# DEGREES OF THE ELLIPTIC TEICHMÜLLER LIFT

LUÍS R. A. FINOTTI

Abstract. The purpose of this paper is to find upper bounds for the degrees, or equivalently, for the order of the poles at $O$, of the coordinate functions of the elliptic Teichmüller lift of an ordinary elliptic curve over a perfect field of characteristic $p$. We prove the following bounds:

$$\mathrm{ord}_0(x_n) \geq -(n+2)p^n + np^{n-1}, \quad \mathrm{ord}_0(y_n) \geq -(n+3)p^n + np^{n-1}.$$

Also, we prove that the bound for $x_n$ is not the exact order if, and only if, $p$ divides $(n+1)$, and the bound for $y_n$ is not the exact order if, and only if, $p$ divides $(n+1)(n+2)/2$. Finally, we give an algorithm to compute the reduction modulo $p^3$ of the canonical lift for $p \neq 2, 3$.

## 1. Introduction

Voloch and Walker in [5] applied the theory of *canonical lifts* of elliptic curves to construct error-correcting codes. In that paper, the degrees of some polynomials, that we shall make precise later, have some importance in estimating exponential sums. We here try to analyze those degrees, giving upper bounds and finding when the degrees are strictly less than those bounds. Also, we describe an algorithm to compute the reduction modulo $p^3$ of canonical lifts explicitly for $p \neq 2, 3$.

We will consider an *ordinary* elliptic curve over a perfect field $k$ of characteristic $p > 0$. The curve can be given by a Weierstrass equation:

$$E/k : \quad y_0^2 + a_0x_0y_0 + b_0y_0 = x_0^3 + c_0x_0^2 + d_0x_0 + e_0.$$

Such an elliptic curve has a canonical lifting to an elliptic curve over the ring of Witt vectors $W(k)$,

$$\boldsymbol{E}/W(k) : \quad \boldsymbol{y}^2 + \boldsymbol{a}\boldsymbol{x}\boldsymbol{y} + \boldsymbol{b}\boldsymbol{y} = \boldsymbol{x}^3 + \boldsymbol{c}\boldsymbol{x}^2 + \boldsymbol{d}\boldsymbol{x} + \boldsymbol{e},$$

with $\boldsymbol{a} = (a_0, a_1, \dots), \boldsymbol{b} = (b_0, b_1, \dots), \dots, \boldsymbol{e} = (e_0, e_1, \dots) \in W(k)$, for which we can lift the $p^{\text{th}}$ power Frobenius map. (See [2].)

We have an injective group homomorphism (given by a section of the reduction map) $\tau : E(\bar{k}) \to \boldsymbol{E}(W(\bar{k}))$, called the **elliptic Teichmüller lift** of $E$:

$$(x_0, y_0) \stackrel{\tau}{\mapsto} (\boldsymbol{x}, \boldsymbol{y}) = ((x_0, x_1, x_2, \dots), (y_0, y_1, y_2, \dots)).$$

---

1991 *Mathematics Subject Classification.* Primary 11G20; Secondary 11T71.

*Key words and phrases.* elliptic curves, canonical liftings, elliptic Teichmüller lift.

This work was funded by CAPES (an agency of the Brazilian government).

We notice that we can identify $\boldsymbol{E}/W(k)$ with its *Greenberg transform* $G(\boldsymbol{E})/k$, for which $\tau$ becomes simply

$$(x_0, y_0) \overset{\tau}{\mapsto} (x_0, x_1, x_2, \dots, y_0, y_1, y_2, \dots).$$

By theorem 4.1 of [5], with $\boldsymbol{G} = \boldsymbol{O}$ (the origin of $\boldsymbol{E}$), the functions $x_n$ and $y_n$ are regular except at $O$ (the origin of $E$), so are of the form $R(x_0) + y_0 S(x_0)$ for some polynomials $R, S \in k[x_0]$. For $p \neq 2$, $-(y_0, y_1, \dots) = (-y_0, -y_1, \dots)$, and using $\tau(-P) = -\tau(P)$, one can deduce that $x_n \in k[x_0]$ and $y_n = y_0 \cdot F_n(x_0)$, with $F_n \in k[x_0]$. For $p = 2$, a similar argument also gives us that $x_n \in k[x_0]$, but $y_n$ does *not* have to be of the form $y_0 \cdot F_n$.

Our first goal is to get good bounds for the degrees of these polynomials, or equivalently, for the order of poles of $x_n$ and $y_n$ at $O$. We prove

**Theorem 1.1.** *Let $v \stackrel{\text{def}}{=} \operatorname{ord}_O$, i.e., $v$ is the valuation on the function field $K$ of $E$ given by the order of vanishing of functions at $O$. Then, $v(x_n) \geq -((n+2)p^n - np^{n-1})$ and $v(y_n) \geq -((n+3)p^n - np^{n-1})$, for all $n \geq 0$.*

The case $n = 1$ was proved by Voloch and Walker in [5]. We will get the theorem 1.1 as a special case of the theorem 3.1 below.

## 2. Witt Vectors and Valuations

Let $p$ be a prime, and for any non-negative integer $n$ consider

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

the corresponding **Witt polynomial**. Then, there exist polynomials $S_n, P_n \in \mathbb{Z}[X_0, \dots, X_n, Y_0, \dots, Y_n]$ satisfying:

$$W_n(S_0, \dots, S_n) = W_n(X_0, \dots, X_n) + W_n(Y_0, \dots, Y_n) \tag{2.1}$$

and

$$W_n(P_0, \dots, P_n) = W_n(X_0, \dots, X_n) \cdot W_n(Y_0, \dots, Y_n). \tag{2.2}$$

(See [4].)

Thus, if $\boldsymbol{s} = (s_0, s_1, \dots)$ and $\boldsymbol{t} = (t_0, t_1, \dots)$ are Witt vectors, we have by definition

$$\boldsymbol{s} + \boldsymbol{t} \stackrel{\text{def}}{=} (S_0(s_0, t_0), S_1(s_0, s_1, t_0, t_1), \dots)$$

and

$$\boldsymbol{s} \cdot \boldsymbol{t} \stackrel{\text{def}}{=} (P_0(s_0, t_0), P_1(s_0, s_1, t_0, t_1), \dots).$$

We may write, to simplify the notation,

$$S_n(\boldsymbol{s}, \boldsymbol{t}) \stackrel{\text{def}}{=} S_n(s_0, \dots, s_n, t_0, \dots, t_n)$$

and

$$P_n(\boldsymbol{s}, \boldsymbol{t}) \stackrel{\text{def}}{=} P_n(s_0, \dots, s_n, t_0, \dots, t_n).$$

Now, let $K$ be a field of characteristic $p > 0$, and let us consider $W(K)$. (Note that although soon we will consider $K$ as the function field of $E$, as in the theorem 1.1, for now $K$ is *any* field of characteristic $p$.) Since the entries of our Witt vectors are in characteristic $p$, we can use the polynomials $\bar{S}_n, \bar{P}_n \in \mathbb{F}_p[X_0, \dots, X_n, Y_0, \dots, Y_n]$, that are the reductions of $S_n, P_n$ modulo $p$, to give us the sum and product of Witt vectors.

