CANONICAL AND MINIMAL DEGREE LIFTINGS OF CURVES

by

LUíS RENATO ABIB FINOTTI, B.S., M.S.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

August 2001

The Dissertation Committee for Luís Renato Abib Finotti
Certifies that this is the approved version of the following dissertation:

CANONICAL AND MINIMAL DEGREE LIFTINGS OF CURVES

Committee:

José Felipe Voloch, Supervisor

Fernando Rodriguez-Villegas

Judy Walker

John Tate

Jeffrey Vaaler

I dedicate this work to the people that guided me through the different paths of life and knowledge: my parents, my godparents and my family; my advisors, Felipe Voloch and Paulo A. Martin; the professors Daniel Levcovitz, John Tate, Fernando Rodriguez-Villegas and Jeff Vaaler; my dearest friend, Heather Lehr.

Acknowledgments

The author would like to thank: Felipe Voloch, for his many suggestions and ideas and most valuable discussions, the referee from the Journal of Number Theory, who is currently analyzing a paper consisting of the basic ideas of chapter 2, whose comments gave stronger results with easier proofs, and CAPES, an institution of the Brazilian government, for financial support. Also, the author acknowledges the use of the softwares Magma and Mathematica for the computations mentioned in the text.

CANONICAL AND MINIMAL DEGREE LIFTINGS OF CURVES

Publication No. ____________________

Luís Renato Abib Finotti, Ph.D.
The University of Texas at Austin, 2001

Supervisor: José Felipe Voloch

We first find upper bounds for the degrees of the coordinate functions of the elliptic Teichmüller lift of an ordinary elliptic curve over a perfect field of characteristic $p > 0$, giving exact conditions for the bound to be achieved. Also, we give an algorithm to compute the reduction modulo p^3 of the canonical lift and the elliptic Teichmüller.

Next, motivated by coding theory, we look for lifts with degrees smaller than the degrees of the elliptic Teichmüller, finding again some upper bounds. We obtain some more precise information about those lifts modulo p^3, such as precise degrees and verify that we can lift of the Frobenius on the affine parts. We again show how to compute those lifts.

We then compute lifts of hyperelliptic curves with "small" degrees, give a lower bound for these degrees and conditions to achieve this bound. Finally, we give an example of a lift that is possibly a Mochizuki lift.

Table of Contents

Chapter 1

Introduction

Let k be a perfect field of characteristic $p > 0$. An elliptic curve E over k is **ordinary** if $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$, for all $r \geq 1$. If $p \neq 2$ and E is given by an equation

$$E/k : \quad y_0^2 = f(x_0),$$

then E is ordinary if, and only if, the coefficient of x_0^{p-1} of $f(x_0)^{(p-1)/2}$, say A, is non zero. (Theorem V.4.1 of [7].) This A is called the **Hasse invariant** of E. (Note that this implies that if σ is the Frobenius of k and E is ordinary, then E^σ is also ordinary. Also, our definition is different from the one given in [7]: if $A \neq 0$, Silverman defines the Hasse invariant to be one.)

Ordinary elliptic curves have associated to them **canonical lifts** over the ring of Witt vectors $W(k)$ (see [2]), meaning that for every ordinary E/k we have a *unique* (up to isomorphism) elliptic curve $\boldsymbol{E}/W(k)$, whose reduction modulo p is E, and a lift of points $\tau : E(\bar{k}) \to \boldsymbol{E}(W(\bar{k}))$, called the **elliptic Teichmüller lift**, that is an injective group homomorphism. Moreover, if we also denote by σ the Frobenius of $W(k)$, i.e.,

$$(a_0, a_1, a_2, \dots)^\sigma = (a_0^\sigma, a_1^\sigma, a_2^\sigma, \dots) = (a_0^p, a_1^p, a_2^p, \dots),$$

the canonical lift of E^σ is $\boldsymbol{E}^\sigma$ and if $\phi : E \to E^\sigma$ is the Frobenius (for curves over k), there exists a **lift of the Frobenius** associated to τ, i.e., a map, that we will also denote by ϕ, from $\boldsymbol{E}$ to $\boldsymbol{E}^\sigma$ that makes the following diagram commute:

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

(In fact, one has that $\phi(\tau(P)) = \tau(P)^\sigma$, for all $P \in E(\bar{k})$.)

Thus

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

We notice that we can always identify $\boldsymbol{E}/W(k)$ with its **Greenberg transform** $G(\boldsymbol{E})/k$, that is the infinite dimensional scheme given by the equations (over k) that appear in the coordinates of the equation of $\boldsymbol{E}$. With this identification, τ becomes simply

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

(In this perspective, the map τ is defined over k.) As we shall soon verify (proposition 2.2), the x_n's and y_n's are polynomials in x_0 and y_0.

Voloch and Walker in [9] applied this theory of canonical lifts of elliptic curves to construct error-correcting codes. In that paper, the degrees of x_n and y_n have some importance in estimating exponential sums, that tells us how "good" the obtained codes possibly are.

In chapter 2 we analyze the degrees of the elliptic Teichmüller lift, 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.

While trying to compute canonical lifts, I found some lifts modulo p^3 that I thought to be the canonical, but as it turned out, those lifts were defined only on the affine part of the curve. On the other hand, those lifts had degrees smaller than the elliptic Teichmüller itself, and for the purposes of constructing codes, those might be even better, since smaller degrees would probably give better codes. In chapter 3, we discuss the existence of such lifts, analyze the possible degrees and check when the Frobenius will lift for the affine parts of the curves.

Voloch and Walker in [8] also used non elliptic curves to construct codes. On the other hand, if the genus of the curve is greater than 1, there is no lift of the Frobenius. (See [5].) We can construct lifts though, by purely algebraic techniques, which is done also in chapter 3 for hyperelliptic curves, since the techniques are the same as the ones we would use for elliptic curves. But in chapter 4 we look at the minimal possible degrees with a more theoretical approach, finding a lower bound for the degrees and a necessary condition to achieve that bound. (The condition also seems to be sufficient!)

Finally, on the last part of chapter 4, we try to find a **Mochizuki lift** of a curve of genus 2 in characteristic 3. In [4], Mochizuki proves that if we take off an appropriate set of $(p-1)(g-2)$ points of an "ordinary" curve of genus g over a perfect field of characteristic p, we have the existence of a lift with "small" degrees for which the Frobenius lifts. Not many examples of such lifts are known, and in this last part of the chapter, we follow an idea given to the author by Voloch, to try to find an example. We computed the lift modulo p^3 to verify that we can indeed lift the Frobenius, at least modulo p^3.

Chapter 2

Degrees of the Elliptic Teichmüller Lift

2.1 Introduction

Let E/k be an *ordinary* elliptic curve over a perfect field k of characteristic $p > 0$. If $p \neq 2, 3$, we will assume that such a curve is given by the equation:

$$E/k : \quad y_0^2 = x_0^3 + a_0 x_0 + b_0.$$

Let

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

be its canonical lift, where $\boldsymbol{a} = (a_0, a_1, \dots)$ and $\boldsymbol{b} = (b_0, b_1, \dots)$.

We will consider only ordinary elliptic curves, and thus, for $p = 2$ and $p = 3$, we will *always* assume, by extending k if necessary, that E has the forms $y_0^2 + x_0 y_0 = x_0^3 + a_0$ and $y_0^2 = x_0^3 + x_0^2 + a_0$ respectively, and we can assume that their canonical liftings have similar forms.

Let $\tau : E(\bar{k}) \to \boldsymbol{E}(W(\bar{k}))$, denote the *elliptic Teichmüller lift* of E:

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

or, identifying $\boldsymbol{E}/W(k)$ with its *Greenberg transform* $G(\boldsymbol{E})/k$, we can see τ as

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

For $n > 1$, theorem 4.1 in [9] tells us that $\deg x_n \circ \tau \leq 2^{n+1}p^n$ and $\deg y_n \circ \tau \leq 3\,(2p)^n$. In that same paper, better bounds were proved for $n = 1$ in proposition 4.2, and we use similar ideas to improve the bounds for $n > 1$. The goal is to prove:

Theorem 2.1. *An upper bound for the degrees of the composition of τ with coordinate functions x_n's is $(n+2)p^n - np^{n-1}$, and with the y_n's is $(n+3)p^n - np^{n-1}$.*

We may sometimes write, for simplicity, x_n meaning $x_n \circ \tau$, and the same for y_n, $\boldsymbol{x}$ and $\boldsymbol{y}$.

Proposition 2.2. *The function x_n is a polynomial in x_0 and the function y_n is a polynomial in x_0 and y_0. Moreover, if $p \neq 2$, then y_n is a product of y_0 with a polynomial in x_0.*

Proof. We have that τ is a morphism from E to $G(\boldsymbol{E})$. Thus, the maps have to be given by rational functions on x_0 and y_0, over k. But using the equation defining E, we may write

$$x_n = \frac{F_1(x_0) + y_0 G_1(x_0)}{F_2(x_0) + y_0 G_2(x_0)},$$

where the F_i's and G_i's are polynomials.

Since τ is injective, the only point mapped to $\boldsymbol{O}$, the origin of $\boldsymbol{E}$, is O, the origin of E, i.e., τ maps the affine part of E into the affine part of $\boldsymbol{E}$. So x_n cannot have poles in the affine part of E, and therefore the denominator of x_n can be taken to be constant. Thus, we can write

$$x_n = F(x_0) + y_0 G(x_0),$$

with F and G polynomials. A similar argument shows that y_n is also a polynomial in x_0 and y_0.

If $(x_0, y_0) \in E(\bar{k})$, then its inverse with respect to the group law is $(x_0, -y_0)$, for $p \neq 2$, or $(x_0, x_0 + y_0)$, for $p = 2$. Since τ is a homomorphism, for $p \neq 2$, we have that $\tau(x_0, -y_0)$ is the inverse of $\tau(x_0, y_0)$. But if

$$\tau(x_0, y_0) = (x_0, x_1, \dots, x_i, \dots, y_0, y_1, \dots, y_i, \dots) = (\boldsymbol{x}, \boldsymbol{y}),$$

since the inverse of $(\boldsymbol{x}, \boldsymbol{y})$ is $(\boldsymbol{x}, -\boldsymbol{y})$, we get

$$\tau(x_0, -y_0) = (\boldsymbol{x}, -\boldsymbol{y}) = (x_0, x_1, \dots, x_i, \dots, -y_0, -y_1, \dots, -y_i, \dots),$$

observing that for $p \neq 2$,

$$-\boldsymbol{s} = -(s_0, s_1, \dots) = (-s_0, -s_1, \dots).$$

Thus, $x_n \circ \tau(x_0, y_0) = x_n \circ \tau(x_0, -y_0)$, i.e., $F(x_0) + y_0 G(x_0) = F(x_0) - y_0 G(x_0)$, what gives us $G = 0$.

A similar argument with inverses gives the result for y_n.

If $p = 2$, we just need to observe that $x_n(x_0, y_0) = x_n(x_0, x_0 + y_0)$, i.e., $x_0 G(x_0) = 0$, for any x_0. Thus $G = 0$ and x_n is a polynomial in x_0.

$\square$

Thus, $\deg x_n = -\operatorname{ord}_O x_n$ and $\deg y_n = -\operatorname{ord}_O y_n$. (Unless mentioned otherwise, we will use the word "degree" for degree as functions on E, *not as polynomials*.) Then, we may look at ord_O instead of deg to prove the theorem, i.e., it suffices to prove that $\operatorname{ord}_O x_n \geq -(n+2)p^n + np^{n-1}$ and $\operatorname{ord}_O y_n \geq -(n+3)p^n + np^{n-1}$.

2.2 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 [6].)

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

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

We start with an elementary lemma that we shall use soon:

Lemma 2.3. *Let v_p denote the p-adic valuation on $\mathbb{Z}$. Then*

$$v_p\left(\binom{p^t}{i}p^i\right) = t + i - v_p(i), \quad \text{for } i = 1, \ldots, p^t.$$

In particular,

$$\binom{p^t}{i}p^i \equiv 0 \pmod{p^{t+1}}.$$

Proof. We prove it by induction on i. The case $i = 1$ is trivial. Now suppose true for some $i < p^t$ and we prove for $i + 1$. We have

$$\begin{aligned} v_p\left(\binom{p^t}{i+1}p^{i+1}\right) &= v_p\left(\binom{p^t}{i}p^i\,\frac{p^t - i}{i+1}\,p\right) \\ &= t + i - v_p(i) + v_p(p^t - i) - v_p(i+1) + 1 \\ &= t + (i+1) - v_p(i+1) + (v_p(p^t - i) - v_p(i)) \\ &= t + (i+1) - v_p(i+1), \end{aligned}$$

and the last equality holds since $i < p^t$.

The last part is trivially true, since $i > v_p(i)$. □

Now, let K be a field of characteristic $p > 0$, and let us consider $W(K)$. Since the entries of our Witt vectors are in characteristic p, we can use the polynomials $\bar{S}_n, \bar{P}_n \in \mathbb{F}_p[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$, that are the reductions of S_n, P_n modulo p, to give us the sum and product of Witt vectors.

We now introduce four technical lemmas that will be useful in estimating degrees.

Lemma 2.4. *The monomials $\prod X_i^{a_i} \prod Y_j^{b_j}$ (disregarding the coefficient) occurring in $\bar{P}_n$ satisfy*

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

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

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:

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

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 $t = 0, \ldots, n-1$, 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 $\frac{1}{p^t} P_{n-t}^{p^t}$ to $\bar{P}_n$: that is given by the monomials of $\tilde{P}_{n-t}^{p^t}$ (by lemma 2.3), 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 K. For $e \geq 0$, define:

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

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

Lemma 2.5. *The set $U(e)$ is a subgroup of $W(K)^\times$.*

Proof. Let $\boldsymbol{s}, \boldsymbol{t} \in U(e)$. We have that the $(n+1)$-th coordinate of $\boldsymbol{s}\,\boldsymbol{t}$ is given by $\bar{P}_n(\boldsymbol{s}, \boldsymbol{t})$. By lemma 2.4, 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, $v(\bar{P}_n(\boldsymbol{s},\boldsymbol{t})) \geq p^n(v(s_0t_0) - ne)$ 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 2.6. *Let $\boldsymbol{s},\boldsymbol{t} \in U(e)$, and assume $v(t_0) > v(s_0)$. Then $v(\bar{S}_n(\boldsymbol{s},\boldsymbol{t})) \geq p^n(v(s_0) - ne)$. Moreover, if $e > 0$, the equality holds if, and only if, $v(s_n) = p^n(v(s_0) - ne)$.*

Proof. We prove by induction on n. For $n = 0$, it is trivial, since $\bar{S}_0(\boldsymbol{s},\boldsymbol{t}) = s_0 + t_0$. We have

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

and again we observe that this polynomial has integer coefficients. Notice that, when taking the valuation in $\bar{S}_n$, we can again disregard the coefficients of the monomials $\prod X_i^{a_i} \prod Y_j^{b_j}$ that appear in S_n. So, we assume (inductively) that every monomial of that form in S_t, for $t = 0, \ldots, (n-1)$, is such that

$v(\prod s_i^{a_i} \prod t_j^{b_j}) \geq p^t(v(s_0) - te)$. So, the monomials of $S_t^{p^{n-t}}$ are products of p^{n-t} monomials of S_t, and therefore they have valuation, when computed at $\boldsymbol{s}$ and $\boldsymbol{t}$, greater than or equal to $p^{n-t}p^t(v(s_0) - te) \geq p^n(v(s_0) - ne)$, and equality never holds if $e > 0$. The remaining monomials of S_n are of the forms $X_i^{p^{n-i}}$ and $Y_j^{p^{n-j}}$. The former gives valuations greater than or equal to $p^n(v(s_0) - ie) \geq p^n(v(s_0) - ne)$, and if $e > 0$, we have the equality only for $i = n$ and $v(s_n) = p^n(v(s_0) - ne)$. The latter gives valuation greater than or equal to $p^n(v(t_0) - je) > p^n(v(s_0) - ne)$, which finishes the proof.

