0^{i} + \cdots$$
where $M' = (3p^{n-1} - 1)/2$ and $N' = (4p^n - p - 3)/2$ and the omitted terms where computed as described in the previous section, and only $c_0, \ldots, c_{M'}, d_0, \ldots, d_{N'}$ are still unknown (from F_n and H_n).

As observed in the previous section, *any* solution of the linear system (on a_n, b_n, $c_0, \ldots, c_{M'}$, $d_0, \ldots, d_{N'}$) given by Eq. (5.7) gives the $(n+1)$-st coordinates of the Weierstrass coefficients of the canonical lifting and its associate elliptic Teichmüller lift.

In this section we prove the following result:

Proposition 6.1. *With the notation and terminology above, the solution of the linear system on a_n, b_n, $c_0, \ldots, c_{M'}$, $d_0, \ldots, d_{N'}$ given by Eq.* (5.7) *has the following properties:*

1. *it has exactly one free parameter;*
2. *this free parameter can be assigned to the value of either a_n, b_n, or c_n, and hence we can choose any value for one of these three variables;*
3. *the values for c_i for $i \neq p^{n-1}$ do not depend on the free parameter.*

The rest of this section is dedicated to the proof of this proposition.

Suppose then that we have two solutions to this system, 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 $\boldsymbol{\lambda} \in \boldsymbol{W}_{n+1}(\bar{\mathbb{K}})$, where $\boldsymbol{W}_k$ denote the ring of Witt vectors of length k, such that:
$$(a, \ldots, a_{n-1}, a_n') = \boldsymbol{\lambda}^4 (a, \ldots, a_{n-1}, a_n),$$
$$(b, \ldots, b_{n-1}, b_n') = \boldsymbol{\lambda}^6 (b, \ldots, b_{n-1}, b_n).$$

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 $\mathbb{K}$ (or in some extension of $\mathbb{K}$). Hence, this gives us that

$$\begin{aligned} a_n' &= a_n + 4\lambda a^{p^n}, \\ b_n' &= b_n + 6\lambda b^{p^n}. \end{aligned}$$

If we subtract Eq. (5.7) from the same equation for the second solution (i.e., $(a_n', b_n', \ldots)$), we get

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

Since the elliptic Teichmüller is uniquely determined by the Weierstrass coefficients, there is a unique solution for c_i''s and d_i''s for any fixed choice 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 $a_n' = a_n + 4\lambda a^{p^n}$ and $b_n' = b_n + 6\lambda b^{p^n}$.

This shows that the nullspace of the coefficient matrix of the system given by Eq (5.7) has dimension 1 (and thus proves item 1 of Proposition 6.1), generated by

$$(4a^{p^n}, 6b^{p^n}, 0, \ldots, 0, 2, 0, \ldots, 0, 3b^{(p^n-1)/2}, \ldots, 3, 0, \ldots, 0),$$

where 2 appears in the coordinate corresponding to $c_{p^{n-1}}$ and $3b^{(p^n-1)/2}$ appears in the coordinate corresponding to d_0. 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, proving item 3 of Proposition 6.1.

The observation above also show that we can choose the value for either $c_{p^{n-1}}$, a_n or b_n, proving item 2 of Proposition 6.1.

It is worth noting that one can choose the value of a_n or b_n since $a, b \neq 0$ in $\mathbb{K} = \mathbb{F}_p(a, b)$. When solving this system for a given pair (a_0, b_0) in some field, we might not be able to choose the value of a_n (resp., b_n) if $a_0 = 0$ (resp., $b_0 = 0$). But, *we can always choose the value of $c_{p^{n-1}}$!*

7. Universality

In Section 5 we showed that Eq. (5.7) gives a linear system whose solutions (known to exist) give the canonical lifting and elliptic Teichmüller lift. We were working on $\mathbb{K} = \mathbb{F}_p(a, b)$, with a and b as indeterminates, and hence these give formulas (for a_i, b_i, F_i and H_i) work for any $(a_0, b_0) \in \Bbbk^2_{\text{ord}}$, where $\Bbbk$ is a field of characteristic p, *as long as these formulas do not have poles when evaluated at $a = a_0$ and $b = b_0$.* What we will do in this section is to show that one can find solutions that will be defined for *every* pair $(a_0, b_0) \in \Bbbk^2_{\text{ord}}$ as above, i.e., we can get formulas that yield no poles in $\Bbbk^2_{\text{ord}}$.