We now introduce three useful technical lemmas..

**Lemma 2.1.** *The monomials $\prod X_i^{a_i} \prod Y_j^{b_j}$ (disregarding the coefficient) occurring in $\bar{P}_n$ satisfy*

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

*Moreover,*

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

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

*Proof.* We prove it by induction. The case $n = 0$ is trivial, since $\bar{P}_0 = X_0 Y_0$. Now assume the lemma true for all $t \leq n-1$. We have:

$$\begin{aligned} P_n = {} & \frac{1}{p^n}\Big[(X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - \\ & \qquad \Big(P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p\Big)\Big] \\ = {} & (X_0^{p^n} Y_n + X_1^{p^{n-1}} Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) \\ & + \frac{1}{p}(X_0^{p^n} Y_{n-1}^p + \cdots + X_{n-1}^p Y_0^{p^n}) \\ & \vdots \\ & + \frac{1}{p^n}(X_0^{p^n} Y_0^{p^n}) - \frac{1}{p^n} P_0^{p^n} - \cdots - \frac{1}{p} P_{n-1}^p \\ & + p\left(X_1^{p^{n-1}} Y_n + X_2^{p^{n-2}}(Y_{n-1}^p + pY_n) + \dots\right). \end{aligned} \tag{2.3}$$

First we observe that the above polynomial has its coefficients in $\mathbb{Z}$. Also, the part that is a multiple of $p$ doesn't contribute to $\bar{P}_n$, and so we can disregard that last line of the equation above.

For $t = 0, \dots, n-1$, write $P_t = \tilde{P}_t + pR_t$, where we collected all the monomials of $P_t$ that have coefficients divisible by $p$ in $pR_t$. By the induction hypothesis, $\tilde{P}_t$ also satisfy the lemma. So, now we look at the contribution of $\frac{1}{p^{n-t}} P_t^{p^{n-t}}$ to $\bar{P}_n$: that is given by the monomials of $\tilde{P}_t^{p^{n-t}}$, which have the form

$$\prod X_i^{\sum_{r=1}^{p^{n-t}} a_{ir}} \prod Y_j^{\sum_{r=1}^{p^{n-t}} b_{jr}},$$

where the $\prod X_i^{a_{i_r}} \prod Y_j^{b_{j_r}}$ are monomials of $\tilde{P}_t$ for $r = 1, \dots, p^{n-t}$. So,

$$\sum_i \left[ \sum_{r=1}^{p^{n-t}} a_{i_r} \right] p^i = \sum_{r=1}^{p^{n-t}} \left[ \sum_i a_{i_r} p^i \right] = \sum_{r=1}^{p^{n-t}} p^t = p^n,$$

(and the analogous for the $b_{j_r}$ also holds) and

$$\begin{aligned} &\sum_i i \left[ \sum_{r=1}^{p^{n-t}} a_{i_r} \right] p^i + \sum_j j \left[ \sum_{r=1}^{p^{n-t}} b_{j_r} \right] p^j \\ &\quad = \sum_{r=1}^{p^{n-t}} \left[ \sum_i i a_{i_r} p^i + \sum_j j b_{j_r} p^j \right] \leq t p^n < n p^n. \end{aligned}$$

Observing that the last line of the equation (2.3) won't contribute to $\bar{P}_n$, all the remaining terms are of the form $X_i^{p^{n-i}} Y_j^{p^{n-j}}$. Excluding the ones of the form $X_i^{p^{n-i}} Y_{n-i}^{p^i}$, the remaining are such that $i + j < n$, and the lemma follows.

□

Now, let $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation of field $K$. (In the applications below, we will choose $K$ to be the function field of $E/k$ and $v$ to be the order of vanishing at a point $P \in E(\bar{k})$.) For $e \geq 0$, define:

$$U(e) \stackrel{\text{def}}{=} \left\{ \boldsymbol{s} = (s_0, s_1, \dots) \in W(K)^\times \;\middle|\; v(s_n) \geq p^n (v(s_0) - ne), \, \forall n > 0 \right\}.$$

(Note that $W(K)^\times = \{ \boldsymbol{s} = (s_0, s_1, \dots) \in W(K) \mid s_0 \neq 0 \}$.)

**Lemma 2.2.** *The set $U(e)$ is a subgroup of $W(K)^\times$.*

*Proof.* Let $\boldsymbol{s}, \boldsymbol{t} \in U(e)$. The $(n+1)$-th coordinate of $\boldsymbol{s}\,\boldsymbol{t}$ is given by $\bar{P}_n(\boldsymbol{s}, \boldsymbol{t})$. By lemma 2.1, for each monomial of $\bar{P}_n(\boldsymbol{s}, \boldsymbol{t})$ we have:

$$\begin{aligned} v\left( \prod s_i^{a_i} \prod t_j^{b_j} \right) &= \sum a_i v(s_i) + \sum b_j v(t_j) \\ &\geq \sum a_i p^i (v(s_0) - ie) + \sum b_j p^j (v(t_0) - je) \\ &\geq p^n (v(s_0) + v(t_0) - ne). \end{aligned} \tag{2.4}$$

Therefore, $v(\bar{P}_n(\boldsymbol{s}, \boldsymbol{t})) \geq p^n (v(s_0 t_0) - ne)$ for all $n$, i.e., $\boldsymbol{s}\,\boldsymbol{t} \in U(e)$. (Note that since all elements of $\mathbb{F}_p^\times$ are roots of unity, $v$ is zero on all its elements, and we don't have to worry about the coefficients of the monomials in $\bar{P}_n$.)

We prove that $\boldsymbol{t} \stackrel{\text{def}}{=} \boldsymbol{s}^{-1} \in U(e)$ by induction on the coordinate: assume that for all $i < n$ we have $v(t_i) \geq p^i (v(t_0) - ie)$. We observe that:

$$\bar{P}_n(\boldsymbol{s}, \boldsymbol{t}) = t_n \, s_0^{p^n} + \cdots = 0$$

where no omitted term involves $t_n$. So, $v(t_n\, s_0^{p^n})$ is equal to the valuation of the omitted terms. But for those, we can use (2.4), and so

$$v(t_n\, s_0^{p^n}) \geq p^n(v(s_0) + v(t_0) - ne),$$

and this gives us $v(t_n) \geq p^n(v(t_0) - ne)$.