□

Lemma 2.7. *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 $v(s_n) \geq 1 \geq p^n[1 - n(p-1)/p] = np^{n-1} - (n-1)p^n$. □

2.3 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 of $\boldsymbol{g} \in \boldsymbol{K}$ 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 $\boldsymbol{g}_2 \not\equiv 0 \pmod{p}$ (i.e., $\boldsymbol{R}$ is the valuation ring of $\boldsymbol{K}$ with respect to the valuation associated to p). Then, for every $\boldsymbol{g} \in \boldsymbol{R}$, we have that $\boldsymbol{g} = (g_0, g_1, \dots) \in W(K)$, and if $\boldsymbol{g}$ is regular at $\tau(P)$, for $P \in E(\bar{k})$, then $\boldsymbol{g}(\tau(P)) = (g_0(P), g_1(P), \dots)$.

Observe that since $\mathrm{ord}_{\boldsymbol{O}}\, \boldsymbol{x}/\boldsymbol{y} = \mathrm{ord}_{\boldsymbol{O}}\, \boldsymbol{y}/\boldsymbol{x}^2 = 1$, both $\boldsymbol{x}/\boldsymbol{y}$ and $\boldsymbol{y}/\boldsymbol{x}^2$ satisfy the conditions of lemma 2.7, and thus they are in the subgroup $U((p-1)/p)$ of $\boldsymbol{R}^\times$. This implies that $\boldsymbol{x}$ and $\boldsymbol{y}$ are also in that group, which proves theorem 2.1.

In fact the same idea can be used to prove a more general statement:

Theorem 2.8. *Let* $\boldsymbol{g} = (g_0, g_1, \dots) \in \boldsymbol{R}^\times$ *such that* $\operatorname{ord}_P g_0 = \operatorname{ord}_{\tau(P)} \boldsymbol{g}$ *for some* $P \in E(\bar{k})$. *Then*

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

Proof. Let $\boldsymbol{\pi} \in \boldsymbol{R}^\times$ be such that $\operatorname{ord}_{\tau(P)} \boldsymbol{\pi} = 1$, i.e., a uniformizer at $\tau(P)$. (Note we can choose $\boldsymbol{\pi}$ as either $(\boldsymbol{x} - \boldsymbol{x}(\tau(P)))$, $\boldsymbol{y}$ or $\boldsymbol{x}/\boldsymbol{y}$, and so $\operatorname{ord}_P \pi_0 = 1$.) By lemma 2.7, $\boldsymbol{\pi} \in U((p-1)/p)$, 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, $\boldsymbol{g} \in U((p-1)/p)$.

□

We observe that if $\operatorname{ord}_{\tau(P)} \boldsymbol{g} < 0$, then the theorem above 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 $n < p(\operatorname{ord}_P g_0)/(p-1)$.

2.4 Leading Coefficients

Our main goal in this section is to verify when we don't have the equality in the upper bounds of theorem 2.1. But since the same techniques give stronger results, we will obtain these results first, and then get our main goal as a corollary.

Let $\boldsymbol{g}$ be a function as in the theorem 2.8 and let π_0 be a uniformizer at P. Let the expansion of g_n in terms of π_0 be

$$g_n = b_n(\boldsymbol{g})\pi_0^{p^n(\operatorname{ord}_P(g_0)-n)+np^{n-1}} + \dots, \tag{2.5}$$

where the omitted terms have higher powers of π_0 (by theorem 2.8). We call $b_n(\boldsymbol{g}) \in k$ the n**-th leading coefficient** of $\boldsymbol{g}$ at P, relative to π_0.

Let $P \in E(\bar{k})$ and, for $p \neq 2$, define

$$\boldsymbol{\pi} \stackrel{\text{def}}{=} \begin{cases} \boldsymbol{x}/\boldsymbol{y}, & \text{if } P = O; \\ (\boldsymbol{x} - \boldsymbol{x}(\tau(P))), & \text{if } 2P \neq O; \\ \boldsymbol{y}, & \text{otherwise.} \end{cases} \tag{2.6}$$

For $p = 2$, we define

$$\boldsymbol{\pi} \stackrel{\text{def}}{=} \begin{cases} \boldsymbol{x}/\boldsymbol{y}, & \text{if } P = O; \\ (\boldsymbol{x} - \boldsymbol{x}(\tau(P))), & \text{if } x_0(P) \neq 0; \\ \boldsymbol{y}, & \text{if } x_0(P) = 0; \end{cases} \tag{2.7}$$

So $\boldsymbol{\pi}$ is a uniformizer at $\tau(P)$. (Remember that τ is an injective homomorphism.) Also, if we write $\boldsymbol{\pi} = (\pi_0, \pi_1, \dots)$, we have that π_0 is a uniformizer at P. Moreover, $\operatorname{ord}_P \pi_n \geq 0$ for all $n \geq 0$. Then, write

$$\pi_1 = \alpha\, \pi_0 + \dots$$

where the omitted terms have larger powers of π_0. We have then:

Theorem 2.9. *Let $\boldsymbol{\pi}$ be as above and $\boldsymbol{g}$ as in theorem 2.8. Let $v_0 \stackrel{\text{def}}{=} \operatorname{ord}_P g_0$ and write*

$$\boldsymbol{g} = \boldsymbol{c}\boldsymbol{\pi}^{v_0} + \dots \quad (\boldsymbol{c} = (c_0, c_1, \dots) \in W(k))$$

where the omitted terms have larger powers of $\boldsymbol{\pi}$. We then have

$$\frac{b_n(\boldsymbol{g})}{c_0^{p^n}} = \binom{v_0}{n} \alpha^{np^{n-1}}.$$

Proof. Note that the theorem is trivially true for $\boldsymbol{\pi}$ itself: for $n > 1$, $p^n(1 - n) + np^{n-1} < 0$, and since $\operatorname{ord}_P \pi_n > 0$, $b_n(\boldsymbol{\pi}) = 0$ for $n > 1$.

Now, by induction, we prove that the theorem is true for $\boldsymbol{\pi}^r$, with $r > 0$: suppose the theorem is true for $\boldsymbol{\pi}^{r-1}$. Write

$$\boldsymbol{\pi}^{r-1} = (u_0, u_1, \dots) \quad \text{and} \quad \boldsymbol{\pi}^r = (v_0, v_1, \dots).$$

Then

$$v_n = \sum_{i=0}^{n} \pi_i^{p^{n-i}} u_{n-i}^{p^i} + \dots$$

where all the omitted terms have order larger than $p^n(r-n)+np^{n-1}$, by lemma 2.4. Thus,

$$\begin{aligned} b_n(\boldsymbol{\pi}^r) &= \sum_{i=0}^{n} b_i(\boldsymbol{\pi})^{p^{n-i}} b_{n-i}(\boldsymbol{\pi}^{r-1})^{p^i} = \left[\sum_{i=0}^{n} \binom{1}{i}\binom{r-1}{n-i}\right] \alpha^{np^{n-1}} \\ &= \left[\sum_{i=0}^{1} \binom{1}{i}\binom{r-1}{n-i}\right] \alpha^{np^{n-1}} = \binom{r}{n}\alpha^{np^{n-1}}. \end{aligned}$$

For $r < 0$, we prove by induction on n. Let

$$\boldsymbol{\pi}^{-r} = (u_0, u_1, \dots) \quad \text{and} \quad \boldsymbol{\pi}^r = (v_0, v_1, \dots).$$

Suppose true for $i = 0, \dots, n-1$. Then,

$$\sum_{i=0}^{n} u_i^{p^{n-i}} v_{n-i}^{p^i} + \dots = 0$$

where all the omitted terms have order larger than $-np^n + np^{n-1}$. So, the terms of order $-np^n + np^{n-1}$ have to cancel, i.e.,

$$\begin{aligned} b_0(\boldsymbol{\pi}^{-r})^{p^n} b_n(\boldsymbol{\pi}^r) &= -\sum_{i=1}^{n} b_i(\boldsymbol{\pi}^{-r})^{p^{n-i}} b_{n-i}(\boldsymbol{\pi}^r)^{p^i} \\ &= -\sum_{i=1}^{n} \binom{-r}{i}\binom{r}{n-i}\alpha^{np^{n-1}} = \binom{-r}{n}\alpha^{np^{n-1}}, \end{aligned}$$

what gives the result, since $b_0(\boldsymbol{\pi}^{-r})^{p^n} = 1$.

For $\boldsymbol{c\pi}^r$, by looking at the expression (2.3) and using lemma 2.4, one can check that the leading term will just be multiplied by $c_0^{p^n}$: write $\boldsymbol{\pi}^r = (u_0, u_1, \dots)$ and consider the monomials in $\bar{P}_n$ of the form $\prod X_i^{a_i} \prod Y_j^{b_j}$. Then, defining $v \stackrel{\text{def}}{=} \operatorname{ord}_P$, in the $(n+1)$-th coordinate of $\boldsymbol{c\pi}^r$ we have valuations of the form

$$\begin{aligned} v\left(\prod u_i^{a_i} \prod c_j^{b_j}\right) &= \sum a_i\, v(u_i) \\ &\geq r\left[\sum a_i\, p^i\right] - \frac{p-1}{p}\left[\sum a_i\, i\, p^i\right] \\ &\geq rp^n - \frac{p-1}{p} np^n, \end{aligned}$$

and it is clear that the equality can occur only if the monomial is $X_n Y_0^{p^n}$. Thus, the formula is true for $\boldsymbol{c\pi}^r$.

Finally we observe that if we write $\boldsymbol{g}$ as in the statement of the theorem, the higher powers of $\boldsymbol{\pi}$ will contribute to the $(n+1)$-th coordinate with terms with powers of π_0 higher than $p^n(v_0 - n) + np^{n-1}$ (as one can see from the proof of lemma 2.6), and so $b_n(\boldsymbol{g}) = b_n(\boldsymbol{c\pi}^{v_0})$, and our formula holds for $\boldsymbol{g}$.

$\square$

Then, using the same notation as before, the above theorem tells us that the map

$$\Phi : \boldsymbol{g} \mapsto \frac{1}{c_0}\left[\sum_{n=0}^{\infty} b_n(\boldsymbol{g})^{p^{-n}} T^n\right],$$

is such that $\Phi(\boldsymbol{g}) = (1 + \alpha^{p^{-1}} T)^{v_0}$.

Now, assuming $p \neq 2$, we compute the α's for the three distinct choices of $\boldsymbol{\pi}$. Assume that E is given by

$$E/k : \quad y_0^2 = f(x_0).$$

Let $P = (r_0, s_0)$, such that $2P \neq O$. Then, we take the uniformizer at $\tau(P) = (\boldsymbol{r}, \boldsymbol{s})$ given by $(\boldsymbol{x} - \boldsymbol{r})$. So,

$$\pi_1 = x_1 - r_1 + \frac{x_0^p - r_0^p - (x_0 - r_0)^p}{p} \quad (r_1 \overset{\text{def}}{=} x_1(r_0)).$$

(We here face a small notation problem: the above expression is in characteristic p, and so it would make no sense dividing by p. One should read an expression as the one above in the following way: first to consider a corresponding polynomial in characteristic zero, in this case $t(x, r) \overset{\text{def}}{=} ((x^p - r^p) - (x - r)^p)/p \in \mathbb{Z}[x, r]$, and then read:

$$\frac{x_0^p - r_0^p - (x_0 - r_0)^p}{p} \overset{\text{def}}{=} t(x_0, r_0).$$

Unfortunately this abuse of notation will appear several times, but we hope that no confusion will arise from it.)

Note that π_1 is a polynomial in x_0, and therefore, $\alpha = d\pi_1/dx_0|_{x_0 = r_0}$. But

$$\frac{d\pi_1}{dx_0} = \frac{dx_1}{dx_0} + x_0^{p-1} - (x_0 - r_0)^{p-1}.$$

We observe that from the proof of proposition 4.2 in [9], one can deduce:

$$\frac{dx_1}{dx_0} = A^{-1} y_0^{p-1} - x_0^{p-1} = A^{-1} f(x_0)^{(p-1)/2} - x_0^{p-1}, \tag{2.8}$$

for $p \neq 2$, where A is the Hasse invariant of the curve. (Note that $A \neq 0$, since our elliptic curve is ordinary.)

Therefore,

$$\frac{d\pi_1}{dx_0} = A^{-1} f(x_0)^{(p-1)/2} - (x_0 - r_0)^{p-1},$$

and hence,

$$\alpha = A^{-1} f(r_0)^{(p-1)/2}.$$

(Note that since $2P \neq O$, $\alpha \neq 0$.)

If $P = (r_0, s_0)$ is finite and $2P = O$, then $f(r_0) = 0$, or $s_0 = 0$. So, we take $\boldsymbol{\pi} = \boldsymbol{y}$, and if we write $y_1 = y_0 F_1(x_0)$, where F_1 is a polynomial, then we have $\alpha = F_1(r_0)$.

To try to find a more explicit expression for $F_1(r_0)$, we look at the reduction modulo p^2 of the equation of $\boldsymbol{E}$. We assume here $p \neq 3$. The case $p = 3$ can be easily calculated, and gives similar results. So for $p \neq 2, 3$, we take $f(x_0) = x_0^3 + a_0 x_0 + b_0$. Then, 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:

$$\begin{aligned} 2y_0^p y_1 = {} & 3x_0^{2p} x_1 + a_0^p x_1 + a_1 x_0^p + b_1 \\ & + \frac{1}{p}\left(x_0^{3p} + a_0^p x_0^p + b_0^p - (x_0^3 + a_0 x_0 + b_0)^p\right). \end{aligned} \tag{2.9}$$

Writing $y_0^2 = f(x_0)$ and $y_1 = y_0 F_1(x_0)$, we get:

$$\begin{aligned} 2f(x_0)^{(p+1)/2} F_1(x_0) = {} & 3x_0^{2p} x_1 + a_0^p x_1 + a_1 x_0^p + b_1 \\ & + \frac{1}{p}\left(x_0^{3p} + a_0^p x_0^p + b_0^p - (x_0^3 + a_0 x_0 + b_0)^p\right). \end{aligned}$$

Taking derivatives with respect to x_0 of both sides, one gets

$$f'(x_0)\,F_1(x_0)+2f(x_0)\frac{dF_1}{dx_0}(x_0)=f'(x_0)\left[A^{-1}f'(x_0)^{p-1}-f(x_0)^{(p-1)/2}\right].$$

(We observe that the formula above is also true for $p=3$, as one can easily check.) So, $\alpha = F_1(r_0) = A^{-1}f'(r_0)^{p-1}$. Note that since the curve is non-singular, we have that $f'(r_0)\neq 0$.

Finally let $P=O$. Then, we take $\boldsymbol{\pi}=\boldsymbol{x}/\boldsymbol{y}$, and we have

$$\pi_1=\frac{x_1}{y_0^p}-\frac{y_1x_0^p}{y_0^{2p}}.$$

We observe that

$$x_0=\left(\frac{x_0}{y_0}\right)^{-2}+\dots \quad\text{and}\quad y_0=\left(\frac{x_0}{y_0}\right)^{-3}+\dots. \tag{2.10}$$

So, if $x_1=\beta x_0^{(3p-1)/2}+\dots$ and $y_1=y_0(\gamma x_0^{2p-2}+\dots)$, then we have

$$\pi_1=(\beta-\gamma)\frac{x_0}{y_0}+\dots.$$

Since $dx_1/dx_0=A^{-1}f(x_0)^{(p-1)/2}-x_0^{p-1}$, we have that $\beta=-2A^{-1}$. For $p\neq 3$, by looking at the terms of highest degrees in the equation (2.9), one gets that $\gamma=2/3\,\beta=-3A^{-1}$. So, in this case, $\alpha=A^{-1}$. For $p=3$, we refer to [9], where x_1 and y_1 where computed. We get then $\alpha=A^{-1}=1$. (Remember that, by our choice of the form of $f(x_0)$ for $p=3$, we always have $A=1$.)