More precisely, we shall prove the following:

Proposition 7.1. *Let $\mathbb{K} = \mathbb{F}_p(a, b)$, with a and b indeterminates, $\Delta = 4a^3 + 27b^2$ be the discriminant of the elliptic curve given by (a, b), $\mathfrak{H}$ be its Hasse invariant, and $\mathbb{L} \stackrel{\text{def}}{=} \mathbb{F}_p[a, b, 1/(\Delta\mathfrak{H})]$. Then, there are $a_i, b_i \in \mathbb{L}$ and $F_i, H_i \in \mathbb{L}[x_0]$, for $i = 1, 2, \ldots$ such that the canonical lifting of the elliptic curve given by (a, b) is given by $((a, a_1, \ldots), (b, b_1, \ldots))$ and the associate Teichmüller lift is given by*

$$\tau(x_0, y_0) = ((x_0, F_1, \ldots), (y_0, y_0 H_1, \ldots)).$$

This proposition gives the following corollary, which is the universal part (as defined in Definition 2.1) of Theorem 2.3:

Corollary 7.2. *There are* universal *rational functions A_i and B_i over $\mathbb{F}_p$ for $i \in \{1, 2, 3, \ldots\}$, such that if $(a_0, b_0) \in \Bbbk^2_{\text{ord}}$, with* $\operatorname{char}(\Bbbk) = p$, *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 of the curve given by (a_0, b_0).

Proof of Corollary 7.2. Simply take $A_i = a_i$ and $B_i = b_i$, with a_i and b_i from Proposition 7.1, as these are clearly universal. □

The rest of this section is dedicated to the proof of Proposition 7.1.

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

$$E/\mathbb{K} \; : \; y_0^2 = x_0^3 + ax_0 + b$$

up to the n-th coordinate, with $a_i, b_i \in \mathbb{L}$ and $F_i, H_i \in \mathbb{L}[x_0]$, and we will use, again, the linear system given by Eq. (5.7) to find a_n, b_n, F_n and H_n, with $a_n, b_n \in \mathbb{L}$, and $F_n, H_n \in \mathbb{L}[x_0]$.

First, observe that all the omitted terms of Eq. (5.7) are in $\mathbb{L}$. For most of them this follows from the induction hypothesis. But also the terms in $\hat{F}_n$ are in $\mathbb{L}$ by the induction hypothesis and the formula for F_n' (in Theorem 4.1). Moreover, the c_i's, for $i \in \{M'+1, \dots, M\}$ are in $\mathbb{L}$, 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 $\mathcal{F}, \mathcal{H} \in \mathbb{L}[x_0]$) when n is even, or $\deg(\mathcal{H}F_n + \mathcal{G}) < (3(n+1)p^n - 3)/2$ (for some polynomials $\mathcal{G}, \mathcal{H} \in \mathbb{L}[x_0]$) 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 $i \in \{N'+1, \dots, N\}$ are also in $\mathbb{L}$ 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, by item 3 of Proposition 6.1, we know that all c_i's, for $i \leq M'$, except for $c_{p^{n-1}}$, are universal, since they are independent of any choices. Thus, they are all must be in $\mathbb{L}$. (Here is where the denominator Δ could conceivably appear, although they do not appear in examples explicitly computed.) Also, by item 2 of the same proposition, we may choose the value of $c_{p^{n-1}}$, and *we will now choose it to be zero*, and hence also in $\mathbb{L}$. Since the general solution to the system had only one free parameter (item 1 of the proposition), 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. (5.7), we get a system of the form:

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

where all "$*$" entries are in $\mathbb{L}$. So, also $d_i \in \mathbb{L}$ for all i.