□

**Lemma 2.3.** *If $v(s_0) = 1$ and $v(s_n) \geq 1$ for all $n$, then $s \in U((p-1)/p)$.*

*Proof.* Just note that $v(s_n) \geq 1 \geq p^n[1 - n(p-1)/p] = np^{n-1} - (n-1)p^n$. □

## 3. Upper Bounds

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

Define, for $P \in E(\bar{k})$,

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

and

$$\boldsymbol{U}_0(P) \stackrel{\text{def}}{=} \left\{\boldsymbol{g} \in \boldsymbol{U}(P) \mid \operatorname{ord}_P(g_0) = 0\right\}.$$

Observe that clearly $\boldsymbol{U}(P)$ is a subgroup of $\boldsymbol{R}^\times$ and $\boldsymbol{U}_0(P)$ is a subgroup of $\boldsymbol{U}(P)$.

**Theorem 3.1.** *Let $\boldsymbol{g} = (g_0, g_1, \dots) \in \boldsymbol{U}(P)$. Then*

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

*Proof.* Let $\boldsymbol{\pi} \in \boldsymbol{U}(P)$ be such that $\operatorname{ord}_{\tau(P)}(\boldsymbol{\pi}) = 1$. (Note we can choose $\boldsymbol{\pi}$ as either $(\boldsymbol{x} - \boldsymbol{x}(\tau(P)))$, $\boldsymbol{y}$ or $\boldsymbol{x}/\boldsymbol{y}$.) By lemma 2.3, $\boldsymbol{\pi} \in U((p-1)/p)$, now with $v \stackrel{\text{def}}{=} \operatorname{ord}_P$. In the same way, $\boldsymbol{\pi}^{1-v(g_0)}\boldsymbol{g} \in U((p-1)/p)$. Since $U((p-1)/p)$ is a group, $\boldsymbol{g} \in U((p-1)/p)$.

□

Theorem 1.1 then follows, applying the previous theorem with $P = O$ and $\boldsymbol{g} = \boldsymbol{x}, \boldsymbol{y}$.

We observe that if $\operatorname{ord}_{\tau(P)}(\boldsymbol{g}) < 0$, then theorem 3.1 gives us upper bounds for the order of the poles of the $g_n$'s, for all $n \geq 0$. If $\operatorname{ord}_{\tau(P)}(\boldsymbol{g}) > 0$, the theorem still gives us some information: it gives lower bounds for the order of the zeros for $n < p(\operatorname{ord}_P(g_0))/(p-1)$.

## 4. Leading Coefficients

Our main goal in this section is to verify when we don't have the equality in the upper bounds of theorem 1.1. But since the same techniques give stronger results, we will obtain these results first, and then get our main goal as a corollary.

As observed in the proof of the theorem 3.1, we can always take a uniformizer $\pi_0$ at $P$ that is a reduction of a uniformizer $\boldsymbol{\pi}$ at $\tau(P)$. Let $\pi_0$ be such a uniformizer at $P$ and let $\boldsymbol{g} \in \boldsymbol{U}(P)$. Also, let the expansion of $g_n$ in terms of $\pi_0$ be

$$g_n = b_n(\boldsymbol{g})\pi_0^{p^n(\mathrm{ord}_P(g_0)-n)+np^{n-1}} + \dots, \tag{4.1}$$

where the omitted terms have higher powers of $\pi_0$ (by theorem 3.1). We call $b_n(\boldsymbol{g}) \in k$ the **$n$-th leading coefficient** of $\boldsymbol{g}$ at $P$, relative to $\pi_0$.

Finally, define

$$\Phi(\boldsymbol{g}) \stackrel{\text{def}}{=} \sum_{n=0}^{\infty} b_n(\boldsymbol{g})^{p^{-n}}\, T^n.$$

**Theorem 4.1.** *The function $\Phi : \boldsymbol{U}(P) \to (k[[T]])^\times$ is a group homomorphism.*

*Proof.* Let $\boldsymbol{g}, \boldsymbol{h} \in \boldsymbol{U}(P)$. We must prove that $\Phi(\boldsymbol{gh}) = \Phi(\boldsymbol{g})\Phi(\boldsymbol{h})$, i.e.,

$$b_n(\boldsymbol{gh}) = \sum_{i=0}^{n} b_i(\boldsymbol{g})^{p^{n-i}}\, b_{n-i}(\boldsymbol{h})^{p^i}.$$

This is another application of lemma 2.1: taking valuations $v \stackrel{\text{def}}{=} \mathrm{ord}_P$ on the terms of $\bar{P}_n(\boldsymbol{g}, \boldsymbol{h})$ (the $(n+1)$-th coordinate of $\boldsymbol{gh}$), the part with valuation $p^n(v(g_0\, h_0) - n) + np^{n-1}$ comes from

$$\sum_{i=0}^{n} g_i^{p^{n-i}} h_{n-i}^{p^i},$$

and thus, the $n$-th leading coefficient of $\boldsymbol{gh}$ is obtained by multiplying the leading coefficients of the terms in the sum.

□

**Theorem 4.2.** *For $\boldsymbol{g} \in \boldsymbol{U}_0(P)$, $\Phi(\boldsymbol{g}) = g_0(P)$.*

*Proof.* Just observe that $p^n(\mathrm{ord}_P(g_0) - n) + np^{n-1} < 0$ for $n \geq 1$, and it is zero for $n = 0$. □

**Theorem 4.3.** *If $A$ is the Hasse invariant of $E$ relative to the invariant differential $\lambda$ such that $(d\pi_0/\lambda)(P) = 1$, then*

$$\Phi(\boldsymbol{\pi}) = (1 + A^{-p^{-1}}T).$$

*Proof.* Since $\mathrm{ord}_{\tau(P)}(\boldsymbol{\pi}) = \mathrm{ord}_P(\pi_0) = 1$, then $p^n(\mathrm{ord}_P(\pi_0) - n) + np^{n-1}$ is equal to 1 for $n = 0, 1$, and it is negative for $n > 1$. So

$$\Phi(\boldsymbol{\pi}) = 1 + \alpha^{p^{-1}}T,$$

where $\pi_1 = \alpha\,\pi_0 + \dots$. Hence we need to prove that

$$\frac{d\pi_1}{d\pi_0}(P) = A^{-1}. \tag{4.2}$$

So, let $\boldsymbol{u} \in \boldsymbol{U}(P)$ such that $\boldsymbol{u}\,d\boldsymbol{\pi}$ is an invariant differential (i.e., holomorphic) on $\boldsymbol{E}$, with $u_0(P) = 1$. Thus, $\lambda = u_0\,d\pi_0$.