For $P=O$ and $p=2$, we can follow the same idea above, and we also have formulas for x_1 and y_1 in [9]. Those give us $\alpha=1$.

Hence:

Corollary 2.10. *We have* $\deg x_n < (n{+}2)p^n - np^{n-1}$ *if, and only if, p divides* $(n{+}1)$, *and* $\deg y_n < (n{+}3)p^n - np^{n-1}$ *if, and only if, p divides* $(n{+}1)(n{+}2)/2$.

Proof. First, we remember that for x_n and y_n we have $\deg = -\operatorname{ord}_O$. So the order of x_n (resp. y_n) is larger than $(-2{-}n)p^n + np^{n-1}$ (resp. $(-3{-}n)p^n + np^{n-1}$) if, and only if, $b_n(\boldsymbol{x}) = 0$ (resp. $b_n(\boldsymbol{y}) = 0$), relative to the uniformizer $\boldsymbol{\pi} = \boldsymbol{x}/\boldsymbol{y}$.

But by theorem 2.9,

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

and

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

what gives the result, since $\alpha \neq 0$.

□

Remark. Note that since x_n is a polynomial, we have that the degree of x_n *as a polynomial in* x_0 is less than or equal to $r \stackrel{\text{def}}{=} \left[(n+2)p^n - np^{n-1}\right]/2$, and $b_n(\boldsymbol{x})$ is also the coefficient of x_0^r in x_n (using equation (2.10)). Also, if 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 $b_n(y)$ (again, using (2.10)).

2.5 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:

Proposition 2.11. *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 τ of the reduction from $G(\boldsymbol{E})$ to E, in the category of k-schemes over $E\backslash\{O\}$, given by*

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

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 τ is the elliptic Teichmüller lift.

Proof. The proof is just the last paragraph of the proof of proposition 4.2 in [9]. □

Note that in the general case, in contrast to what happens for the second coordinate (see proposition 4.2 in [9]), 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, we have that the elliptic curve

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

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

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

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:

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

Now, we proceed trying 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 [9]. So, we try to obtain the analogues of those results to deduce a way to compute the third coordinates.

As we observed before,

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

for $p \neq 2$. Following the same idea:

Proposition 2.12. *For $p \neq 2$, we have*

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

Proof. We consider the differential

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

where ϕ is the lift of the Frobenius. This is a well-defined holomorphic differential on $\boldsymbol{E}$, and its reduction modulo p, say ω, depends only on dx/y. (See [3].) On one hand, since this differential is holomorphic, it has the form $\boldsymbol{\alpha} d\boldsymbol{x}/\boldsymbol{y}$, where $\boldsymbol{\alpha} \in W(k)$, and so its reduction modulo p has the form $\alpha_0 dx_0/y_0$, where α_0 is just the reduction of $\boldsymbol{\alpha}$.

If we apply the Cartier operator, we get

$$C(\omega) = C\left(\alpha_0 \frac{dx_0}{y_0}\right) = \alpha_0^{1/p} A^{1/p} \frac{dx_0}{y_0}. \tag{2.11}$$

On the other hand, by [1], we know that the p-derivation

$$\delta\boldsymbol{u} \stackrel{\text{def}}{=} \frac{\boldsymbol{u}^\sigma \circ \phi - \boldsymbol{u}^p}{p}, \tag{2.12}$$

where $\boldsymbol{u}^\sigma$ is obtained by applying the Frobenius σ for Witt vectors on the coefficients of $\boldsymbol{u}$, is such that the reduction modulo p of $\delta^i \boldsymbol{x}$ is equal to $x_i + P_i$, where P_i is a polynomial in $x_0, \ldots x_{i-1}$ that we can compute explicitly. (Note that P_i is not the polynomial that defines the Witt product. From now on, we won't use those anymore, and the P_i's will always denote these universal polynomials arising from the reduction modulo p of $\delta^i \boldsymbol{x}$.) For $i = 1$ such a polynomial is zero, and for $i = 2$ (and $p \neq 2$),

$$P_2(x_0, x_1) \stackrel{\text{def}}{=} -x_0^{p(p-1)} x_1.$$

Since $\boldsymbol{u} \circ \phi = p\delta \boldsymbol{u} + \boldsymbol{u}^p$, we get

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

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

The reduction of such differential modulo p, that is again ω, 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 ω and using (2.8), we get

$$C(\omega) = \frac{1}{y_0^p}(dx_1 + x_0^{p-1}dx_0) = A^{-1}\frac{dx_0}{y_0}. \tag{2.13}$$

Comparing equations (2.11) and (2.13), we get that $\alpha_0 = A^{-(p+1)}$, and comparing the two forms for ω, we have

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

$\square$

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:

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

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 all the summands in

$$-\frac{x_1^p y_1^p}{y_0^{2p^2}} + \frac{x_2}{y_0^{p^2}} + \frac{x_0^{p^2} y_1^{2p}}{y_0^{3p^2}} - \frac{x_0^{p^2} y_2}{y_0^{2p^2}} \tag{2.14}$$

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.

Now for $p \neq 2, 3$, looking at the third coordinates of the expression of our elliptic curve, we have that

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

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 (2.14) that has to add up to have positive order is

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

Looking at the second coordinate of the equation of the elliptic curve, 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 (2.14) that has to add up to have positive order is

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

Using

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

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

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

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^{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 2.12, 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 2.11, allows us to deduce the following theorem:

Theorem 2.13. *If $p \neq 2,3$ and $\boldsymbol{E}/W_3(k)$ is an elliptic curve with reduction E, and if we have a section τ of the reduction from $G(\boldsymbol{E})$ to E, in the category of k-schemes over $E\backslash\{O\}$, 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 τ are the canonical lift and the elliptic Teichmüller modulo p^2, then the same is true modulo p^3 if, and only if, $\deg[x_0^{p^2}x_2 - 3/4\,x_1^{2p}] \leq 5p^2-1$. *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 2.12 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 p powers of x_0. $\square$

2.6 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 $p \neq 2, 3$.

First we compute x_1 by integrating formally the formula (2.8), and we leave the constant term, say c_0, and the coefficient of the term in x_0^p, say c_1, as indeterminates.

Since y_1 is y_0 times a polynomial in x_0, equation (2.9) (keeping a_1 and b_1 as indeterminates) tells us that the division of polynomials (in x_0)

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

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 [9] 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 2.12, 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 2.13 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 2.5. In fact, we were able to compute, using that algorithm, the canonical lift for a generic ordinary elliptic curve in characteristic 5: if

$$y_0^2 = x_0^3 + a_0x_0 + b_0$$

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

$$\begin{aligned}
a_1 &= a_0^2b_0^2 + \frac{b_0^4}{a_0}, \\
a_2 &= 2a_0^{25} + a_0^{22}b_0^2 + a_0^{19}b_0^4 + 3a_0^{16}b_0^6 + 2a_0^{13}b_0^8 + a_0^7b_0^{12} + 4a_0b_0^{16} \\
&\qquad + \frac{3b_0^{18}}{a_0^2} + \frac{4b_0^{20}}{a_0^5} + \frac{4b_0^{22}}{a_0^8} + \frac{4b_0^{24}}{a_0^{11}}, \\
b_1 &= 4a_0^6b_0 + a_0^3b_0^3 + b_0^5, \\
b_2 &= a_0^{36}b_0 + 4a_0^{33}b_0^3 + 3a_0^{27}b_0^7 + 4a_0^{21}b_0^{11} + 4a_0^{15}b_0^{15} + a_0^{12}b_0^{17} + 3a_0^6b_0^{21} + b_0^{25}.
\end{aligned}$$

(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

$$a_1 = 0, \qquad a_2 = 0,$$
$$b_1 = 4, \qquad b_2 = 0,$$

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 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 2.12, 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" ν in section 2.5.) 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. In the next chapter we will verify the existence of those lifts and estimate the degrees obtained.

Chapter 3

Minimal Degree Liftings of Elliptic Curves

3.1 Minimal Degrees

In section 2.5, we exhibited a map ν between the affine part of an elliptic curve (over a field k of characteristic 5) and its canonical lift with degree of x_2 smaller than the degree of the corresponding x_2 of the elliptic Teichmüller. We now study the existence of such maps with smaller degrees in more detail. We will show that the affine part of the canonical lifting always has a *unique* section of the reduction modulo p^{n+1}, for $p \neq 2$, with $\deg x_i \leq (3p^i + 1)$ and $\deg y_i \leq (i+3)p^i - ip^{i-1}$, for $i = 1, \ldots, n$.

In this section we will be a little more generic and consider *hyperelliptic* curves for $p \neq 2$. For simplicity, we shall write

$$C/k : \quad y_0^2 = f(x_0),$$

where f is a monic polynomial of degree $d \geq 3$ with simple roots, and

$$\boldsymbol{C}/W(k) : \quad \boldsymbol{y}^2 = \boldsymbol{f}(\boldsymbol{x}),$$

where $\boldsymbol{f}$ is a monic polynomial that reduces to f modulo p. Looking at the $(n+1)$-th coordinate of the equation of $\boldsymbol{C}$ we have:

$$2y_0^{p^n} y_n + \cdots = f'(x_0)^{p^n} x_n + \ldots \tag{3.1}$$

(where $f'(x_0)$ represents the formal derivative of $f(x_0)$) where neither x_n nor y_n appear in any of the omitted terms.

We shall use "$\deg_{x_0}$" to denote the degree as polynomial in x_0, to not be confused with "deg" that denotes degrees as functions on the curve. To make our exposition clearer, we introduce the following useful lemma:

Lemma 3.1. *Let $a, b, c \in k[x_0]$, with $\deg_{x_0}(a) = n$, $\deg_{x_0}(b) = m$, $\deg_{x_0}(c) = r$. Also, let $s \stackrel{\text{def}}{=} \max\{r, n+m-1\}$ and assume $(a,b) = 1$. Then, there exists a* unique *pair of polynomials $u, v \in k[x_0]$ with $\deg_{x_0}(u) \leq m-1$ and $\deg_{x_0}(v) \leq s-m$ such that $au + bv = c$.*

Proof. We follow the basic idea of lemma IV.1 in [8]. Let $L(i)$ denote the vector space of polynomials in $k[x_0]$ with degrees less than or equal to i. Consider the linear map

$$\psi : L(m-1) \oplus L(s-m) \to L(s),$$

given by $\psi(u,v) \stackrel{\text{def}}{=} au + bv$. Since $(a,b) = 1$, $\psi(u,v) = 0$ if, and only if, $u = bz$ and $v = -az$, for some polynomial $z \in k[x_0]$. But $\deg_{x_0}(u) \leq m-1 < \deg_{x_0}(b)$, what implies $u = z = 0$. Thus $\ker \psi = \{0\}$. Now, since $\dim L(i) = i+1$, comparing dimensions, we have that ψ is an isomorphism, and since $c \in L(s)$, there exist a *unique* pair u, v as in the statement. $\square$

We need to introduce some new notation here: for $r \geq 0$, let

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

Note that the proof of lemma 2.5 (that tells us that $U(e)$ is a group) can be used to prove that $U_r(e)$ is also a group.

Proposition 3.2. *Given* any *curve*

$$\boldsymbol{C}/W(k): \quad \boldsymbol{y}^2 = \boldsymbol{f}(\boldsymbol{x})$$

where $\boldsymbol{f}(\boldsymbol{x})$ is a monic polynomial of degree d with reduction $f(x_0)$ modulo p such that $(f(x_0), f'(x_0)) = 1$, then there exists a unique *lift of the affine part of the curve*

$$C/k : y_0^2 = f(x_0),$$

to the affine part of $\boldsymbol{C}$, say

$$\nu = ((x_0, \tilde{x}_1, \tilde{x}_2, \dots), (y_0, \tilde{y}_1, \tilde{y}_2, \dots)),$$

where $\tilde{x}_n$ is a polynomial in x_0 and $\tilde{y}_n$ is y_0 times a polynomial in x_0, with $\deg \tilde{x}_n \leq d(p^n+1)-2$ *and* $\deg \tilde{y}_n \leq [n(d-2)+d]p^n + [n(d-2)]p^{n-1}$. *Moreover, the degrees of the $\tilde{x}_n$ are minimal.*

Proof. We will consider groups of the form $U_r((d-2)(p+1)/p)$ (with an appropriate r), where the valuation is defined by $v \stackrel{\text{def}}{=} -\deg$. (Note that will be dealing only with polynomials in x_0 and y_0.)

We prove the theorem by induction on n. The case $n = 0$ is trivial. Now suppose we have ν up to the n-th coordinate. We construct $\tilde{x}_n$ and $\tilde{y}_n$ in the following way: observe that $(x_0, \tilde{x}_1, \dots, \tilde{x}_{n-1})$ and $(y_0, \tilde{y}_1, \dots, \tilde{y}_{n-1})$ are both in the group $U_{n-1}((d-2)(p+1)/p)$, by the induction hypothesis. We now "find" $\tilde{x}_n$ and $\tilde{y}_n$. Write down the $(n+1)$-th coordinate of the equation of $\boldsymbol{C}/W_{n+1}(k)$, regarding $\tilde{x}_n$ and $\tilde{y}_n$ as unknowns to be found. Since we want $\tilde{y}_n$ to be of the form $y_0\,\tilde{F}_n(x_0)$, with $\tilde{F}_n(x_0) \in k[x_0]$, we need in fact to find $\tilde{F}_n$.

We then have

$$-f'(x_0)^{p^n}\tilde{x}_n + 2f(x_0)^{(p^n+1)/2}\tilde{F}_n = \dots, \tag{3.2}$$

where no omitted term has $\tilde{x}_n$ nor $\tilde{y}_n$.

Looking carefully at the proof of 2.5, we notice that we actually bound *each summand* that appears in the $(n+1)$-th coordinate of product $\boldsymbol{s}\cdot\boldsymbol{t}$, with $\boldsymbol{s},\boldsymbol{t}\in U(e)$, by $p^n(v(s_0)+v(t_0)-ne)$. So, in particular, if $\boldsymbol{s},\boldsymbol{t}\in U_{n-1}(e)$, all the terms in the $(n+1)$-th coordinate of $\boldsymbol{s}\cdot\boldsymbol{t}$ that do not have s_n and t_n have to satisfy this bound, since they depend only on $(s_0,\dots,s_{n-1})$ and $(t_0,\dots,t_{n-1})$ (even though we would not have control over the terms with s_n and t_n).

Hence all the terms in (3.2) that do not involve $\tilde{x}_n$ or $\tilde{F}_n$ have degrees less than or equal to $[n(d-2)+2d]p^n+[n(d-2)]p^{n-1}$ (since the highest degrees should come from $\boldsymbol{x}^d$ and $\boldsymbol{y}^2$, by lemma 2.6).

Now let c denote the omitted terms of (3.2). (Note that c is a polynomial in x_0.) Let $a \stackrel{\text{def}}{=} -f'(x_0)^{p^n}$ and $b \stackrel{\text{def}}{=} 2f(x_0)^{(p^n+1)/2}$, and by lemma 3.1, there are u and v polynomials in x_0 such that $au+bv=c$, and $\deg u \leq d(p^n+1)-2$ and $\deg v \leq [n(d-2)+d]p^n+[n(d-2)]p^{n-1}-d$. So, we take $\tilde{x}_n \stackrel{\text{def}}{=} u$, and $\tilde{y}_n \stackrel{\text{def}}{=} y_0\, v$.