Finally, now looking at terms of degrees p^n and 0 in Eq. (5.7), we can see that also $a_n, b_n \in \mathbb{L}$, which finishes the proof of Proposition 7.1.

8. Modularity

In this section we prove the following proposition:

Proposition 8.1. *With the choice of $c_{p^{n-1}} = 0$, the rational functions A_i and B_i from Corollary 7.2 (obtained from a_i and b_i from Proposition 7.1) are in fact in $\mathcal{S}_{4p^i}$ and $\mathcal{S}_{6p^i}$ respectively.*

Thus, this proves the modularity part of Theorem 2.3, and so, together with Corollary 7.2, finishes the proof of the theorem.

Proof. For the sake of consistency of notation with the previous sections, we will use a_i and b_i (as in Proposition 7.1) instead of A_i and B_i.

To simplify the exposition, we shall extended the definition of $\mathcal{S}_n$. First, let $\mathrm{wgt}(x_0) \overset{\text{def}}{=} 2$ and $\mathrm{wgt}(y_0) \overset{\text{def}}{=} 3$, while still assuming that $\mathrm{wgt}(a) = 4$ and $\mathrm{wgt}(b) = 6$, so that y_0^2 and $x_0^3 + ax_0 + b$ are both homogeneous of weight 6. Then, define:

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

So, again, we are dealing with a graded ring and we have $\mathcal{S}_n = \hat{\mathcal{S}}_n \cap \mathbb{F}_p(a, b)$.

We again use induction to prove the proposition. So, we assume that, for $i < n$, we have that $F_i \in \hat{\mathcal{S}}_{2p^i}$, $y_0 H_i \in \hat{\mathcal{S}}_{3p^i}$, $a_i \in \hat{\mathcal{S}}_{4p^i}$ and $b_i \in \hat{\mathcal{S}}_{6p^i}$ and shall to prove that the method described in the previous sessions (with the choice of $c_{p^{n-1}} = 0$) gives that $a_n \in \hat{\mathcal{S}}_{4p^n}$, $b_n \in \hat{\mathcal{S}}_{6p^n}$, $F_n \in \hat{\mathcal{S}}_{2p^n}$ and $H_n \in \hat{\mathcal{S}}_{3p^n}$. Of course, since $a_n, b_n \in \mathbb{F}_p(a, b)$, this means that $a_n \in \mathcal{S}_{4p^n}$ and $b_n \in \mathcal{S}_{6p^n}$, which is what we want in this proposition.

By Lemma 3.1, we have that the omitted terms in Eq. (5.1) (or Eq. (5.2)) are all in $\hat{\mathcal{S}}_{6p^n}$. 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 $\hat{\mathcal{S}}_{2p^n}$, by Theorem 4.1. Thus, all omitted terms of Eq. (5.3) are also in $\hat{\mathcal{S}}_{6p^n}$.

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 $\hat{\mathcal{S}}_{-p^n}$, and hence the terms $\mathcal{F} + y_0 \mathcal{G}$ inside the brackets in Eq. (5.6) are in $\hat{\mathcal{S}}_{(3n+2)p^n}$. This implies that $F_{n,1} = \sum_{i=M'+1}^{M} c_i x_0^{ip} \in \hat{\mathcal{S}}_{2p^n}$. Then, Eq. (5.3), by equating degrees, gives us that $\sum_{i=N'+1}^{N} d_i x_0^i \in \hat{\mathcal{S}}_{3p^n-3}$. So, all of the omitted terms of Eq. (5.7) are in $\hat{\mathcal{S}}_{6p^n}$.