Now, let $\phi$ be the lift of the Frobenius to $\boldsymbol{E}$. Then, $\phi^*(\boldsymbol{u}^\sigma\,d\boldsymbol{\pi}^\sigma)/p$, where $\boldsymbol{v}^\sigma$, for $\boldsymbol{v} \in \boldsymbol{R}$, is obtained by applying the Frobenius $\sigma$ for Witt vectors on the coefficients of $\boldsymbol{v}$, is a well defined homomorphic differential on $\boldsymbol{E}$, and its reduction modulo $p$, say $\omega$, depends only on $u_0\,d\pi_0$. (See [3].) Thus,

$$\omega = cu_0\,d\pi_0 = c\,\lambda, \tag{4.3}$$

for some $c \in k$.

If we apply the Cartier operator, we get

$$C(\omega) = C\,(c\,\lambda) = c^{1/p}\,A^{1/p}\,\lambda. \tag{4.4}$$

On the other hand, by [1], we know that, for $\boldsymbol{v} \in \boldsymbol{R}$, the $p$-derivation

$$\delta\boldsymbol{v} \stackrel{\text{def}}{=} \frac{\boldsymbol{v}^\sigma \circ \phi - \boldsymbol{v}^p}{p}, \tag{4.5}$$

is such that the reduction modulo $p$ of $\delta^i\boldsymbol{v}$ is equal to $v_i + B_i$, where $B_i$ is a polynomial in $v_0, \dots v_{i-1}$ that we can compute explicitly. (We observe that this polynomial is zero for $i = 1$.) Therefore,

$$\frac{1}{p}\phi^*(\boldsymbol{u}^\sigma\,d\boldsymbol{\pi}^\sigma) = (p\delta\boldsymbol{u} + \boldsymbol{u}^p)\,\left(d(\delta\boldsymbol{\pi}) + \boldsymbol{\pi}^{p-1}d\boldsymbol{\pi}\right)$$

and, reducing modulo $p$, we deduce that

$$\omega = u_0^p(d\pi_1 + \pi_0^{p-1}d\pi_0) \tag{4.6}$$

Applying the Cartier operator in this new expression for $\omega$ we get $C(\omega) = u_0\,d\pi_0 = \lambda$, and comparing with (4.4), we get $c = A^{-1}$. So, comparing equations (4.3) and (4.6), we obtain (4.2).

□

**Corollary 4.4.** *If $\boldsymbol{g} = \boldsymbol{c}\boldsymbol{\pi}^v$, with $\boldsymbol{c} \in \boldsymbol{U}_0(P)$, then*

$$b_n(\boldsymbol{g}) = c_0(P)^{p^n}\binom{v}{n}A^{-np^{n-1}}.$$

*(With $A$ as in the statement of the theorem 4.3.)*

*Proof.* We have

$$\Phi(\boldsymbol{g}) = \Phi(\boldsymbol{c})\,\Phi(\boldsymbol{\pi})^v = c_0(P)\left(1 + A^{-p^{-1}}T\right)^v.$$

Hence

$$b_n(\boldsymbol{g})^{p^{-n}} = c_0(P)\binom{v}{n}A^{-np^{-1}}.$$

□

**Corollary 4.5.** *The inequality in theorem 3.1 is an equality unless* $\binom{\mathrm{ord}_P(g_0)}{n} \equiv 0 \pmod{p}$*, in which case it is a strict inequality.*

*Proof.* This a simple consequence of the previous corollary (and the definition of $b_n(\boldsymbol{g})$). Note that $A \neq 0$ since our elliptic curve is ordinary. □

**Corollary 4.6.** *Let* $v \stackrel{\text{def}}{=} \mathrm{ord}_O$*. Then,* $v(x_n) > -((n+2)p^n - np^{n-1})$ *if, and only if,* $p$ *divides* $(n+1)$*, and* $v(y_n) > -((n+3)p^n - np^{n-1})$*, if, and only if,* $p$ *divides* $(n+1)(n+2)/2$*.*

*Proof.* The valuation of $x_n$ (resp. $y_n$) is larger than $-((n+2)p^n - np^{n-1})$ (resp. $-((n+3)p^n - np^{n-1})$) if, and only if, $b_n(\boldsymbol{x}) = 0$ (resp. $b_n(\boldsymbol{y}) = 0$), relative to the uniformizer $\boldsymbol{\pi} = \boldsymbol{x}/\boldsymbol{y}$.

We observe that

$$\boldsymbol{x} = \left(\frac{\boldsymbol{x}}{\boldsymbol{y}}\right)^{-2} + \dots \quad \text{and} \quad \boldsymbol{y} = \left(\frac{\boldsymbol{x}}{\boldsymbol{y}}\right)^{-3} + \dots,$$

and hence, by corollary 4.4,

$$b_n(\boldsymbol{x}) = \binom{-2}{n} A^{-np^{n-1}} = (-1)^n (n+1) A^{-np^{n-1}}$$

and

$$b_n(\boldsymbol{y}) = \binom{-3}{n} A^{-np^{n-1}} = (-1)^n \frac{(n+1)(n+2)}{2} A^{-np^{n-1}},$$

what gives the result.

□

*Remark.* Theorem 1.1 tells us that the degree of $x_n$ as a polynomial in $x_0$ is less than or equal to $r \stackrel{\text{def}}{=} \left[(n+2)p^n - np^{n-1}\right]/2$. Since

$$x_0 = \left(\frac{x_0}{y_0}\right)^{-2} + \dots \quad \text{and} \quad y_0 = \left(\frac{x_0}{y_0}\right)^{-3} + \dots, \tag{4.7}$$

one can see that

$$b_n(\boldsymbol{x}) = (-1)^n (n+1) A^{-np^{n-1}}$$

is also the coefficient of $x_0^r$ in $x_n$. Also, if $p \neq 2$ and we write $y_n = y_0 F_n$, where $F_n$ is a polynomial in $x_0$, then the degree of $F_n$ as a polynomial in $x_0$ is less than or equal to $s \stackrel{\text{def}}{=} \left[(n+3)p^n - np^{n-1} - 3\right]/2$, and its coefficient of $x_0^s$ is

$$b_n(\boldsymbol{y}) = (-1)^n \frac{(n+1)(n+2)}{2} A^{-np^{n-1}}$$

(again, using (4.7)).