The minimality comes from the uniqueness in the lemma. We cannot have a $\tilde{\tilde{x}}_n$ with degree less than the degree of $\tilde{x}_n$, unless we allow $\deg \tilde{\tilde{y}}_n > [n(d-2)+d]p^n+[n(d-2)]p^{n-1}$. But in this case the degree of the left hand side of the equation

$$-f'(x_0)^{p^n}\tilde{\tilde{x}}_n + 2y_0^{p^n}\tilde{\tilde{y}}_n = \dots,$$

would have degree larger than the upper bound for the degree of the right hand side. Therefore, there can be no such pair $\tilde{\tilde{x}}_n, \tilde{\tilde{y}}_n$. $\square$

We call the above ν the **minimal lift** of C to $\boldsymbol{C}$ (**with respect to** $\boldsymbol{x}$). Therefore, although we may neglect to mention it, whenever we talk about minimal lifts, we will be considering the *affine parts* of the curves only.

One can also use the same approach to minimize the degrees of the y_n instead. In such case we get:

Proposition 3.3. *With the same hypothesis and notation as proposition 3.2, and assuming p does not divide $d-1$, there exists a unique lift ν with* $\deg \tilde{y}_n \leq 2(d-1)p^n + (d-2)$ *and* $\deg \tilde{x}_n \leq [n(d-2)+2]p^n + n(d-2)p^{n-1}$. *In this case,* $\deg \tilde{y}_n$ *is minimal.*

Proof. The proof follows the exact same idea as the proof of proposition 3.2: again we will work in $U((d-2)(p+1)/p)$ and we just apply lemma 3.1 with $a \stackrel{\text{def}}{=} 2f(x_0)^{(p^n+1)/2}$, $b \stackrel{\text{def}}{=} -f'(x_0)^{p^n}$, and c as before. $\square$

The above propositions have obvious applications to elliptic curves, by taking $d = 3$. But by theorem 2.1, we can see that taking E ordinary and $\boldsymbol{E}$ its canonical lift, we can have $\deg x_1 \leq 3p - 1$, $\deg y_1 \leq 4p - 1$. This gives the motivation for the following proposition, with better bounds to $\tilde{y}_n$:

Proposition 3.4. *Assume again the same hypothesis and notation from proposition 3.2 and suppose further that we have a lift modulo p^2, say*

$$\nu = ((x_0, \tilde{x}_1), (y_0, \tilde{y}_1)),$$

such that $\deg \tilde{x}_1 \leq dp - (d-2)$ *and* $\deg \tilde{y}_1 \leq (2d-2)p - (d-2)$. *Then, we can complete* ν *to*

$$\nu(x_0, y_0) = ((x_0, \tilde{x}_1, \tilde{x}_2, \dots), (y_0, \tilde{y}_1, \tilde{y}_2, \dots)),$$

with $\deg \tilde{x}_n \leq d(p^n + 1) - 2$ *and* $\deg \tilde{y}_n \leq [n(d-2) + d]p^n - n(d-2)p^{n-1}$ *in a* unique *way.*

Proof. The idea is that the restrictions on $\tilde{x}_1$ and $\tilde{y}_1$ allows us to work on $U((d-2)(p-1)/p)$ instead of $U((d-2)(p+1)/p)$. Inductively, the term c (as in the proof of proposition 3.2) will have degree less than or equal to $[n(d-2) + 2d]p^n - n(d-2)p^{n-1}$, and we just apply lemma 3.1 again. □

3.2 Minimal Degrees Modulo p^3

In this section we will consider elliptic curves only and $p \neq 2, 3$.

Proposition 3.2 gives us upper bounds for the minimal degrees. We notice that our choices for $\boldsymbol{E}$ (here denoting *any* curve with reduction E) give different $\tilde{x}_2$'s, and one can ask which choice would give us the minimal possible degree for $\tilde{x}_2$, which we shall call the **absolute minimal degree lift** of E, and exactly what degree would $\tilde{x}_2$ have. (Note that the absolute minimal lift is not necessarily unique.) In this section we try to answer these questions for the reduction modulo p^3, at least for an *ordinary* E.

First of all, we observe that modulo p^2, those answers are given by proposition 4.2 of [9]: the choice of curve that gives the minimal possible degree for $\tilde{x}_1$ is the canonical lift itself, the minimal degree map is the elliptic Teichmüller and the degree of $\tilde{x}_1$ (or x_1 in this case) is *exactly* $3p - 1$.

We remember here that we mentioned in section 2.6 that we could change the algorithm presented to compute the canonical lift to give a $\tilde{x}_2$ with degree $3p^2 - 1$, with the same derivative as x_2, at least in all cases we tried. By proposition 3.2, this map has minimal degree, meaning that no other lift *to the canonical lift* $\boldsymbol{E}$ could have smaller degrees.

We start our analysis with a conjecture:

Conjecture 3.5. *The division of polynomials*

$$\frac{3}{4}x_1^2 = [x_0^p f(x_0)^{(p+1)/2}]q(x_0) + r(x_0)$$

(where x_1 comes from the elliptic Teichmüller and E is given by $y_0^2 = f(x_0)$) is such that $\deg_{x_0} r(x_0) \leq (5p-1)/2$.

First, observe that the division algorithm tells us that $\deg_{x_0} r(x_0) \leq (5p+1)/2$, i.e., the bound is one more than the one stated in the conjecture. To verify the statement of conjecture 3.5 we wrote a routine in Magma that checked that it is true for *any* ordinary E in characteristic p from 5 to 877. We checked by formally integrating dx_1/dx_0 and adding $c_1 x_0^p + c_0$, leaving c_1 and c_0 as independent variables, so that we did not have to compute them precisely. Unfortunately, we don't have yet a proof.

We now show the implications of such conjecture in answering the question modulo p^3:

Theorem 3.6. *Assume conjecture 3.5 is true. Then, the absolute minimal degree lift*

$$\nu = ((x_0, x_1, \tilde{x}_2), (y_0, y_1, \tilde{y}_2))$$

is such that $\deg \tilde{x}_2 = 3p^2-1$ *and* $\boldsymbol{E}$ *is the canonical lift (modulo* p^3*). Moreover, we have that*

$$\frac{d\tilde{x}_2}{dx_0} = \frac{dx_2}{dx_0}.$$

Proof. First we observe, as we mentioned above, that $\boldsymbol{E}$ modulo p^2 has to be the canonical lift, and x_1 and y_1 come from the elliptic Teichmüller.

We now prove that we always have such a lift to the canonical lift. We will actually give a way to construct the absolute minimal degree lift: if

$$\tau = ((x_0, x_1, x_2), (y_0, y_1, y_2))$$

is the elliptic Teichmüller lift, we compute, using the division algorithm,

$$x_2 = f(x_0)^{(p^2+1)/2}\, q_1(x_0) + r_1(x_0) \quad (\deg_{x_0} r_1 \leq (3p^2+1)/2).$$

Now define $\tilde{x}_2 \stackrel{\text{def}}{=} r_1(x_0)$ and $\tilde{y}_2 \stackrel{\text{def}}{=} y_2 - y_0[f'(x_0)^{p^2} q_1(x_0)]/2$. Then, we have

$$2y_0^{p^2}\tilde{y}_2 - f'(x_0)^{p^2}\tilde{x}_2 = 2y_0^{p^2} y_2 - f'(x_0)^{p^2} x_2,$$

and thus, by equation (3.1),

$$\nu \stackrel{\text{def}}{=} ((x_0, x_1, \tilde{x}_2), (y_0, y_1, \tilde{y}_2))$$

is another lift from E to its canonical lift, and since $\deg \tilde{x}_2 \leq (3p^2+1)$, by proposition 3.2, it is the minimal lift. We now have to prove that $\deg \tilde{x}_2 = 3p^2-1$: let $d(x_0) \stackrel{\text{def}}{=} x_0^{p^2} x_2 - 3/4 x_1^{2p}$. So, theorem 2.13 tells us that $\deg_{x_0} d(x_0) = (5p^2-1)/2$. We can then write

$$\begin{aligned} x_0^{p^2} x_2 &= x_0^{p^2} f(x_0)^{(p^2+p)/2} q(x_0)^p + [r(x_0)^p + d(x_0)] \\ &= x_0^{p^2} f(x_0)^{(p^2+1)/2} \left[f(x_0)^{(p-1)/2} q(x_0)^p\right] + [r(x_0)^p + d(x_0)], \end{aligned} \tag{3.3}$$

with $\deg_{x_0}[r(x_0)^p + d(x_0)] = (5p^2 - 1)/2$ (since we are assuming the conjecture to be true), and thus it is the remainder of the division of $x_0^{p^2} x_2$ by $x_0^{p^2} f(x_0)^{(p^2+1)/2}$. We see then that $x_0^{p^2}$ divides this remainder and $\tilde{x}_2 = r_1(x_0) = [r(x_0)^p + d(x_0)]/x_0^{p^2}$, which implies that $\deg_{x_0} \tilde{x}_2 = (3p^2 - 1)/2$.

After we prove that this is indeed the absolute minimal lift of E, the last part of the statement of the theorem is just a consequence of equation (3.3): we have

$$\begin{aligned} x_2 &= f(x_0)^{(p^2+p)/2} q(x_0)^p + \frac{r(x_0)^p + d(x_0)}{x_0^{p^2}} \\ &= f(x_0)^{(p^2+p)/2} q(x_0)^p + \tilde{x}_2, \end{aligned}$$

and taking derivatives gives us the result.

Now, we prove that this indeed gives us the absolute minimal degree lift: assume we have some lift of E to some curve $\boldsymbol{E}$ (not necessarily the canonical lift) with $\deg \tilde{x}_2 \leq 3p^2 - 1$. Let

$$\tilde{\tilde{x}}_2 \stackrel{\text{def}}{=} \tilde{x}_2 + [q(x_0) f(x_0)^{(p+1)/2}]^p$$

(with the $q(x_0)$ from the conjecture) and

$$\tilde{\tilde{y}}_2 \stackrel{\text{def}}{=} \tilde{y}_2 + \frac{y_0}{2}[f'(x_0)^{p^2} f(x_0)^{(p-1)/2} q(x_0)^p].$$

Then,

$$\tilde{\nu} : (x_0, y_0) \mapsto ((x_0, x_1, \tilde{\tilde{x}}_2), (y_0, y_1, \tilde{\tilde{y}}_2)),$$

is another lift, since

$$2y_0^{p^2} \tilde{\tilde{y}}_2 - f'(x_0)^{p^2} \tilde{\tilde{x}}_2 = 2y_0^{p^2} \tilde{y}_2 - f'(x_0)^{p^2} \tilde{x}_2.$$

But then, by hypothesis,

$$x_0^{p^2} \tilde{\tilde{x}}_2 - \frac{3}{4} x_1^{2p} = x_0^{p^2} \tilde{x}_2 + \left[x_0^p\, q(x_0)\, f(x_0)^{(p+1)/2}\right]^p - \frac{3}{4} x_1^{2p} = x_0^{p^2} \tilde{x}_2 - r(x_0)^p$$

has degree, as a polynomial in x_0, less than or equal to $(5p^2-1)/2$. Theorem 2.13 then tells us that $\boldsymbol{E}$ is the canonical lift modulo p^3, $\tilde{\tilde{x}}_2$ and $\tilde{\tilde{y}}_2$ are x_2 and y_2 from the elliptic Teichmüller, and $\deg_{x_0}[x_0^{p^2}\tilde{x}_2 - r(x_0)] = (5p^2-1)/2$, what implies $\deg \tilde{x}_2 = 3p^2-1$.

□

Thus, if the conjecture is true, the minimal lift among all choices of curves $\boldsymbol{E}$ occurs for $\boldsymbol{E}$ equal to the canonical lift, and with this minimal degree of $\tilde{x}_2$ *exactly* $3p^2-1$.

Theorem 3.6 justifies why our modified algorithm (when we did not introduce the terms from x_1^{2p} in the computation of x_2) described in the end of the section 2.6 seems to work. That modified algorithm computes the absolute minimal degree lift and the canonical lift. Also, note that we can verify the existence of such lift with $\deg \tilde{x}_2 = 3p^2-1$ before we really have to compute x_2, since its existence depends only on the conjecture, that deals only with x_1 (which can be computed fairly fast). Using the modified algorithm, we can then compute $\tilde{x}_2$ and $\tilde{y}_2$ without computing x_2 and y_2. Our function written for Magma gives you an option to compute this absolute minimal degrees lift instead of the Teichmüller is this exact way. Note that the curve obtained by this algorithm is then *necessarily* the canonical lift.

3.3 Minimal Lifts and the Frobenius

Having a lift from E to $\boldsymbol{E}/W_2(k)$ is equivalent to having a lift of the Frobenius (see [1]) in the affine part of E. In fact, if the lift is given by

$$(x_0, y_0) \mapsto ((x_0, x_1), (y_0, y_1)),$$

one can define $\phi(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\text{def}}{=} (\boldsymbol{x}^p + p\boldsymbol{x}_1, \boldsymbol{y}^p + p\boldsymbol{y}_1)$, where $\boldsymbol{x}_1$ is any polynomial in $W_2(k)[\boldsymbol{x}]$ with reduction x_1 and $\boldsymbol{y}_1$ is any polynomial in $W_2(k)[\boldsymbol{x}, \boldsymbol{y}]$ with reduction y_1.

On the other hand, having a lift from E to $\boldsymbol{E}/W_3(k)$ just guarantees a lift of ϕ^2:

$$\phi^2(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\text{def}}{=} (\boldsymbol{x}^{p^2} + p\boldsymbol{x}_1^p + p^2(\boldsymbol{x}_2 - \boldsymbol{x}^{p(p-1)}\boldsymbol{x}_1), (\boldsymbol{y}^{p^2} + p\boldsymbol{y}_1^p + p^2(\boldsymbol{y}_2 - \boldsymbol{y}^{p(p-1)}\boldsymbol{y}_1))).$$

Of course, the canonical lift always has a lift of ϕ associated to τ. So, one could ask if the Frobenius also lifts (at least for the the affine parts) for these minimal lifts, making the diagram

$$\begin{array}{ccc} \boldsymbol{E}(W_3(\bar{k})) & \xrightarrow{\phi} & \boldsymbol{E}^\sigma(W_3(\bar{k})) \\ {\scriptstyle\nu}\big\uparrow & & \big\uparrow{\scriptstyle\nu} \\ E(\bar{k}) & \xrightarrow{\phi} & E^\sigma(\bar{k}) \end{array} \tag{3.4}$$

commute. (Here σ represents the Frobenius in k and $W(k)$.) Note that in the case where $\boldsymbol{E}$ is the canonical lift of E (and therefore $\boldsymbol{E}^\sigma$ is the canonical lift of E^σ), we cannot use the lift of the Frobenius associated to the elliptic Teichmüller, since the diagram would not commute.