Remember we are choosing $c_{p^{n-1}} = 0$, and hence the solution for the system given by Eq (5.7) is unique. Moreover, by Proposition 7.1, the denominators of c_i's, d_i's, a_n and

b_n that give the solution can be taken to be powers of $\Delta \cdot \mathfrak{H}$, and hence are *homogeneous* polynomials on a, b, since Δ and $\mathfrak{H}$ are homogeneous with $\mathrm{wgt}(\Delta) = 12$ and $\mathrm{wgt}(\mathfrak{H}) = p-1$. 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

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

This way, since only terms of same weight can cancel each other out, we have, by Eq. (5.7), 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. (5.7) (i.e., all the known terms), 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. (5.7), 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, $F_n \in \hat{\mathbb{S}}_{2p^n}$, $y_0 H_n \in \hat{\mathbb{S}}_{3p^n}$, $A_n = a_n \in \hat{\mathbb{S}}_{4p^n}$ and $B_n = b_n \in \hat{\mathbb{S}}_{6p^n}$, which is what we needed to prove. □

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

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

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

Thus, if we want to preserve the weights, we must choose $\lambda \in \mathbb{S}_0$. If we want to keep it universal, we must choose $\lambda \in \mathbb{L}$, and hence all possible A_n's and B_n's satisfying Theorem 2.3 come from choosing $\lambda \in \mathbb{L} \cap \mathbb{S}_0$ 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 $c_{p^{n-1}} \in \mathbb{L} \cap \mathcal{S}_0$ when solving the system given by Eq. (5.7).

9. Final Observations

First, we prove the following proposition about the possible weights of modular functions A_i and B_i:

Proposition 9.1. *Suppose that, with the same notation as above, we have functions A_i and B_i giving the coordinates of the Weierstrass coefficients of the canonical lifting, with $A_i \in \mathcal{S}_{r_i}$ and $B_i \in \mathcal{S}_{s_i}$. Then we must have $r_i = 4p^i$ and $s_i = 6p^i$. In other words, if A_i and B_i are modular functions, their weights must be $4p^i$ and $6p^i$ respectively.*

Proof. 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 $4p^i$ and $6p^i$, respectively, and in this case we also must have $\lambda_i = 0$ for $i > 0$, and hence $\boldsymbol{\lambda} = (\lambda_0, 0, 0, \ldots)$.

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, $A_n \in \mathcal{S}_{r_n}$, for some r_n.

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

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

and so

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

Since the left hand side is in $\mathcal{S}_{4p^n}$ and the right hand side is in $\mathcal{S}_{r_n}$, we must have $r_n = 4p^n$, 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 $r_n = 4p^n$ or $A_n = 0$, and so $A_n \in \mathcal{S}_{4p^n}$.

Also, since now we have $\lambda_n = 0$, Eq. (9.2) 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 as a denominator, but we never explicitly introduce a denominator of Δ. On the other hand, when solving the system given by Eq. (5.7), the determinant of the coefficient matrix can introduce new denominators. 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. In any event, it would be nice to find bounds for the powers of $\mathfrak{H}$ that appear in the denominator.

We make a final observation in regard to *pseudo-canonical liftings*: as observed in Section 1, there are unique functions $J_1, J_2, \ldots$, for $p \geq 5$, such that if j_0 is the j-invariant of an ordinary elliptic curve, then the Witt vector $(j_0, J_1(j_0), J_2(j_0), \ldots)$ is the j-invariant of its canonical lifting.

Now, suppose that $j = j_0$ is the j-invariant of a *supersingular* elliptic curve, but assume that $J_1, J_2, \ldots, J_n$ are all defined at j_0. Then, the elliptic curve over $\boldsymbol{W}_{n+1}(\Bbbk)$ with j-invariant $(j_0, J_1(j_0), \ldots, J_n(j_0))$ is, of course, *not* the canonical lifting, as these do not exist for supersingular elliptic curves. On the other hand, it is given by the *same formulas* that give the canonical lifting (for ordinary j-invariants). We then call this elliptic curve given by $(j_0, J_1(j_0), \ldots, J_n(j_0))$ a *pseudo-canonical lifting* (modulo p^n) of the curve given by j_0.