## 5. Reduction Modulo $p^3$

In the next section we will describe an algorithm to compute the reduction modulo $p^3$ of the canonical lift and the elliptic Teichmüller map explicitly for $p \neq 2, 3$. To make sure that our computation gives us the right answer, we introduce the following sufficient condition (true for all primes):

**Proposition 5.1.** *Let $k$ be a perfect field of characteristic $p > 0$. If $\boldsymbol{E}/W_{n+1}(k)$ is an elliptic curve with reduction $E$, and if we have a section $\tau$ over $E \backslash \{O\}$ of the reduction from $G(\boldsymbol{E})$ to $E$ in the category of $k$-schemes, given by*

$$(x_0, y_0) \mapsto (\boldsymbol{x}, \boldsymbol{y}) = ((x_0, \dots, x_n), (y_0, \dots, y_n)),$$

*where $\boldsymbol{x}/\boldsymbol{y}$ is regular at $O$ with $\boldsymbol{x}/\boldsymbol{y}(O) = 0$, then $\boldsymbol{E}$ is the canonical lift of $E$ and $\tau$ is the elliptic Teichmüller lift.*

*Proof.* The proof is just the last paragraph of the proof of proposition 4.2 in [5]. □

Note that in the general case, in contrast to what happens for the second coordinate (see proposition 4.2 in [5]), it is not enough that $\deg(x_i) \leq (n+2)p^n - np^{n-1}$ and $\deg(y_i) \leq (n+3)p^n - np^{n-1}$ instead of $\boldsymbol{x}/\boldsymbol{y}(O) = 0$: e.g., in characteristic 5, considering just the first three coordinates, the elliptic curve

$$\boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{x}$$

has reduction $y_0^2 = x_0^3 + x_0$, and the map

$$\begin{aligned}
\nu(x_0, y_0) \stackrel{\text{def}}{=} ((&x_0, 4x_0^7 + x_0^3, 4x_0^5 + 3x_0^{13} + 2x_0^{15} + 2x_0^{17} + x_0^{19} + 4x_0^{23} + \\
&\qquad 3x_0^{25} + x_0^{27} + 4x_0^{31} + 3x_0^{33} + 2x_0^{37}), \\
&\qquad (y_0, y_0(x_0^8 + 2x_0^6 + 2x_0^4 + x_0^2 + 3), \\
&y_0(x_0^{56} + 2x_0^{54} + x_0^{52} + 3x_0^{48} + 3x_0^{44} + 2x_0^{42} + x_0^{40} + 2x_0^{38} + x_0^{36} + 2x_0^{34} + 3x_0^{32} + 4x_0^{30} \\
&\qquad + x_0^{26} + 3x_0^{24} + x_0^{16} + x_0^{14} + x_0^{10} + 4x_0^8 + 3x_0^6 + 3x_0^2 + 4))),
\end{aligned}$$

is a section of the reduction, but this map is not such that

$$\nu^*(\boldsymbol{x}/\boldsymbol{y}) = (\boldsymbol{x} \circ \nu) \,/\, (\boldsymbol{y} \circ \nu)$$

is regular at $O$, and therefore, this is not the elliptic Teichmüller lift. Using the techniques introduced later, we can compute the correct map:

$$\begin{aligned}\tau(x_0,y_0) \stackrel{\text{def}}{=} ((&x_0, 4x_0^7 + x_0^3, 4x_0^5 + 3x_0^{13} + 4x_0^{15} + 2x_0^{17} + x_0^{19} + 4x_0^{23} + x_0^{27} + 4x_0^{31} + \\ &3x_0^{33} + x_0^{35} + 2x_0^{37} + 2x_0^{45}), \\ &(y_0, y_0(x_0^8 + 2x_0^6 + 2x_0^4 + x_0^2 + 3), \\ &y_0(4x_0^{56} + 3x_0^{54} + 4x_0^{52} + 3x_0^{48} + 3x_0^{44} + 2x_0^{42} + x_0^{40} + 2x_0^{38} + 2x_0^{32} + 4x_0^{30} + 4x_0^{26} + 4x_0^{24} \\ &+ 3x_0^{22} + 4x_0^{14} + 4x_0^{12} + x_0^{10} + 4x_0^8 + 4x_0^6 + 2x_0^4 + 4x_0^2 + 4))).\end{aligned}$$

We now try to find properties that will allow us to compute explicitly coordinates of the coefficients of the canonical lift and the elliptic Teichmüller. We first observe that a method to compute the second coordinates can be derived from results in [5]. So, we try to obtain the analogues of those results to deduce a way to compute the third coordinates.

From the proof of proposition 4.2 in [5], one can deduce:

$$\frac{dx_1}{dx_0} = A^{-1}y_0^{p-1} - x_0^{p-1}, \tag{5.1}$$

for $p \neq 2$, where $A$ is the Hasse invariant of the curve associated to the invariant differential $dx_0/y_0$ (from this point on, $A$ will always denote this particular Hasse invariant). Following the same idea:

**Proposition 5.2.** *For $p \neq 2$, we have*

$$\frac{dx_2}{dx_0} = A^{-(p+1)}y_0^{p^2-1} - x_0^{p^2-1} - x_1^{p-1}\,\frac{dx_1}{dx_0}.$$

*Proof.* We consider the differential

$$\frac{1}{p}\phi^*\left(\frac{1}{p}\phi^*\left(\frac{d\boldsymbol{x}}{\boldsymbol{y}}\right)\right),$$

where $\phi$ is the lift of the Frobenius. Its reduction modulo $p$, say $\omega$, is of the form $c\,dx_0/y_0$, for some $c \in k$.