Lemma 3.7. *Let $P(X, Y)$ be a polynomial over a field of characteristic zero.*

Then

$$
\begin{aligned}
&P(X_0 + pX_1, Y_0 + pY_1) \\
&\qquad \equiv P(X_0, Y_0) + p\left(\frac{\partial P}{\partial X}(X_0, Y_0)X_1 + \frac{\partial P}{\partial Y}(X_0, Y_0)Y_1\right) \pmod{p^2}.
\end{aligned}
$$

Proof. This is an easy application of Taylor's formula for P. □

Proposition 3.8. *Assume conjecture 3.5 is true. Let ν be the minimal lift from affine part of E (ordinary) to the affine part of $\boldsymbol{E}/W_3(k)$, such that, modulo p^2, ν gives us the Teichmüller. We have a lift of the Frobenius (for the affine parts) that make the diagram* (3.4) *commute if, and only if,* $\deg \tilde{x}_2 = 3p^2 - 1$ *(and then ν is the absolute minimal degree lift and $\boldsymbol{E}$ is the canonical lift).*

Proof. Note that the minimality of ν implies that $\boldsymbol{E}$ is the canonical lift modulo p^2. Now assume that we have a lift of ϕ associated to ν:

$$\phi(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}^p + p\boldsymbol{x}_1 + p^2\boldsymbol{P}, \boldsymbol{y}^p + p\boldsymbol{y}_1 + p^2\boldsymbol{Q}).$$

Let δ be the p-derivation associated to ϕ (as in equation (2.12)). We have

$$\delta\boldsymbol{x} = \boldsymbol{x}_1 + p\boldsymbol{P}$$

and, using lemma 3.7,

$$
\begin{aligned}
\delta^2\boldsymbol{x} &= \frac{(\boldsymbol{x}_1 + p\boldsymbol{P})^\sigma \circ \phi - (\boldsymbol{x}_1 + p\boldsymbol{P})^p}{p} \\
&= \frac{\boldsymbol{x}_1^\sigma(\boldsymbol{x}^p) - \boldsymbol{x}_1^p}{p} + \frac{d\boldsymbol{x}_1{}^\sigma}{d\boldsymbol{x}}(\boldsymbol{x}^p) \cdot \boldsymbol{x}_1 + \boldsymbol{P}^\sigma(\boldsymbol{x}^p) + p \cdot (\dots).
\end{aligned}
\tag{3.5}
$$

But, by [1], we have that the reduction modulo p of $\delta^2\boldsymbol{x}$ must be equal to $\tilde{x}_2 - x_0^{p(p-1)}x_1$. Taking derivatives, the reduction modulo p of $\boldsymbol{P}^\sigma(\boldsymbol{x}^p)$ vanishes (it is a p-power). So all that is left after taking derivative does not depend on $\boldsymbol{P}$, it depends only on x_1, and then, should give the same result as if we had used the lift of the Frobenius given by the elliptic Teichmüller (that maybe takes E to an $\boldsymbol{E}' \neq \boldsymbol{E}$, but necessarily $\boldsymbol{E}' \equiv \boldsymbol{E} \pmod{p^2}$). Therefore

$$\frac{d\tilde{x}_2}{dx_0} - x_0^{p(p-1)} \frac{dx_1}{dx_0} = \frac{dx_2}{dx_0} - x_0^{p(p-1)} \frac{dx_1}{dx_0}.$$

Since $\deg \tilde{x}_2 \leq 3p^2 + 1$ and it has the same derivative as x_2, we have $\deg \tilde{x}_2 = 3p^2 - 1$.

Conversely, assume ν is such that $\deg \tilde{x}_2 = 3p^2 - 1$. By theorem 3.6, the curve $\boldsymbol{E}$ is the canonical lift of E and $dx_2/dx_0 = d\tilde{x}_2/dx_0$. Hence, $\Delta x \stackrel{\text{def}}{=} x_2 - \tilde{x}_2$ is a p-power. This implies that $\Delta y \stackrel{\text{def}}{=} y_2 - \tilde{y}_2$ can also be written as a p-power, since

$$2y_0^{p^2} \Delta y = f'(x_0)^{p^2} \Delta x.$$

Let

$$\phi_1(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}^p + p\boldsymbol{x}_1 + p^2\boldsymbol{P}_1, \boldsymbol{y}^p + p\boldsymbol{y}_1 + p^2\boldsymbol{Q}_1)$$

be the Frobenius associated to τ. Define now $\boldsymbol{P}_2$ as $\boldsymbol{P}_1$ minus a lift of $(\Delta x)^{1/p}$, that we shall call $\Delta \boldsymbol{P}$, and $\boldsymbol{Q}_2$ as $\boldsymbol{Q}_1$ minus a lift of $(\Delta y)^{1/p}$, that we shall call $\Delta \boldsymbol{Q}$. We claim that in this case, the ϕ_2 as defined as

$$\phi_2(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}^p + p\boldsymbol{x}_1 + p^2\boldsymbol{P}_2, \boldsymbol{y}^p + p\boldsymbol{y}_1 + p^2\boldsymbol{Q}_2),$$

is a lift of the Frobenius associated to ν. First, we check that it is well defined: let $\mathcal{X} \stackrel{\text{def}}{=} \boldsymbol{x}^p + p\boldsymbol{x}_1 + p^2\boldsymbol{P}_1$ and $\mathcal{Y} \stackrel{\text{def}}{=} \boldsymbol{y}^p + p\boldsymbol{y}_1 + p^2\boldsymbol{Q}_1$. Then

$$\mathcal{Y}^2 \equiv \boldsymbol{f}^\sigma(\mathcal{X}) \pmod{p^3}$$

and we need to prove

$$(\mathcal{Y} - p^2 \Delta \boldsymbol{Q})^2 \equiv \boldsymbol{f}^{\sigma}(\mathcal{X} - p^2 \Delta \boldsymbol{P}) \pmod{p^3}.$$

But, applying lemma 3.7, that is equivalent to

$$2\mathcal{Y}\Delta \boldsymbol{Q} \equiv (\boldsymbol{f}')^{\sigma}(\mathcal{X}) \cdot \Delta \boldsymbol{P} \pmod{p},$$

or

$$2\, y_0^p\, (\Delta y)^{1/p} = f'(x_0)^p\, (\Delta x)^{1/p},$$

that we can see is true, by raising both sides of the equation to the p-th power.

Clearly ϕ_2 is a lift of the Frobenius, and the fact that it makes the diagram (3.4) commute is equivalent to the fact that $\delta_2 \boldsymbol{x} = \tilde{x}_2 - x_0^{p(p-1)} x_1$ and $\delta_2 \boldsymbol{y} = \tilde{y}_2 - y_0^{p(p-1)} y_1$, where δ_2 is the p-derivation associated to ϕ_2. This can be easily checked by noticing that the reduction of

$$\begin{aligned} \delta_i^2 \boldsymbol{x} &= \frac{(\boldsymbol{x}_1 + p\boldsymbol{P}_i)^{\sigma} \circ \phi_i - (\boldsymbol{x}_1 + p\boldsymbol{P}_i)^p}{p} \\ &= \frac{\boldsymbol{x}_1^{\sigma}(\boldsymbol{x}^p) - \boldsymbol{x}_1^p}{p} + \frac{d\boldsymbol{x}_1{}^{\sigma}}{d\boldsymbol{x}}(\boldsymbol{x}^p) \cdot \boldsymbol{x}_1 + \boldsymbol{P}_i^{\sigma}(\boldsymbol{x}^p) + p \cdot (\dots). \end{aligned} \tag{3.6}$$

for $i = 2$ differs from the reduction for $i = 1$ by Δx (that is, the p-power of the reduction of $\Delta \boldsymbol{P}$), and the analogue will hold for $\delta_2 \boldsymbol{y}$. □

The above proposition then says that conjecture 3.5 implies that the minimal degree lift from the affine part of E to the affine part of its canonical lift has a lift of the Frobenius associated to it.

Also, the proof the proposition also gives us:

Proposition 3.9. *Let C be the hyperelliptic curve*

$$C/k: \quad y_0^2 = f(x_0),$$

where f is a monic polynomial of degree $d \geq 3$ with simple roots, and suppose that we have a lift of C

$$\boldsymbol{C}/W_3(k): \quad \boldsymbol{y}^2 = \boldsymbol{f}(\boldsymbol{x}).$$

for which the Frobenius lift in the affine part of $\boldsymbol{C}$. Let

$$\nu \stackrel{\text{def}}{=} ((x_0, x_1, x_2), (y_0, y_1, y_2))$$

be the lift of points, and also assume that x_i is a polynomial in x_0. Then,

$$\frac{dx_2}{dx_0} = \left(\frac{dx_1}{dx_0}\right)^{p+1} + \left(\frac{dx_1}{dx_0}\right)^p x_0^{p-1} + \left(x_0^{p(p-1)} - x_1^{p-1}\right) \frac{dx_1}{dx_0}.$$

In particular, if $dx_1/dx_0 = \lambda\, y_0^{p-1} - x_0^{p-1}$ for some $\lambda \in k^*$, then

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

Proof. Let $\boldsymbol{x}_1$ and $\boldsymbol{y}_1$ be lifts of x_1 and y_1 to $W_3(k)[\boldsymbol{x}]$ and $W_3(k)[\boldsymbol{x}, \boldsymbol{y}]$ respectively. Then the lift of the Frobenius has the form

$$\phi(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}^p + p\boldsymbol{x}_1 + p^2\boldsymbol{P}, \boldsymbol{y}^p + p\boldsymbol{y}_1 + p^2\boldsymbol{Q}),$$

for some polynomials $\boldsymbol{P}$ and $\boldsymbol{Q}$. As in the proof of proposition 3.8, formula (3.5) also holds in this case. The reduction of this formula modulo p is equal to $x_2 - x_0^{p(p-1)}$, and taking derivatives of both sides of this equation gives the result. □

3.4 Characteristic 2

We now compute the canonical lifting and the elliptic Teichmüller modulo higher powers of 2 of an elliptic curve in characteristic 2, where our previous analysis does not apply. So, throughout this section we are going to fix $p = 2$.

An ordinary elliptic curve in characteristic 2 over an algebraic closed field (or over some finite extension of our original ground field k) can always be put in the form

$$y_0^2 + x_0\, y_0 = x_0^3 + a_0,$$

and so, we consider the canonical lift having the same form:

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

Voloch and Walker in [9] computed the reduction modulo 4, obtaining

$$a_1 = a_0^2, \quad x_1 = a_0, \quad y_1 = (x_0^2 + x_0)\, y_0 + x_0^3 + a_0\, x_0^2 + a_0.$$

(Notice that for $p = 2$, y_n is not necessarily y_0 times a polynomial in x_0.)

To compute the reduction modulo higher powers of 2, we first computed the derivative of x_n.

Theorem 3.10. *For $p = 2$ and $n \geq 1$, we have*

$$\frac{dx_n}{dx_0} = 0.$$

We are going to break the proof in small lemmas. But first, we introduce the notation

$$\mathcal{F} \stackrel{\text{def}}{=} \frac{1}{p}\phi^*,$$

where ϕ is the lift of the Frobenius. Also, we denote by δ the 2-derivation associated to ϕ.

Lemma 3.11. *We have that*

$$\mathcal{F}^n(d\boldsymbol{x}) = d(\delta^n \boldsymbol{x}) + \boldsymbol{x}^{2^n-1} d\boldsymbol{x} + \dots,$$

where every omitted term that contains $d\boldsymbol{x}$ *is a multiple of* 2 *and no other term contains* $d(\delta^n \boldsymbol{x})$*.*

Proof. We prove it by induction on n. For $n = 1$, we have:

$$\mathcal{F}(d\boldsymbol{x}) = \frac{d(\boldsymbol{x} \circ \phi)}{2} = \frac{d(\boldsymbol{x}^2 + 2\delta\boldsymbol{x})}{2} = \boldsymbol{x}\, d\boldsymbol{x} + d(\delta\boldsymbol{x}).$$

Suppose now the lemma true for n. We prove if for $n+1$:

$$\begin{aligned}
\mathcal{F}^{n+1}(d\boldsymbol{x}) &= \mathcal{F}(\mathcal{F}^n(d\boldsymbol{x})) = \mathcal{F}(d(\delta^n\boldsymbol{x}) + \boldsymbol{x}^{2^n-1} d\boldsymbol{x} + \dots) \\
&= (\delta^n\boldsymbol{x})\, d(\delta^n\boldsymbol{x}) + d(\delta^{n+1}\boldsymbol{x}) \\
&\quad + (\boldsymbol{x}^2 + 2\delta\boldsymbol{x})^{2^n-1} (\boldsymbol{x}\, d\boldsymbol{x} + d(\delta\boldsymbol{x})) + \dots \\
&= d(\delta^{n+1}\boldsymbol{x}) + \boldsymbol{x}^{2^{n+1}-2}(\boldsymbol{x}\, d\boldsymbol{x} + d(\delta\boldsymbol{x})) + \dots \\
&= d(\delta^{n+1}\boldsymbol{x}) + \boldsymbol{x}^{2^{n+1}-1} d\boldsymbol{x} + \dots,
\end{aligned}$$

and the omitted terms do not have a term with $d\boldsymbol{x}$ that is not a multiple of 2 or a term with $d(\delta^{n+1}\boldsymbol{x})$, for $\mathcal{F}$ does not introduce denominators, and thus takes multiples of 2 to multiples of 2, and $\mathcal{F}(d(\delta^i\boldsymbol{x}))$ gives just terms with $d(\delta^i\boldsymbol{x})$ and $d(\delta^{i+1}\boldsymbol{x})$. $\square$

Lemma 3.12. *The reduction modulo* 2 *of* $d(\delta^n\boldsymbol{x})$ *can be written as*

$$dx_n + \sum_{i=1}^{n-1} \frac{\partial P_n}{\partial x_i}\, dx_i.$$

where $P_n \in \mathbb{F}_2[x_0, \dots, x_{n-1}]$*.*

Proof. We recall that the reduction modulo 2 of $\delta^n\boldsymbol{x}$ is $x_n + P_n(x_0, \dots, x_{n-1})$, for some polynomial P_n, that the proof of lemma 2.6 in [1] shows us how to compute. Therefore, the reduction modulo 2 of $d(\delta^n\boldsymbol{x})$ can be written as

$$dx_n + \frac{\partial P_n}{\partial x_0}\, dx_0 + \sum_{i=1}^{n-1} \frac{\partial P_n}{\partial x_i}\, dx_i.$$

So, it suffices to prove that $\partial P_n/\partial x_0 = 0$ for all $n \geq 1$, that is the same as saying that P_n just have even powers of x_0, what we prove by induction on n. For $n = 1$ it is trivial, since $P_1 = 0$. Then, assume it is true for all $i \leq n$. We recall how to compute P_n: let

$$a \stackrel{\text{def}}{=} \sum_{k\geq 0} x_k\, 2^k,$$

considering a in characteristic zero and x_k's as independent variables. Let $\delta^0 a \stackrel{\text{def}}{=} a$ and $\phi(x_i) \stackrel{\text{def}}{=} x_i^2$ and extend ϕ linearly to power series and polynomials. Define

$$\delta^{i+1}(a) \stackrel{\text{def}}{=} \frac{1}{2}\left(\phi(\delta^i a) - (\delta^i a)^2\right).$$

If we write

$$\delta^n a = \sum_{k\geq 0} \Theta_k\, 2^k,$$

where $\Theta_k \in \mathbb{Z}[x_0, x_1, \ldots]$ with coefficients 0 or 1, then

$$P_n(x_0, x_1^2, \ldots, x_{n-1}^{2^{n-1}}) = \Theta_0(x_0, x_1, \ldots, x_n) - x_n^{2^n}. \tag{3.7}$$

(Here we are identifying P_n with the corresponding polynomial with integers coefficients.) Now,

$$\begin{aligned}\delta^{n+1} a = {} & \frac{1}{2}\left[(\phi(\Theta_0) + 2\phi(\Theta_1) + \ldots)\right. \\ & \left. - \left(\Theta_0^2 + 4\Theta_0(\Theta_1 + 2\Theta_2 + \ldots) + 4(\Theta_1 + 2\Theta_2 + \ldots)^2\right)\right] \\ = {} & \frac{\phi(\Theta_0) - \Theta_0^2}{2} + \phi(\Theta_1) + 2(\ldots).\end{aligned}$$

By induction hypothesis and equation 3.7, we have that Θ_0 just has even powers of x_0, and therefore, so does $[\phi(\Theta_0) - \Theta_0^2]/2$. Clearly $\phi(\Theta_1)$ just has even powers of x_0, which finishes the proof, since

$$P_{n+1}(x_0, x_1^2, \ldots, x_n^{2^n}) \equiv \frac{\phi(\Theta_0) - \Theta_0^2}{2} + \phi(\Theta_1) - x_{n+1}^{2^{n+1}} \pmod 2.$$

$\square$

Lemma 3.13. *Let*

$$\omega_n \stackrel{\text{def}}{=} \textit{reduction modulo } 2 \textit{ of } \mathcal{F}^n \left(\frac{d\boldsymbol{x}}{2\boldsymbol{y} + \boldsymbol{x}} \right).$$

Then, $\omega_n = dx_0/x_0$.