We've studied these pseudo-canonical liftings (along with the functions J_i's) in [Fin10], [Fin11], and [Fin12]. We first summarize the main results (Theorems 1.2 and 1.3 from [Fin12]) below:

Theorem 9.2. (1) *We have that the functions J_i are rational functions over $\mathbb{F}_p$.*

(2) *If j_0 gives a supersingular elliptic curve and $j_0 \neq 0, 1728$, then J_n has a pole of order $np^{n-1} + (n-1)p^{n-2}$ at j_0.*

(3) *J_1 never has poles at $j_0 = 0, 1728$, even if those values of j_0 give supersingular elliptic curves.*

(4) *J_2 never has poles at $j_0 = 0$, even if it gives a supersingular elliptic curve, but* does *have a pole at $j_0 = 1728$, if it gives a supersingular elliptic curve.*

(5) *J_3 has a pole at $j_0 = 0$ if it gives a supersingular elliptic curve.*

This means that $j_0 = 0$ gives a pseudo-canonical lifting modulo p^3 (for primes p for which $j_0 = 0$ is supersingular, i.e., $p \equiv 5 \pmod 6$) and $j_0 = 1728$ gives a pseudo-canonical lifting modulo p^2 (for primes p for which $j_0 = 1728$ is supersingular, i.e., $p \equiv 3 \pmod 4$).

One could ask then if this notion of pseudo-canonical liftings would translate to the Weierstrass coefficients also: is there (a_0, b_0) giving a *supersingular* elliptic curve, and universal modular functions $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$, as in Theorem 2.3, such that the A_i's and B_i's are all defined at (a_0, b_0)? One might think that the case for the J_i's might indicated that when $j_0 = 0$, i.e., $a_0 = 0$, gives supersingular elliptic curve, we might be able to get A_1, A_2 and B_1, B_2 which are defined at $(0, b_0)$, since J_1 and J_2 are defined at $j_0 = 0$. (And we could make the analogous guess for when $j_0 = 1728$, i.e., $b_0 = 0$.) But that is not the case, as we see below.

For example, the formula for the j-invariant of the canonical lifting in characteristic 5, in which case $j_0 = 0$ is supersingular, is

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

The algorithm we describe above give the following universal modular functions in this case:

$$\begin{aligned} A_1 &= (a_0^3 b_0^2 + b_0^4)/a_0 \\ B_1 &= 4a_0^6 b_0 + a_0^3 b_0^3 + b_0^5. \end{aligned}$$

So, clearly not defined for $a_0 = 0$. Moreover, as observed at the end of Section 8, any other A_1 and B_1 which are both universal and modular functions would have to be given by Eqs. (8.3) and (8.4), and these imply that if we remove the pole at $a_0 = 0$ from A_1, we introduce it to the new corresponding B_1. Therefore, there are no A_1 and B_1 (universal and modular) which are defined at a_0.

Acknowledgment. The author would like to thank F. Voloch and S. Mulay for the invaluable discussions on the subject of this paper, Delong Li for finding many typos in the original manuscript, and the referee for their helpful comments. Also, the computations mentioned were done with MAGMA.

References

[Bor11] J. Borger. The basic geometry of Witt vectors, I: The affine case. *Algebra Number Theory*, 5(2):231–285, 2011.

[Bui96] A. Buium. Geometry of p-jets. *Duke Math. Journal*, 82:349–367, 1996.

[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.

[Fin11] L. R. A. Finotti. Computations with Witt vectors of length 3. *J. Théor. Nombres Bordeaux*, 23(2):417–454, 2011.

[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.

[Haz09] M. Hazewinkel. Witt vectors. I. In *Handbook of algebra. Vol. 6*, volume 6 of *Handb. Algebr.*, pages 319–472. Elsevier/North-Holland, Amsterdam, 2009.

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

[LS03] F. Loeser and J. Sebag. Motivic integration on smooth rigid varieties and invariants of degenerations. *Duke Math. J.*, 119(2):315–344, 2003.

[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.

[Rab14] J. Rabinoff. The Theory of Witt Vectors. *arXiv e-prints*, page arXiv:1409.7445, September 2014.

[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
Email address: `lfinotti@utk.edu`