If we apply the Cartier operator, we get

$$C(\omega) = C\left(c\,\frac{dx_0}{y_0}\right) = c^{1/p}\,A^{1/p}\,\frac{dx_0}{y_0}. \tag{5.2}$$

On the other hand,

$$\frac{1}{p}\phi^*\left(\frac{1}{p}\phi^*\left(\frac{d\boldsymbol{x}}{\boldsymbol{y}}\right)\right) = \frac{1}{p}\phi^*\left(\frac{d(\delta\boldsymbol{x}) + \boldsymbol{x}^{p-1}d\boldsymbol{x}}{p\delta\boldsymbol{y} + \boldsymbol{y}^p}\right)$$

$$= \frac{d(\delta^2\boldsymbol{x}) + (\delta\boldsymbol{x})^{p-1}d(\delta\boldsymbol{x}) + (p\delta\boldsymbol{x} + \boldsymbol{x}^p)^{p-1}(d(\delta\boldsymbol{x}) + \boldsymbol{x}^{p-1}d\boldsymbol{x})}{p(p\,\delta^2\boldsymbol{y} + (\delta\boldsymbol{y})^p) + (p\delta\boldsymbol{y} + \boldsymbol{y}^p)^p}.$$

Since the universal polynomial $B_2(x_0, x_1) = -x_0^{p(p-1)} x_1$, the reduction of the differential above modulo $p$, that is again $\omega$, is

$$\frac{d(x_2 - x_0^{p(p-1)}x_1) + x_1^{p-1}dx_1 + x_0^{p(p-1)}(dx_1 + x_0^{p-1}dx_0)}{y_0^{p^2}}$$

$$= \frac{dx_2 + x_1^{p-1}dx_1 + x_0^{p^2-1}dx_0}{y_0^{p^2}},$$

and computing the Cartier operator using this form of $\omega$ and using (5.1), we get

$$C(\omega) = \frac{1}{y_0^p}(dx_1 + x_0^{p-1}dx_0) = A^{-1}\frac{dx_0}{y_0}. \tag{5.3}$$

Comparing equations (5.2) and (5.3), we get that $c = A^{-(p+1)}$, and comparing the two forms for $\omega$, we have

$$\frac{dx_2}{dx_0} = A^{-(p+1)}y_0^{p^2-1} - x_0^{p^2-1} - x_1^{p-1}(A^{-1}y_0^{p-1} - x_0^{p-1}).$$

□

*Remark.* We note that for characteristic 2, similar computations would give

$$\frac{dx_1}{dx_0} = \frac{dx_2}{dx_0} = 0.$$

Hence, the proposition above allows us to find $x_2$, except for finitely many terms of the form $d_n x_0^{np}$. (We can find the number of missing terms from the bounds for the degree.)

Now, we take a closer look at the quotient $\boldsymbol{x}/\boldsymbol{y}$ up to the third coordinate. In this case we have:

$$\frac{\boldsymbol{x}}{\boldsymbol{y}} = \left(\frac{x_0}{y_0}, \frac{x_1}{y_0^p} - \frac{y_1 x_0^p}{y_0^{2p}}, -\frac{x_1^p y_1^p}{y_0^{2p^2}} + \frac{x_2}{y_0^{p^2}} + \frac{x_0^{p^2} y_1^{2p}}{y_0^{3p^2}} - \frac{x_0^{p^2} y_2}{y_0^{2p^2}} \right.$$
$$\left. + \frac{1}{p}\left(\frac{x_1^p}{y_0^{p^2}} - \frac{y_1^p x_0^{p^2}}{y_0^{2p^2}} - \left(\frac{x_1}{y_0^p} - \frac{y_1 x_0^p}{y_0^{2p}}\right)^p\right)\right).$$

(We have here a small notation problem, since we cannot divide by $p$. But notice that the polynomial

$$\frac{1}{p}\left(X^p - Y^p - (X - Y)^p\right)$$

has *integer* coefficients, and we can substitute

$$X = \frac{x_1}{y_0^p}, \quad Y = \frac{y_1 x_0^p}{y_0^{2p}}$$

in this polynomial to obtain what we write as

$$\frac{1}{p}\left(\frac{x_1^p}{y_0^{p^2}} - \frac{y_1^p x_0^{p^2}}{y_0^{2p^2}} - \left(\frac{x_1}{y_0^p} - \frac{y_1 x_0^p}{y_0^{2p}}\right)^p\right)$$

in characteristic $p$. This abuse of notation will appear again below, but we hope that no confusion will arise from it.)

Looking at the orders in the third coordinate, we see that

$$\frac{1}{p}\left(\frac{x_1^p}{y_0^{p^2}} - \frac{y_1^p x_0^{p^2}}{y_0^{2p^2}} - \left(\frac{x_1}{y_0^p} - \frac{y_1 x_0^p}{y_0^{2p}}\right)^p\right)$$

has already positive order at $O$, and that, for $p \neq 2, 3$, all the summands in

$$-\frac{x_1^p y_1^p}{y_0^{2p^2}} + \frac{x_2}{y_0^{p^2}} + \frac{x_0^{p^2} y_1^{2p}}{y_0^{3p^2}} - \frac{x_0^{p^2} y_2}{y_0^{2p^2}} \tag{5.4}$$

have the same order, namely $-p^2+2p$. (Note that the orders of $x_2$ and $y_2$ are precisely $-4p^2+2p$ and $-5p^2+2p$, as we may see from our analysis of the leading coefficients.) But since $\tau^*(\boldsymbol{x}/\boldsymbol{y})(O) = 0$, those terms have to add up to have positive order.

So now we restrict ourselves to $p \neq 2, 3$, and then we may assume that $E$ is given by an equation of the form

$$E/k: \quad y_0^2 = x_0^3 + a_0 x_0 + b_0, \tag{5.5}$$

and that the canonical lift is given by

$$\boldsymbol{E}/W(k): \quad \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b}, \tag{5.6}$$

Looking at the third coordinates of the expression of (5.6), we see

$$\begin{aligned}
\frac{x_0^{p^2} y_2}{y_0^{2p^2}} &= \frac{x_0^{p^2}}{2y_0^{3p^2}}(2y_0^{p^2} y_2) \\
&= \frac{x_0^{p^2}}{2y_0^{3p^2}}\left(3x_0^{2p^2} x_2 + 3x_0^{p^2} x_1^{2p} - y_1^{2p} + \dots\right),
\end{aligned}$$

where the terms not shown have order greater than $-7p^2$, and so when multiplied by $x_0^{p^2}/2y_0^{3p^2}$, they give terms of positive order.