Proof. Let C be the Cartier operator. Then, since $\mathcal{F}$ is the "inverse" of C (see [3]), we have that $C^n(\omega_n) = dx_0/x_0$. On the other hand, since ω_n is holomorphic, $\omega_n = \alpha\, dx_0/x_0$, and so $C^n(\omega_n) = \alpha^{1/2^n} dx_0/x_0$. Thus $\alpha = 1$, and $\omega_n = dx_0/x_0$. $\square$

With these lemmas, we prove the theorem:

Proof of Theorem 3.10. The theorem is equivalent to say that $dx_n = 0$ for $n \geq 1$. We prove it by induction on n. With the same notation as in the the previous lemma, for $n = 1$ we have:

$$\omega_1 = \frac{x_0\, dx_0 + dx_1}{x_0^2} = \frac{dx_0}{x_0}$$

where the last equality comes from lemma 3.13. This equation gives us $dx_1 = 0$.

Now, assume $dx_i = 0$ for $i = 1, \ldots, n-1$. We prove that $dx_n = 0$: we have that ω_n is given by

$$\omega_n = \frac{dx_n + x_0^{2^n-1} dx_0 + \ldots}{x_0^{2^n}},$$

where all omitted term can be written only with $dx_1, \ldots, dx_{n-1}$, by lemmas 3.11 and 3.12. By induction hypothesis and lemma 3.13, we have

$$\frac{x_0^{2^n-1}\, dx_0 + dx_n}{x_0^{2^n}} = \frac{dx_0}{x_0},$$

which proves that $dx_n = 0$. $\square$

We can now compute the canonical lift modulo 2^3: the algorithm described in section 2.6 does not work, but we can still compute it. We know that $dx_2/dx_0 = 0$, and so x_2 just has even powers of x_0, and from chapter 2, we know that $\deg x_2 = 12$, with leading coefficient 1, and that $\deg y_2 < 16$. The third coordinate of the equation is not too complicated, and we simply write

$$x_2 = x_0^6 + \sum_{i=0}^{2} A_{2i}\, x_0^{2i}$$

and

$$y_2 = \sum_{i=0}^{7} B_i\, x_0^i + y_0 \sum_{i=0}^{6} C_i\, x_0^i,$$

leaving the A_{2i}'s, B_i's, C_i's and a_2 as unknowns in the third coordinate of the equation of the curve, and force the equality by solving the linear system given by this equation.

Solving that we find an *unique* solution:

$$\begin{aligned} a_2 &= a_0^4 \\ x_2 &= a_0\, x_0^2 + x_0^6 \\ y_2 &= (a_0^2 + a_0^4) + (a_0 + a_0^3)\, x_0^2 + a_0^4\, x_0^4 + (1 + a_0^2)\, x_0^5 + (1 + a_0 + a_0^2)\, x_0^6 \\ &\quad + [(1 + a_0^2)\, x_0^3 + a_0\, x_0^4 + x_0^6]\, y_0. \end{aligned}$$

The uniqueness implies that this has to give us the canonical lift and the Teichmüller map, as one can also check by analyzing $\boldsymbol{x}/\boldsymbol{y}$.

To check solutions with smaller degrees, we can try to write

$$x_2 = \sum_{i=0}^{6} A_i\, x_0^i + y_0 \sum_{i=0}^{4} A_i'\, x_0^i,$$

and y_2 as before and try to solve it in the same way, but we will still find exactly one single solution to the corresponding system, again having the canonical lift and the Teichmüller map as the result.

But, in this case, we do have a lift

$$\nu = ((x_0, x_1, \tilde{x}_2), (y_0, y_1, \tilde{y}_2))$$

with $\deg \tilde{x}_2 < \deg x_2$, but in this case, in contrast to what happens to characteristic different from 2, we have $\deg \tilde{y}_2 > \deg y_2$. Such a lift is:

$$\begin{aligned}
a_2 &= a_0^4 \\
\tilde{x}_2 &= a_0\, x_0^2 \\
\tilde{y}_2 &= (a_0^2 + a_0^4) + (a_0 + a_0^2 + a_0^3)\, x_0^2 + (a_0 + a_0^4)\, x_0^4 \\
&\quad + (1 + a_0^2)\, x_0^5 + (1 + a_0 + a_0^2)\, x_0^6 + x_0^7 + x_0^8 + x_0^{10} \\
&\quad + [(1 + a_0^2)\, x_0^3 + a_0\, x_0^4 + x_0^5 + x_0^6]\, y_0
\end{aligned}$$

If we compute another coordinate, we have $\deg x_3 < 28$ and $\deg y_3 < 36$, by our analysis of leading coefficients. Proceeding as described above, we can try to find the canonical lift and possibly some lift with smaller degrees, we can set

$$x_3 = \sum_{i=0}^{13} A_i\, x_0^i + y_0 \sum_{i=0}^{11} B_i\, x_0^i$$

and

$$y_3 = \sum_{i=0}^{17} C_i\, x_0^i + y_0 \sum_{i=0}^{16} D_i\, x_0^i,$$

and solve the corresponding system. We get, as solutions $a_3 = a_0^8$,

$$x_3 = a_0^8 + a_0\, x_0^6 + A_8\, x_0^8 + A_9\, x_0^9 + x_0^{10} + x_0^{12} + y_0\, (D_{16}\, x_0^8),$$

and

$$\begin{aligned} y_3 = a_0^4 + a_0^5 + a_0^4\,A_8 + a_0^4\,A_9\,x_0 + a_0^5\,x_0^2 + (a_0^2 + a_0^6 + a_0^8 + a_0^{10} + a_0^2\,A_8)\,x_0^4 \\ + (a_0^4 + a_0^2\,A_9)\,x_0^5 + (a_0 + a_0^5 + a_0^7 + a_0^9 + a_0\,A_8)\,x_0^6 \\ + (a_0^2 + a_0^3 + a_0^4 + a_0\,A_9 + a_0\,D_{16})\,x_0^7 + (a_0 + a_0^2 + a_0^3 + a_0^4 + a_0^6)\,x_0^8 \\ + (1 + a_0^6 + a_0^8 + A_8)\,x_0^9 + (1 + a_0^6 + a_0^8 + A_8 + A_9 + D_{16})\,x_0^{10} \\ + (1 + a_0^2 + a_0^3 + A_9)\,x_0^{11} + (1 + a_0 + a_0^3 + a_0^8 + A_8)\,x_0^{12} \\ + (1 + a_0^2 + a_0^4 + A_9)\,x_0^{13} + (1 + a_0 + a_0^2 + a_0^4)\,x_0^{14} \\ + (1 + a_0 + a_0^2 + a_0^4 + A_8)\,x_0^{16} + A_9\,x_0^{17} + y_0\,[a_0^4\,D_{16} + a_0^4\,x_0^3 \\ + (a_0^5 + a_0^2\,D_{16})\,x_0^4 + a_0^2\,x_0^5 + (a_0^2 + a_0^3 + a_0\,D_{16})\,x_0^6 \\ + (1 + a_0 + a_0^2 + a_0^3 + a_0^6 + a_0^8 + A_8)\,x_0^7 + (a_0 + a_0^3 + a_0^5 + A_9 + D_{16})\,x_0^8 \\ + (1 + a_0 + D_{16})\,x_0^9 + (1 + a_0^3 + a_0^4 + D_{16})\,x_0^{10} + (a_0 + a_0^4)\,x_0^{11} \\ + (a_0 + a_0^2 + D_{16})\,x_0^{12} + x_0^{13} + x_0^{14} + D_{16}\,x_0^{16}]. \end{aligned}$$

Thus, clearly, to get the minimal and the Teichmüller lifts, we need to choose $D_{16} = 0$. This leaves us the choices of A_8 and A_9. Again, to get minimal degrees and the Teichmüller (since $dx_3/dx_0 = 0$), we choose $A_9 = 0$. So, we have

$$x_3 = a_0^8 + a_0\,x_0^6 + A_8\,x_0^8 + x_0^{10} + x_0^{12},$$

and

$$
\begin{aligned}
y_3 = {} & a_0^4 + a_0^5 + a_0^4 A_8 + a_0^5 x_0^2 + (a_0^2 + a_0^6 + a_0^8 + a_0^{10} + a_0^2 A_8) x_0^4 + a_0^4 x_0^5 \\
& + (a_0 + a_0^5 + a_0^7 + a_0^9 + a_0 A_8) x_0^6 + (a_0^2 + a_0^3 + a_0^4) x_0^7 \\
& + (a_0 + a_0^2 + a_0^3 + a_0^4 + a_0^6) x_0^8 + (1 + a_0^6 + a_0^8 + A_8) x_0^9 \\
& + (1 + a_0^6 + a_0^8 + A_8) x_0^{10} + (1 + a_0^2 + a_0^3) x_0^{11} \\
& + (1 + a_0 + a_0^3 + a_0^8 + A_8) x_0^{12} + (1 + a_0^2 + a_0^4) x_0^{13} \\
& + (1 + a_0 + a_0^2 + a_0^4) x_0^{14} + (1 + a_0 + a_0^2 + a_0^4 + A_8) x_0^{16} \\
& + y_0 [a_0^4 x_0^3 + a_0^5 x_0^4 + a_0^2 x_0^5 + (a_0^2 + a_0^3) x_0^6 \\
& + (1 + a_0 + a_0^2 + a_0^3 + a_0^6 + a_0^8 + A_8) x_0^7 + (a_0 + a_0^3 + a_0^5) x_0^8 + (1 + a_0) x_0^9 \\
& + (1 + a_0^3 + a_0^4) x_0^{10} + (a_0 + a_0^4) x_0^{11} + (a_0 + a_0^2) x_0^{12} + x_0^{13} + x_0^{14}].
\end{aligned}
$$

The choice of $A_8 = 1 + a_0 + a_0^2 + a_0^3 + a_0^6 + a_0^8$, clearly gives us the smaller degrees, but in fact, it does not gives us the canonical lift. One can check that by looking at $\boldsymbol{x}/\boldsymbol{y}$. The fourth coordinate of $\boldsymbol{x}/\boldsymbol{y}$ is given by,

$$
\begin{aligned}
& \frac{x_3}{y_0^8} + \frac{x_0^2 x_1^3 y_1}{y_0^{10}} + \frac{x_0^2 x_1 x_2 y_1}{y_0^{10}} + \frac{x_0^4 x_2 y_1^2}{y_0^{12}} + \frac{x_1^2 x_2 y_1^2}{y_0^{12}} + \frac{x_0^2 x_1^3 y_1^3}{y_0^{14}} \\
& \quad + \frac{x_0^8 y_1^4}{y_0^{16}} + \frac{x_0^4 x_1^2 y_1^4}{y_0^{16}} + \frac{x_1^4 y_1^4}{y_0^{16}} + \frac{x_0^4 x_2 y_1^4}{y_0^{16}} + \frac{x_2^2 y_1^4}{y_0^{16}} + \frac{x_0^6 x_1 y_1^5}{y_0^{18}} + \frac{x_0^8 y_1^6}{y_0^{20}} \\
& \quad + \frac{x_0^4 x_1^2 y_1^6}{y_0^{20}} + \frac{x_1^4 y_1^8}{y_0^{24}} + \frac{x_0^8 y_1^{12}}{y_0^{32}} + \frac{x_0^4 x_2 y_2}{y_0^{12}} + \frac{x_0^6 x_1 y_1 y_2}{y_0^{14}} + \frac{x_0^8 y_1^2 y_2}{y_0^{16}} \\
& \qquad + \frac{x_0^4 x_1^2 y_1^2 y_2}{y_0^{16}} + \frac{x_0^8 y_1^4 y_2}{y_0^{20}} + \frac{x_0^8 y_2^2}{y_0^{16}} + \frac{x_1^4 y_2^2}{y_0^{16}} + \frac{x_0^8 y_3}{y_0^{16}}
\end{aligned}
$$

The part that has non-positive order at infinity and the part in x_3 and y_3 is

$$
\frac{x_3}{y_0^8} + \frac{x_0^4 x_2 y_1^4}{y_0^{16}} + \frac{x_2^2 y_1^4}{y_0^{16}} + \frac{x_0^8 y_1^{12}}{y_0^{32}} + \frac{x_0^8 y_3}{y_0^{16}}.
$$

Using the expressions of x_1, y_1, x_2, y_2, we get that

$$\frac{x_0^4\,x_2\,y_1^4}{y_0^{16}} + \frac{x_2^2\,y_1^4}{y_0^{16}} + \frac{x_0^8\,y_1^{12}}{y_0^{32}}$$

has actually positive order at infinity, and since x_3/y_0^8 has order 0 (for any choice of A_8), we have that the Teichmüller lift had $\deg y_3 = 32$, and $A_8 = a_0 + a_0^2 + a_0^4$. In this case, we have a lift

$$\nu = ((x_0, x_1, x_2, \tilde{x}_3), (y_0, y_1, y_2, \tilde{y}_3)),$$

with $\deg \tilde{x}_3 = \deg x_3$ and $\deg \tilde{y}_3 < \deg y_3$.

On the other hand if we use $\tilde{x}_2$ and $\tilde{y}_2$ as before, we can get a lift

$$\tilde{\nu} = ((x_0, x_1, \tilde{x}_2, \tilde{\tilde{x}}_3), (y_0, y_1, \tilde{y}_2, \tilde{\tilde{y}}_3))$$

with

$$\tilde{\tilde{x}}_3 = a_0^8 + a_0^6\,x_0^6$$

and

$$\begin{aligned}
\tilde{\tilde{y}}_3 = {} & a_0^4 + a_0^6 + (a_0^3 + a_0^6 + a_0^7)\,x_0^2 + (a_0^3 + a_0^4 + a_0^5 + a_0^8 + a_0^{10})\,x_0^4 \\
& + (a_0^2 + a_0^6)\,x_0^5 + (a_0 + a_0^2 + a_0^3 + a_0^4 + a_0^5 + a_0^6 + a_0^7 + a_0^9)\,x_0^6 \\
& + (a_0^2 + a_0^3)\,x_0^7 + (a_0^2 + a_0^6)\,x_0^8 + (1 + a_0 + a_0^6 + a_0^8)\,x_0^9 \\
& + (a_0 + a_0^2 + a_0^3 + a_0^5 + a_0^6 + a_0^8)\,x_0^{10} + (a_0 + a_0^2 + a_0^3)\,x_0^{11} \\
& + (1 + a_0 + a_0^3 + a_0^8)\,x_0^{12} + (1 + a_0)\,x_0^{13} + (a_0^2 + a_0^4)\,x_0^{16} \\
& + (1 + a_0)\,x_0^{18} + x_0^{19} + x_0^{21} + x_0^{22} + x_0^{24} \\
& + y_0\,[(a_0^2 + a_0^6)\,x_0^3 + a_0^5\,x_0^4 + (a_0^2 + a_0^4)\,x_0^5 + a_0^2\,x_0^6 \\
& + (1 + a_0^3 + a_0^6 + a_0^8)\,x_0^7 + (a_0 + a_0^3 + a_0^5)\,x_0^8 + a_0\,x_0^9 \\
& + (1 + a_0^3 + a_0^4)\,x_0^{10} + (a_0 + a_0^2)\,x_0^{11} + (1 + a_0^2)\,x_0^{12} + a_0\,x_0^{14} + x_0^{16} + x_0^{17} + x_0^{19}]
\end{aligned}$$

And so, $\deg \tilde{\tilde{x}}_3 = 12$ and $\deg \tilde{\tilde{y}}_3 = 48$.

3.5 Characteristic 3

In characteristic 3, an ordinary elliptic curve over an algebraic closed field (or over a finite extension of our original base field k) can be put in the form:

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

(and then, we have the Hasse invariant $A = 1$) and we consider the canonical lifting having the same form:

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

We notice that the formulas for the derivatives of x_1 and x_2 remain the same as for characteristic $p \geq 5$ we used before. An analogous analysis to the one done to prove theorem 2.13 tells us, though, that $\deg x_2 = 3p^2 - 1$, and in fact, we can use the modified algorithm described to produce a lifting modulo 3^3. What we obtain is:

$$a_1 = 0, \quad a_2 = a_0^9 + a_0^{12},$$

and

$$x_1 = 2\,a_0^2 + a_0\,x_0 + (1 + 2\,a_0)\,x_0^3 + x_0^4$$

$$y_1 = x_0^2\,y_0$$

$$\begin{aligned} x_2 = {} & 2\,a_0^5 + 2\,a_0^9 + \left(a_0^4 + 2\,a_0^5\right) x_0 + a_0^4\,x_0^2 + \left(a_0^3 + a_0^4 + a_0^5 + 2\,a_0^6\right) x_0^3 + 2\,a_0^2\,x_0^5 \\ & + \left(2\,a_0^2 + a_0^3 + a_0^4\right) x_0^6 + a_0^2\,x_0^7 + a_0\,x_0^8 + \left(2\,a_0 + a_0^2 + a_0^3\right) x_0^9 + 2\,a_0^2\,x_0^{10} \\ & + (2 + a_0)\,x_0^{11} + \left(2\,a_0 + 2\,a_0^3\right) x_0^{12} + x_0^{13} \end{aligned}$$

$$\begin{aligned} y_2 = {} & y_0 \left[2\,a_0^4 + a_0^7 + a_0^6\,x_0^2 + \left(2\,a_0^4 + a_0^6\right) x_0^3 + 2\,a_0^2\,x_0^4 + \left(a_0^2 + 2\,a_0^3\right) x_0^5 \right. \\ & + \left(2\,a_0^2 + 2\,a_0^3 + a_0^4\right) x_0^6 + a_0\,x_0^7 + \left(a_0 + a_0^3\right) x_0^8 + \left(2\,a_0 + a_0^3 + a_0^4\right) x_0^9 \\ & \left. + 2\,x_0^{10} + \left(2 + a_0^3\right) x_0^{11} + \left(1 + 2\,a_0 + a_0^3\right) x_0^{12} + 2\,x_0^{14} + 2\,x_0^{15}\right] \end{aligned}$$

So, for $p = 3$, the Teichmüller lift is also the absolute minimal degree lift.

If we look modulo 3^4, though, we have that $\deg x_3 = 108$, with leading coefficient 2. So, in this case, proposition 3.4 tells us that we have a lift with $\deg \tilde{x}_3 \leq 82$. We can try to look at such lift to see if similar properties happen to this minimal lift as it happened to minimal lifts modulo p^3 for $p \geq 5$, e.g. is $d\tilde{x}_3/dx_0 = dx_3/dx_0$? What is its degree?

To compute the Teichmüller in this case, it would be useful to know again the derivative. We wrote a program in Magma to help us, and some numerical evidence allows us to conjecture:

Conjecture 3.14. *For $p \neq 2$ and $n \geq 1$, we have that the reduction modulo p of $\mathcal{F}^n(d\boldsymbol{x}/\boldsymbol{y})$ is given by*

$$\frac{1}{y_0^{p^n}} \sum_{i=0}^{n} x_i^{(p^{n-i}-1)}\, dx_i,$$

which implies that

$$\frac{dx_n}{dx_0} = A^{-(p^n-1)/(p-1)}\, y_0^{p^n-1} - x_0^{p^n-1} - \sum_{i=1}^{n-1} x_i^{(p^{n-i}-1)}\, \frac{dx_i}{dx_0}.$$

Voloch was the first to "guess" the formula above, and we did some calculations to confirm it in some cases. We checked it to be true for: $p = 3$ and $n \leq 6$, $p = 5, 7, 11, 13$ and $n \leq 4$, $p = 17$ and $n \leq 3$.

The main difficulty of proving this conjecture is maybe dealing with Buium's polynomials P_i's (as in lemma 3.12 – or check lemma 2.6 in [1]). Even with Magma running on fast computers, the computations of such polynomials take *very* long for large p's or large i's, and there does not seem to be a straightforward way to deal with them theoretically to work out a proof.

We now proceed to compute x_3. Since we know its derivative (the conjecture was verified for $p = 3$ and $n = 3$), we follow the same idea of the algorithm described in section 2.6, leaving the coefficients of x_3 that cannot be obtained by the derivative as indeterminates. We can then compute the canonical lift and the elliptic Teichmüller map. The expressions are too long to be put in here, but as an example, taking $a_0 = 1$, we would have:

$$a_3 = 1$$

$$\begin{aligned} x_3 = & 2 + 2\,x_0^3 + x_0^4 + 2\,x_0^6 + x_0^7 + x_0^8 + 2\,x_0^9 + x_0^{10} + x_0^{11} + 2\,x_0^{12} + 2\,x_0^{16} \\ & + 2\,x_0^{17} + 2\,x_0^{18} + 2\,x_0^{20} + x_0^{25} + 2\,x_0^{27} + 2\,x_0^{28} + 2\,x_0^{29} + x_0^{30} + x_0^{32} \\ & + 2\,x_0^{34} + x_0^{35} + 2\,x_0^{36} + x_0^{37} + 2\,x_0^{38} + x_0^{40} + x_0^{45} + 2\,x_0^{54} \end{aligned}$$

$$\begin{aligned} y_3 = & y_0\,[2 + 2\,x_0^3 + 2\,x_0^4 + 2\,x_0^6 + x_0^7 + x_0^9 + 2\,x_0^{10} + x_0^{12} + x_0^{13} + 2\,x_0^{15} \\ & + 2\,x_0^{17} + 2\,x_0^{18} + 2\,x_0^{19} + x_0^{20} + x_0^{21} + x_0^{22} + 2\,x_0^{23} + x_0^{27} + 2\,x_0^{28} \\ & + 2\,x_0^{29} + x_0^{30} + 2\,x_0^{31} + 2\,x_0^{34} + 2\,x_0^{35} + x_0^{36} + 2\,x_0^{37} + 2\,x_0^{38} + 2\,x_0^{39} \\ & + x_0^{43} + 2\,x_0^{44} + 2\,x_0^{48} + 2\,x_0^{50} + x_0^{53} + x_0^{54} + 2\,x_0^{60} + 2\,x_0^{62} + x_0^{63} \\ & + 2\,x_0^{65} + 2\,x_0^{66}] \end{aligned}$$

In the generic case, we get always the same curve, having

$$a_3 = 2\,a_0^{27} + 2\,a_0^{33} + a_0^{36} + 2\,a_0^{45}.$$

The general formula can be found in the web address cited in chapter 2. To find the minimal degree lift to the canonical lift, we proceed in an analogous way as in theorem 3.6, we make the division of polynomials

$$x_3 = f(x_0)^{14}\,q(x_0) + \tilde{x}_3, \quad (f(x_0) = x_0^3 + x_0^2 + a_0)$$

and define

$$\tilde{y}_3 = y_3 - \frac{y_0}{2}[f'(x_0)^{27} q(x_0)].$$

Again, (in the general case) we get that $\deg \tilde{x}_3 = 80$, not 82 as it could be. For $a_0 = 1$ again, we would have:

$$\begin{aligned}\tilde{x}_3 =& 1 + 2\,x_0^3 + x_0^4 + 2\,x_0^6 + x_0^7 + x_0^8 + 2\,x_0^9 + x_0^{10} + x_0^{11} + 2\,x_0^{12} + 2\,x_0^{16} + 2\,x_0^{17}\\ &+ x_0^{18} + 2\,x_0^{20} + x_0^{25} + x_0^{27} + 2\,x_0^{28} + 2\,x_0^{29} + x_0^{30} + x_0^{32} + 2\,x_0^{34} + x_0^{35} + x_0^{37}\\ &+ 2\,x_0^{38} + x_0^{40}\end{aligned}$$

$$\begin{aligned}\tilde{y}_3 =& y_0\,[2 + 2\,x_0^3 + 2\,x_0^4 + 2\,x_0^6 + x_0^7 + x_0^9 + 2\,x_0^{10} + x_0^{12} + x_0^{13} + 2\,x_0^{15} + 2\,x_0^{17}\\ &+ 2\,x_0^{18} + 2\,x_0^{19} + x_0^{20} + x_0^{21} + x_0^{22} + 2\,x_0^{23} + 2\,x_0^{27} + 2\,x_0^{28} + 2\,x_0^{30} + 2\,x_0^{31}\\ &+ x_0^{33} + 2\,x_0^{34} + 2\,x_0^{37} + x_0^{43} + 2\,x_0^{44} + 2\,x_0^{48} + 2\,x_0^{50} + x_0^{53} + x_0^{54} + 2\,x_0^{60}\\ &+ 2\,x_0^{62} + x_0^{63} + 2\,x_0^{65} + 2\,x_0^{66}]\end{aligned}$$

(Again, one can see the general formula at the web address.)

We also observe that x_3 and $\tilde{x}_3$ have the same derivative (even in the generic case), and many of the properties observed in section 3.3 for $\tilde{x}_2$ will hold here for $\tilde{x}_3$ in a very similar way: the Frobenius will also lift and $\tilde{x}_3$ will give us the absolute minimal lift, and thus the minimal degree occurs for the canonical lift, and lifting to every other curve will give a map $\tilde{\tilde{x}}_3$ with degree larger or equal to 82. For the first claim, just observe that $x_3 - \tilde{x}_3$ and $y_3 - \tilde{y}_3$ are 3-powers. The second claim follows from analyzing the part of $\boldsymbol{x}/\boldsymbol{y}$ that can be singular, namely

$$\frac{x_3}{y_0^{27}} + \frac{2\,x_1^9\,y_2^3}{y_0^{54}} + \frac{2\,x_0^{27}\,y_3}{y_0^{54}}.$$

Rewriting

$$y_3 = \frac{1}{y_0^{27}}\,\left[y_1^9\,y_2^3 + 2x_0^{27}x_3 + \ldots\right],$$

we get an expression for the terms of higher power in x_0 of x_3 that makes it the one from Teichmüller, and if $\deg \tilde{\tilde{x}}_3 \leq 80$, we can add this terms and modify $\tilde{\tilde{y}}_3$ to get the Teichmüller (again, as in section 3.3), which forces the curve to be the canonical lift and the degree to be 80.

Chapter 4

Hyperelliptic Curves

4.1 Minimal Degrees

Again, let k be a perfect field of characteristic $p \neq 2$, and consider the (non-singular) hyperelliptic curve given by

$$C/k : y_0^2 = f(x_0),$$

with $\deg_{x_0} f = d \geq 3$. Let ϵ be the number of points at infinity of C, and let U denote the affine part of C.

Theorem 4.1. *Suppose that we have a curve*

$$\boldsymbol{C}/W_{n+1}(k) : \quad \boldsymbol{y}^2 = \boldsymbol{f}(\boldsymbol{x})$$

with reduction C modulo p such that there is a lift of the Frobenius to the affine part *of $\boldsymbol{C}$. Assume that the first part of conjecture 3.14 holds at least for n and p, and that the lift of U to the affine part of $\boldsymbol{C}$ associated to the Frobenius is given by*

$$\nu = ((x_0, x_1, \ldots, x_n), (y_0, y_1, \ldots, y_n)),$$

where x_i's are polynomials in x_0 and with $\deg x_i = d(p^i - 1) + 2$ *and* $\deg y_i \leq [i(d-2)+d]p^i - i(d-2)p^{i-1}$, *for* $i = 0, \ldots, (n-1)$. *Then,* $\deg x_n \geq d(p^n - 1) + 2$.

If we have the equality for $\deg x_n$*, we must have*

$$\frac{dx_n}{dx_0} = \lambda f(x_0)^{(p^n-1)/2} - \sum_{i=0}^{n-1} x_i^{p^{n-i}-1} \frac{dx_i}{dx_0},$$

for some $\lambda \in k$*.*

Proof. First, we observe that the first part of conjecture 3.14 depends only on the existence of the lift of the Frobenius and on Buium's polynomials P_i, for $i \leq n$.

Let ϕ denote the Frobenius map and its lift to $\boldsymbol{C}$, and let $\boldsymbol{U}$ denote the affine part of $\boldsymbol{C}$. Then, the conjecture states that the reduction modulo p of $\mathcal{F}^n(d\boldsymbol{x}/\boldsymbol{y})$ is given by

$$\omega \stackrel{\text{def}}{=} \frac{1}{y_0^{p^n}} \left[\sum_{i=0}^{n} x_i^{(p^{n-i}-1)} \frac{dx_i}{dx_0} \right] dx_0.$$

Let P be a point at infinity of C. We have

$$\operatorname{ord}_P(\omega) = p^n \frac{d}{\epsilon} - \left(\frac{2}{\epsilon} + 1 \right) + \operatorname{ord}_P \left(\sum_{i=0}^{n} x_i^{(p^{n-i}-1)} \frac{dx_i}{dx_0} \right).$$

To simplify the notation, we will denote the last summand above α. Also, let β denote the number of zeros, counted with multiplicity, of ω in U. Since $d\boldsymbol{x}/\boldsymbol{y}$ is regular on $\boldsymbol{U}$, ω must be regular on U. Then, by the Riemman-Roch theorem, we have

$$\epsilon\alpha + dp^n - (2+\epsilon) + \beta = 2\,\frac{d-\epsilon}{2} - 2 = d - (\epsilon + 2).$$

Hence,

$$\alpha \leq -\frac{d(p^n-1)}{\epsilon}.$$

By hypothesis, we have

$$\begin{aligned}\operatorname{ord}_P\left(x_i^{p^{n-i}-1}\frac{dx_i}{dx_0}\right) &= -\left[(p^{n-i}-1)\frac{d(p^i-1)+2}{\epsilon}+\frac{d(p^i-1)+2}{\epsilon}-\frac{2}{\epsilon}\right]\\ &= -\left[\frac{dp^n-(d-2)p^{n-i}+2}{\epsilon}\right] > -\frac{d(p^n-1)}{\epsilon},\end{aligned}$$

for $i = 1, \dots, (n-1)$. Therefore

$$\operatorname{ord}_P\left(\frac{dx_n}{dx_0}\right) \leq -\frac{d(p^n-1)}{\epsilon},$$

what implies that $\deg x_n \geq d(p^n-1)+2$.

We have the equality if, and only if, $\beta = 0$. But then, $\operatorname{ord}_P(\omega) = d/\epsilon - (2/\epsilon + 1) = \operatorname{ord}_P(dx_0/y_0)$. So, if we write $\omega = g\, dx_0/y_0$, for some g in the function field of C, g has no zeros or poles at infinity. Since ω and dx_0/y_0 have no poles in U, g has no poles at all, and thus $\lambda \stackrel{\text{def}}{=} g \in k$. Thus, we have

$$\omega = \frac{1}{y_0^{p^n}}\left[\sum_{i=0}^{n} x_i^{(p^{n-i}-1)}\frac{dx_i}{dx_0}\right] dx_0 = \lambda\,\frac{dx_0}{y_0},$$

what implies the formula for the derivative.

□

The proof of the above theorem, for $p = 3$, $d = 6$ and $n = 1$, that could be easily generalized, was shown to the author by Felipe Voloch.