So, the part of (5.4) that has to add up to have positive order is

$$\begin{aligned}
&-\frac{x_1^p y_1^p}{y_0^{2p^2}} + \frac{x_2}{y_0^{p^2}} + \frac{x_0^{p^2} y_1^{2p}}{y_0^{3p^2}} - \frac{x_0^{p^2}}{2y_0^{3p^2}}\left(3x_0^{2p^2} x_2 + 3x_0^{p^2} x_1^{2p} - y_1^{2p}\right) \\
&= -\frac{x_1^p y_1^p}{y_0^{2p^2}} + \frac{x_2}{y_0^{p^2}} + \frac{2^{-1}3x_0^{p^2} y_1^{2p}}{y_0^{3p^2}} - \frac{2^{-1}3x_0^{3p^2} x_2}{y_0^{3p^2}} - \frac{2^{-1}3x_0^{2p^2} x_1^{2p}}{y_0^{3p^2}}.
\end{aligned}$$

Looking at the second coordinate of (5.6), we get

$$y_1 = \frac{2^{-1}3x_0^{2p} x_1 + \dots}{y_0^p},$$

where all the terms on the numerator omitted are of order greater than $-6p$. Then, the part of $x_1^p y_1^p / y_0^{2p^2}$ that has negative order is

$$\frac{2^{-1}3x_0^{2p^2}x_1^{2p}}{y_0^{3p^2}},$$

and the part of $2^{-1}3x_0^{p^2}y_1^{2p}/y_0^{3p^2}$ that has negative order is

$$\frac{8^{-1}27x_0^{5p^2}x_1^{2p}}{y_0^{5p^2}}.$$

So, the part of (5.4) that has to add up to have positive order is

$$\begin{aligned}&-\frac{2^{-1}3x_0^{2p^2}x_1^{2p}}{y_0^{3p^2}}+\frac{x_2}{y_0^{p^2}}+\frac{8^{-1}27x_0^{5p^2}x_1^{2p}}{y_0^{5p^2}}-\frac{2^{-1}3x_0^{3p^2}x_2}{y_0^{3p^2}}-\frac{2^{-1}3x_0^{2p^2}x_1^{2p}}{y_0^{3p^2}}\\ &=y_0^{-5p^2}\left[-\frac{3}{2}x_0^{2p^2}x_1^{2p}y_0^{2p^2}+x_2\,y_0^{4p^2}+\frac{27}{8}x_0^{5p^2}x_1^{2p}-\frac{3}{2}x_0^{3p^2}x_2\,y_0^{2p^2}-\frac{3}{2}x_0^{2p^2}x_1^{2p}y_0^{2p^2}\right].\end{aligned}$$

Using (5.5) and noticing that the part of the above expression that has to add up to have positive order is the part inside the brackets that has order at most $-15p^2$, we get that

$$\begin{aligned}&y_0^{-5p^2}\left[-\frac{3}{2}x_0^{5p^2}x_1^{2p}+x_2\,x_0^{6p^2}+\frac{27}{8}x_0^{5p^2}x_1^{2p}-\frac{3}{2}x_0^{6p^2}x_2-\frac{3}{2}x_0^{5p^2}x_1^{2p}\right]\\ &\qquad=\frac{x_0^{5p^2}}{y_0^{5p^2}}\left[\frac{3}{8}x_1^{2p}-\frac{1}{2}x_0^{p^2}x_2\right]\end{aligned}$$

has to add up to have positive order, i.e., the parts of order smaller or equal to $-5p^2$ inside the brackets above have to cancel out. Since those terms are polynomials in $x_0$, we get that the coefficient of $x_0^{np}$ in $x_2$ is $3/4$ times the $p^{\text{th}}$ power of the coefficient of $x_0^{n+p}$ in $x_1^2$, for all $n \geq (3p{+}1)/2$. (Note that by proposition 5.2, we knew that all the terms of degree, as a polynomial in $x_0$, higher than $(3p^2-1)/2$ in $x_2$ have to come from terms of the form $d_n x_0^{np}$.) Therefore, in the computation of the elliptic Teichmüller, some of the missing coefficients of $x_2$ can be obtained from coefficients of $x_1$.

Thus, this analysis, along with proposition 5.1, allows us to deduce the following theorem:

**Theorem 5.3.** *If $p \neq 2, 3$ and $\boldsymbol{E}/W_3(k)$ is an elliptic curve with reduction $E$, and if we have a section $\tau$ over $E\backslash\{O\}$ of the reduction from $G(\boldsymbol{E})$ to $E$, in the category of $k$-schemes, given by*

$$(x_0, y_0) \mapsto (\boldsymbol{x}, \boldsymbol{y}) = ((x_0, x_1, x_2), (y_0, y_1, y_2)),$$

*such that $\boldsymbol{E}$ and $\tau$ are the canonical lift and the elliptic Teichmüller modulo $p^2$, then the same is true modulo $p^3$ if, and only if, the degree of the polynomial (in $x_0$) $[x_0^{p^2}x_2 - 3/4\,x_1^{2p}]$ is less than or equal to $(5p^2-1)/2$. In fact, if this inequality holds, we must have the equality.*

*Proof.* The only part not discussed before is the last statement. For it, it just suffices to observe that proposition 5.2 implies that the coefficient of $x_0^{(3p^2-1)/2}$ in $x_2$ is not zero (it is $-2A^{-(p+1)}$) and that $x_1^{2p}$ just has powers of $x_0$ multiples of $p$. $\square$

## 6. The Algorithm

So now we see how to compute the canonical lifting and the elliptic Teichmüller explicitly, up to the third coordinate. In this whole section, we assume $p \neq 2, 3$, and that $E$ and $\boldsymbol{E}$ are given by equations (5.5) and (5.6).

First we compute $x_1$ by integrating formally the formula (5.1), and we leave the constant term, say $c_0$, and the coefficient of the term in $x_0^p$, say $c_1$, as indeterminates. (Note that in this case, the Hasse invariant $A$ is the coefficient of $x_0^{p-1}$ of $(x_0^3 + a_0x_0 + b_0)^{(p-1)/2}$.)

The second coordinate of the equation of $\boldsymbol{E}/W_2(k)$, namely

$$(y_0, y_1)^2 = (x_0, x_1)^3 + (a_0, a_1)(x_0, x_1) + (b_0, b_1),$$

is given by:

$$\begin{aligned} 2y_0^p y_1 &= 3x_0^{2p}x_1 + a_0^p x_1 + a_1 x_0^p + b_1 \\ &\quad + \frac{1}{p}\left(x_0^{3p} + a_0^p x_0^p + b_0^p - (x_0^3 + a_0x_0 + b_0)^p\right). \end{aligned} \tag{6.1}$$

Since $y_1$ is $y_0$ times a polynomial in $x_0$, equation (6.1) (keeping $a_1$ and $b_1$ as indeterminates) tells us that the division of polynomials (in $x_0$)

$$\frac{3x_0^{2p}x_1 + a_0^p x_1 + a_1 x_0^p + b_1 + \frac{1}{p}\left(x_0^{3p} + a_0^p x_0^p + b_0^p - (x_0^3 + a_0x_0 + b_0)^p\right)}{2(x_0^3 + a_0x_0 + b_0)^{(p+1)/2}}$$

must be exact. So we compute its remainder, which is a polynomial that has coefficients that depend on $a_1$, $b_1$, $c_0$ and $c_1$. Forcing that remainder to be zero gives us a linear system on those indeterminates. Solving that system gives us the canonical lift (i.e., $a_1$ and $b_1$) and $x_1$ (i.e., $c_0$ and $c_1$). And $y_1$ is just $y_0$ times the quotient of that exact division above.