We observe that curves of genus $g > 1$ do not have a lift of the Frobenius (see [5]), so the restriction to affine parts is necessary if $g > 1$. On the other hand, Mochizuki showed in [4] that there is a lifting of the Frobenius in some open subset of an ordinary curve of genus g defined by taking off some $(g-1)(p-1)$ points from the curve. This was what motivated Voloch to prove the above theorem for $p = 3$, $d = 6$ and $n = 1$: in this case, the curve has genus 2 and is necessarily hyperelliptic, and we have two points to be taken off, that maybe can be put at infinity.

We also note that, although the hypothesis of the theorem seem very strong, it is still gives us some nice results. Besides the case of Mochizuki lift just mentioned, we have:

Corollary 4.2. *Let ν be a lift from the affine part of C to the affine part of $\boldsymbol{C}/W_2(k)$. Then,* $\deg x_1 \geq d(p-1)+2$*, and if we have the equality, we must have that the coefficient of x_0^{p-1} in $f(x_0)^{(p-1)/2}$, say A, is non zero and*

$$\frac{dx_1}{dx_0} = A^{-1} f(x_0)^{(p-1)/2} - x_0^{p-1}.$$

Proof. Remember that having a lift modulo p^2 of U gives a lift of the Frobenius modulo p^2, and we can assume that x_1 is a polynomial in x_0 and y_1 is y_0 times a polynomial in x_0. Also, the conjecture 3.14 is true for $n = 1$. Finally $\deg x_0 = 2$ and $\deg y_0 = d$. So, we can apply the theorem 4.1 with $n = 1$. The fact that $\lambda = A^{-1}$, comes from the fact that a derivative of a polynomial in characteristic p cannot have a term in x_0^{p-1}.

□

The above corollary gives a better lower bound for the degree of x_1 than the one stated in [8], theorem IV.2, for the case of hyperelliptic curves, and it is a little more general, since that theorem just applies for d odd. Also, it gives us a necessary condition to achieve the lower bound: in order for $A^{-1}f(x_0)^{(p-1)/2} - x_0^{p-1}$ to be a derivative, $f(x_0)^{(p-1)/2}$ cannot have a coefficient of x_0^{rp-1} different from zero, except for $r = 1$, in which case such term is necessarily non zero.

The condition also seems to be sufficient: we tried several cases when the condition was satisfied and we were always able to find a lift with the minimal degree.

Also, another interesting corollary of theorem 4.1 is that for elliptic curves, if we proceed finding minimal lifts modulo higher powers of p that give lifts of the Frobenius, then the derivatives of the $\tilde{x}_n$, by induction, would have to be the same as the derivative of x_n, and thus $\deg \tilde{x}_n = 3p^n - 1$.

4.2 Mochizuki Lifts

We will now analyze in more detail the case of Mochizuki lifts. As mentioned before, for $p = 3$ and $g = 2$, we would have to take off two points of the curve to have a lift of the Frobenius. Every curve of genus 2 is hyperelliptic, and if those points to be taken off are invariant by the hyperelliptic involution, we can assume that those points are at infinity. So we will consider the curve

$$C/k : y_0^2 = f(x_0),$$

where k is a perfect field of characteristic 3 and $\deg_{x_0} f = 6$. In order to have the minimal degree, we will assume there exists an $A \in k^*$ such that $A^{-1}f(x_0) - x_0^2$ is a derivative, i.e., it does not have the terms in x_0^2 and x_0^5. Therefore, A is the coefficient of x_0^2 in $f(x_0)$, and working in some finite extension of k, we may assume $A = 1$. Also, the coefficient of x_0^5 has to be zero. So, we can assume that

$$f(x_0) = x_0^6 + \alpha_0 x_0^4 + \beta_0 x_0^3 + x_0^2 + \gamma_0 x_0 + \delta_0.$$

But, with the linear change of variables

$$(x_0, y_0) \mapsto (x_0 + \epsilon_0, y_0),$$

with ϵ_0 satisfying $2\epsilon_0^3 + \alpha_0\,\epsilon_0 + \beta_0 = 0$ (again, maybe in some finite extension of k), allows us to consider f given by

$$f(x_0) = x_0^6 + a_0 x_0^4 + x_0^2 + b_0 x_0 + c_0.$$

In this context, such a curve is "ordinary" if $a_0 \neq 0$.

Assuming that the lift will have minimal degrees and using the formula for the derivative of x_1 from corollary 4.2, we can use the same algorithm described for elliptic curves in section 2.6 to compute the Mochizuki lift. We have a lift of the form

$$\boldsymbol{C}/W_2(k) \,:\, \boldsymbol{y}^2 = \boldsymbol{x}^6 + \boldsymbol{a}\boldsymbol{x}^4 + \boldsymbol{x}^2 + \boldsymbol{b}\boldsymbol{x} + \boldsymbol{c},$$

with

$$\begin{aligned} x_1 = {} & x_0^7 + \frac{b_0}{a_0^2}\,x_0^6 + 2\,a_0\,x_0^5 + \\ & \frac{a_0^4\,c_0^2 + 2\,a_0^4 + 2\,a_0^3\,b_0^2 + 2\,a_0^3\,c_0 + 2\,a_0^2\,b_0^2\,c_0 + 2\,a_0^2\,c_0^2 + a_0^2 + b_0^4}{a_0^2}\,x_0^3 \\ & + 2\,b_0\,x_0^2 + c_0\,x_0 + \frac{a_0^4\,b_0 + 2\,a_0^3\,b_0\,c_0 + a_0^2\,b_0 + b_0}{a_0^5} \end{aligned}$$

$$F_1 = (2\,a_0^3 + a_0)\,x_0^4 + 2\,a_0\,b_0\,x_0^3 + (2\,a_0^2 + 1)\,x_0^2 + (2\,a_0^2\,b_0 + b_0)\,x_0 + 2\,a_0^2\,c_0 + b_0^2$$

$$a_1 = 2\,a_0^5\,c_0^2 + 2\,a_0^5 + a_0^4\,b_0^2 + a_0^4\,c_0 + a_0^3\,b_0^2\,c_0 + a_0^3\,c_0^2 + 2\,a_0^3 + a_0^2\,c_0 + 2\,a_0\,b_0^4 + a_0 + 2\,b_0^2 + c_0$$

$$\begin{aligned} b_1 = {} & \big[2\,a_0^7\,b_0^3\,c_0^2 + 2\,a_0^7\,b_0^3 + a_0^6\,b_0^5 + a_0^6\,b_0^3\,c_0 + a_0^6\,b_0\,c_0^2 + a_0^5\,b_0^5\,c_0 + a_0^5\,b_0^3\,c_0^2 \\ & + 2\,a_0^5\,b_0^3 + a_0^5\,b_0\,c_0 + a_0^4\,b_0 + 2\,a_0^3\,b_0^7 + 2\,a_0^3\,b_0\,c_0 + a_0^2\,b_0 + b_0\big]\,a_0^{-5} \end{aligned}$$

$$c_1 = \frac{a_0^7\,c_0^3 + 2\,a_0^5\,b_0^2\,c_0^2 + 2\,a_0^4\,b_0^4 + a_0^3\,b_0^4\,c_0 + 2\,a_0^2\,b_0^4 + 2\,b_0^4}{a_0^5}$$

(Remember that $y_n = y_0\,F_n$, with F_n a polynomial in x_0.)

I also checked the case $a_0 = 0$ (when C is *not* ordinary), where we have:

$$x_1 = x_0^7 + 2\,b_0\,x_0^6 + (2\,b_0^4 + 2\,b_0^2\,c_0 + 2\,c_0^2 + 1)\,x_0^3 + 2\,b_0\,x_0^2 + c_0\,x_0$$

$$F_1 = x_0^2 + b_0\,x_0 + b_0^2$$

$$a_1 = 2\,b_0^2 + c_0$$

$$b_1 = b_0^7 + b_0^5\,c_0 + b_0^3\,c_0^2 + 2\,b_0^3 + b_0\,c_0$$

$$c_1 = 2\,b_0^2\,c_0^2$$

If the curve with $a_0 \neq 0$ indeed corresponds to the Mochizuki lift, we should be able to also lift the Frobenius modulo 3^3. To compute the lift, say

$$\nu = ((x_0, x_1, x_2), (y_0, y_1, y_2)),$$

that will give the lift of the Frobenius, we use proposition 3.9. We then have that

$$\frac{dx_2}{dx_0} = y_0^8 - x_0^8 - x_1^2\,(y_0^2 - x_0^2).$$

Therefore, we have that $\deg_{x_0} x_2 \geq 25$. We have done the calculations and found that the minimal lift having such derivative has in fact $\deg_{x_0} x_2 = 25$ if $a_0 \neq 0$. Checking the minimal lifts for $a_0 = 0$, we found that if $b_0 \neq 0$, then again $\deg_{x_0} x_2 = 25$. If $a_0 = b_0 = 0$, then $\deg_{x_0} x_2 = 30$. But, we still need to guarantee the existence of the lift of the Frobenius. To check that, we construct polynomials $\boldsymbol{P}$ and $\boldsymbol{Q}$ in $W_3[\boldsymbol{x}]$ and $W_3[\boldsymbol{x}, \boldsymbol{y}]$ respectively, such that

$$\phi(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}^p + p\boldsymbol{x}_1 + p^2\boldsymbol{P}, \boldsymbol{y}^p + p\boldsymbol{y}_1 + p^2\boldsymbol{Q}).$$

is a lift of the Frobenius. We do that by following the idea behind the proof of proposition 3.8, more precisely formula (3.5) and its analogue for $\delta^2\boldsymbol{y}$. We need then, that $x_2 - x_0^{p(p-1)}x_1$ minus the reduction modulo p of $(\boldsymbol{x}_1^\sigma(\boldsymbol{x}^p) - \boldsymbol{x}_1(\boldsymbol{x})^p)/p + (d\boldsymbol{x}_1/d\boldsymbol{x})^\sigma(\boldsymbol{x}^p)\cdot\boldsymbol{x}_1$ is a p-power, which we get by our choice of the derivative of x_2, and also $y_2 - y_0^{p(p-1)}y_1$ minus the reduction modulo p of $(\boldsymbol{y}_1^\sigma(\boldsymbol{x}^p,\boldsymbol{y}^p) - \boldsymbol{x}_1(\boldsymbol{x},\boldsymbol{y})^p)/p + (\partial\boldsymbol{y}_1/\partial\boldsymbol{x})^\sigma(\boldsymbol{x}^p,\boldsymbol{y}^p)\cdot\boldsymbol{x}_1 + (\partial\boldsymbol{y}_1/\partial\boldsymbol{y})^\sigma(\boldsymbol{x}^p,\boldsymbol{y}^p)\cdot\boldsymbol{y}_1$ is a p-power. We actually checked both cases, i.e. $a_0 \neq 0$ and $a_0 = 0$, and in both we could find a lift of the Frobenius. The formulas for $\boldsymbol{P}$ and $\boldsymbol{Q}$ when $a_0 \neq 0$ are too long to be put in here, but if $a_0 = 0$, we have that $\boldsymbol{P}(\boldsymbol{x})^3$ and $\boldsymbol{Q}(\boldsymbol{x},\boldsymbol{y})^3$ are lifts of

$$\begin{aligned}
&(b_0^6 + 2\,b_0^2\,c_0^2 + b_0^8\,c_0^3 + 2\,b_0^6\,c_0^4 + b_0^6\,c_0^6 + 2\,c_0^9)\,x_0^3\\
&\quad + (b_0^3 + 2\,b_0^7 + 2\,b_0^{11} + 2\,b_0\,c_0 + 2\,b_0^5\,c_0 + b_0^9\,c_0 + 2\,b_0^3\,c_0^2 + b_0^5\,c_0^3 + 2\,b_0^3\,c_0^4)\,x_0^6\\
&\quad + (1 + 2\,b_0^8 + 2\,b_0^{16} + 2\,b_0^{24} + b_0^6\,c_0 + 2\,b_0^{10}\,c_0 + 2\,b_0^{14}\,c_0 + b_0^8\,c_0^2 + 2\,b_0^{12}\,c_0^2\\
&\quad + b_0^2\,c_0^3 + b_0^6\,c_0^3 + b_0^{10}\,c_0^3 + 2\,b_0^{14}\,c_0^3 + 2\,c_0^4 + b_0^4\,c_0^4 + b_0^8\,c_0^4 + b_0^{12}\,c_0^4 + 2\,b_0^2\,c_0^5\\
&\quad + b_0^6\,c_0^5 + c_0^6 + b_0^{12}\,c_0^6 + 2\,b_0^6\,c_0^9 + c_0^{12})\,x_0^9 + (2\,b_0^5 + 2\,b_0^9 + b_0^3\,c_0 + 2\,b_0^3\,c_0^3)\,x_0^{12}\\
&\quad + (b_0^2 + 2\,b_0^6 + 2\,c_0)\,x_0^{15} + (2\,b_0^7 + 2\,b_0^{15} + 2\,b_0\,c_0 + 2\,b_0^5\,c_0\\
&\quad + 2\,b_0^3\,c_0^2 + b_0^3\,c_0^6)\,x_0^{18} + (1 + b_0^8 + 2\,b_0^6\,c_0 + b_0^6\,c_0^3 + 2\,c_0^6)\,x_0^{21}\\
&\quad + (b_0^5 + b_0^9 + 2\,b_0^3\,c_0 + 2\,b_0^3\,c_0^3)\,x_0^{24} + b_0^3\,x_0^{30}
\end{aligned}$$

and

$$\begin{aligned}
y_0^3\,[2\,b_0^{10} + b_0^{14} + b_0^{18} + 2\,b_0^4\,c_0 + 2\,b_0^8\,c_0 + 2\,b_0^{12}\,c_0 + 2\,b_0^6\,c_0^2 + c_0^3 \\
+ b_0^{12}\,c_0^3 + 2\,b_0^6\,c_0^6 + 2\,c_0^9 + (b_0^7 + 2\,b_0^{15} + b_0\,c_0 + b_0^5\,c_0 + b_0^3\,c_0^2 + 2\,b_0^9\,c_0^3 \\
+ 2\,b_0^3\,c_0^6)\,x_0^3 + (1 + 2\,b_0^{12} + 2\,b_0^6\,c_0^3 + 2\,c_0^6)\,x_0^6 + 2\,b_0^9\,x_0^9 \\
+ (2\,b_0^2 + c_0 + c_0^3)\,x_0^{12} + 2\,b_0^3\,x_0^{15} + (2 + 2\,b_0^{12} + 2\,b_0^6\,c_0^3 + 2\,c_0^6)\,x_0^{18} \\
+ 2\,b_0^3\,x_0^{27} + x_0^{30}]
\end{aligned}$$

respectively. The existence of this lift of the Frobenius leads us to believe that indeed what we just obtained is indeed the Mochizuki lift of C.

Bibliography

[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] S. Mochizuki. A theory of ordinary p-adic curves. *Publ. Res. Inst. Math. Sci.*, 32:957–1152, 1996.

[5] M. Raynaud. Around the Mordell conjecture for function fields and a conjeture of Serge Lang. *Lecture Notes in Math.*, 1016:1–19, 1983.

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

[7] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1985.

[8] J. F. Voloch and J. L. Walker. Codes over rings from curves of higher genus. *IEEE Trans. Inform. Theory*, 45:1768–1776, 1999.

[9] 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.

Vita

Luís Renato Abib Finotti was born in Uberlândia, Minas Gerais, Brazil, on March 30, 1973, the son of Eliane Espir Abib Finotti and Gilson Finotti. After completing his work at Palmares High School, São Paulo (Brazil), in 1990, he entered University of São Paulo. He received the degree of Bachelor of Science from University of São Paulo in 1994. In 1995, he entered the Masters Program of University of São Paulo, graduating in 1997. In the same year, he entered the Ph.D. Program of the University of Texas at Austin.

Permanent address: 2814 Nueces St.
Austin, TX – 78705

This dissertation was typeset with LaTeX[‡] by the author.

[‡]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.