We observe that the converse of the proposition 4.2 in [5] guarantees that the elliptic curve and map found are the right ones. Also, note that the solution of the system above does not have to be unique, since the canonical lift is only unique up to isomorphism.

The way to compute the third coordinate is analogous: we integrate formally the formula in proposition 5.2, and add the terms of degree in $x_0$ greater than $3p^2$ from $x_1^2$ as explained in the end of the previous section, and consider the coefficients in $x_0^{np}$, say $d_n$, for $n$ from 0 to $[(3p^2-1)/2p]$, as indeterminates.

Then, we just look at the third coordinate of the expression of the elliptic curve, use the fact that $y_2$ is also $y_0$ times a polynomial in $x_0$, and force the corresponding remainder of the analogous division of polynomials to be zero. We get another system, that we solve to get the desired values for the indeterminates, i.e., $a_2$, $b_2$ and the $d_i$'s. Theorem 5.3 then guarantees that this gives the canonical lift and the elliptic Teichmüller. We used this method to compute the canonical lift (the first three coordinates) of

$$y_0^2 = x_0^3 + x_0$$

in characteristic $p = 5$ shown in section 5. In fact, we were able to compute, using that algorithm, the canonical lift for a generic ordinary elliptic curve in characteristic 5: if

$$y_0^2 = x_0^3 + a_0 x_0 + b_0$$

is such curve ($a_0 \neq 0$, since the curve is ordinary), then its canonical lift has

$$\begin{aligned}
a_1 &= a_0^2 b_0^2 + \frac{b_0^4}{a_0}, \\
a_2 &= 2a_0^{25} + a_0^{22} b_0^2 + a_0^{19} b_0^4 + 3a_0^{16} b_0^6 + 2a_0^{13} b_0^8 + a_0^7 b_0^{12} + 4a_0 b_0^{16} \\
&\quad + \frac{3b_0^{18}}{a_0^2} + \frac{4b_0^{20}}{a_0^5} + \frac{4b_0^{22}}{a_0^8} + \frac{4b_0^{24}}{a_0^{11}}, \\
b_1 &= 4a_0^6 b_0 + a_0^3 b_0^3 + b_0^5, \\
b_2 &= a_0^{36} b_0 + 4a_0^{33} b_0^3 + 3a_0^{27} b_0^7 + 4a_0^{21} b_0^{11} + 4a_0^{15} b_0^{15} + a_0^{12} b_0^{17} + 3a_0^6 b_0^{21} + b_0^{25}.
\end{aligned}$$

(The polynomials for the the elliptic Teichmüller map are too long to be put in here.) We also were able to compute the generic cases for $p = 7, 11, 13$. A not too long particular case for $p = 7$ would be:

$$y_0^2 = x_0^3 + 1,$$

for which we have

$$\begin{aligned}
a_1 &= 0, & a_2 &= 0, \\
b_1 &= 4, & b_2 &= 0,
\end{aligned}$$

and

$$\begin{aligned}
x_1 &= 5x_0 + 2x_0^4 + 4x_0^{10}, \\
x_2 &= 4x_0 + 3x_0^4 + 5x_0^7 + 4x_0^{10} + 6x_0^{13} + 6x_0^{19} + 2x_0^{22} + 3x_0^{25} + x_0^{28} + \\
&\qquad 2x_0^{31} + 5x_0^{34} + 6x_0^{37} + 2x_0^{43} + 2x_0^{46} + 2x_0^{52} + 6x_0^{55} + 4x_0^{58} + 2x_0^{61} + \\
&\qquad 2x_0^{64} + 3x_0^{67} + 3x_0^{70} + 6x_0^{73} + 5x_0^{91}, \\
y_1 &= y_0(2x_0^3 + 3x_0^6 + 4x_0^9 + 6x_0^{12}), \\
y_2 &= y_0(2 + 6x_0^3 + 3x_0^6 + 6x_0^9 + x_0^{12} + x_0^{15} + 2x_0^{18} + 5x_0^{21} + x_0^{24} + 3x_0^{30} + \\
&\qquad x_0^{39} + 6x_0^{42} + x_0^{51} + x_0^{54} + 5x_0^{57} + 6x_0^{60} + 4x_0^{66} + 3x_0^{72} + 6x_0^{75} + \\
&\qquad 6x_0^{81} + 4x_0^{84} + 5x_0^{87} + 6x_0^{93} + 2x_0^{96} + 3x_0^{105} + 2x_0^{108} + 2x_0^{111} + 3x_0^{114}).
\end{aligned}$$

We first had implemented the algorithm using the software *Mathematica* and then, for convenience and speed, we switched to *Magma*, and the files are available at

`http://www.ma.utexas.edu/users/finotti/can_lifts.html`

where we also put the generic formulas for characteristic 2, 3, 5, 7, 11 and 13 and some more examples.

We also observe that the algorithm described also seems to "work" if you don't introduce the terms of $x_2$ from $x_1^2$, i.e., you use for $x_2$ just the formal integral of the derivative in proposition 5.2, and the terms of the form $d_i x_0^{ip}$ for $i < (3p^2-1)/2p$. The algorithm will give you back $a_1$, $a_2$, $x_1$, $x_2$, $y_1$ and $y_2$, where $\nu = ((x_0, x_1, x_2), (y_0, y_1, y_2))$ is a section of the reduction. But since $\nu^*(\boldsymbol{x}/\boldsymbol{y})$ is *not* regular at $O$, the curve obtained is in principle *not necessarily* the canonical lift, and the map is *certainly not* the elliptic Teichmüller. (This was how we obtained the "wrong lifting" $\nu$ in section 5.) But it seems that this lift may be used for some applications in coding theory, and it would be nicer than the canonical lift itself, since it has smaller degrees.

**Acknowledgments:** The author would like to thank J. F. Voloch for many of the ideas used in this paper, the referee, whose suggestions made this paper simpler and with stronger results, and CAPES (an agency of the Brazilian government) for financial support.

## References

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

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

[3] B. Mazur. Frobenius and the Hodge filtration, estimates. *Ann. Math.*, 98:58–95, 1973.

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

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

University of California, Department of Mathematics, Santa Barbara, CA – 93106

*E-mail address*: `finotti@math.ucsb.edu`