MINIMAL DEGREE LIFTINGS OF HYPERELLIPTIC CURVES

LUÍS R. A. FINOTTI

ABSTRACT. The main goal of this paper is to analyze the properties of lifts of hyperelliptic curves $y_0^2 = f(x_0)$ over perfect fields of characteristic $p > 2$ (to hyperelliptic curves over the ring of Witt vectors) that have lifts of points whose coordinate functions have minimal degrees. It is shown that, when trying to minimize the degrees of the $\boldsymbol{x}$-coordinate, the $(n+1)$-th entry, say F_n, can be taken to be a polynomial in x_0 such that $(dp^n - (d-2))/2 \leq \deg F_n \leq (dp^n + (d-2))/2$, where $d = \deg f(x_0)$. Besides upper and lower bounds for the degrees, other topics discussed include a necessary condition to achieve the lower bounds and lifting the Frobenius. Computational aspects are also considered and the case of elliptic curves is analyzed in more detail. An explicit formula for derivatives of coordinate functions of the elliptic Teichmüller lift is proved, namely $dF_n/dx_0 = 0$, if $p = 2$, and $dF_n/dx_0 = A^{(p^n-1)/(p-1)}\, y_0^{p^n-1} - \sum_{i=0}^{n-1} F_i^{(p^{n-i}-1)}\, dF_i/dx_0$, if $p \geq 3$, where A is the Hasse invariant of the curve. Finally, we establish a connection between minimal degree liftings and Mochizuki's theory of "canonical liftings" in the case of genus 2 curves.

1. Introduction

Let k be a perfect field of characteristic $p > 0$. We say that an elliptic curve E/k is ordinary if the p-torsion subgroup of E is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Associated to an ordinary elliptic curve E, there exists a unique (up to isomorphisms) elliptic curve $\boldsymbol{E}$ over the ring $\boldsymbol{W}(k)$ of Witt vectors over k, called the *canonical lift* of E, and a map $\tau : E(\bar{k}) \to \boldsymbol{E}(\boldsymbol{W}(\bar{k}))$, called the *elliptic Teichmüller lift*, characterized by the following properties:

(1) the reduction modulo p of $\boldsymbol{E}$ is E;
(2) if σ denotes the Frobenius of both k and $\boldsymbol{W}(k)$, then the canonical lift of E^σ (the elliptic curve obtained by applying σ to the coefficients of the equation that defines E) is $\boldsymbol{E}^\sigma$;
(3) τ is an injective group homomorphism;

1991 *Mathematics Subject Classification.* Primary 11G20; Secondary 11T71.
Key words and phrases. elliptic curves, canonical liftings, elliptic Teichmüller lift, Witt vectors, minimal degree liftings, Mochizuki liftings.
This work was partly funded by CAPES (an agency of the Brazilian government).

(4) let $\phi : E \to E^\sigma$ denote the p-th power Frobenius; then there exists a map $\boldsymbol{\phi} : \boldsymbol{E} \to \boldsymbol{E}^\sigma$, such that the diagram

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

commutes. (In other words, there exists a *lift of the Frobenius.*)

This concept of canonical lifting of elliptic curves was first introduced by Deuring in [Deu41] and then generalized to Abelian varieties by Serre and Tate (see [LST64]). Apart from being of independent interest, this theory has been used in many applications, such as counting rational points in ordinary elliptic curves, as in Satoh's [Sat00], counting torsion points of curves of genus $g \geq 2$, as in Poonen's [Poo01] and Voloch's [Vol97], and coding theory, as in Voloch/Walker's [VW00]. This last reference, together with [VW99] (by the same authors) and Mochizuki's [Moc96], are the main motivation for this paper.

Before we make it clearer what we are going to pursue here, we need to introduce some more notation. We can identify $\boldsymbol{E}/\boldsymbol{W}(k)$ with its *Greenberg transform* $G(\boldsymbol{E})/k$, which is an (infinite dimensional) scheme over k, and we can then view τ as a morphism of schemes over k. Thus,

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

where $F_i, G_i \in k(x_0, y_0)$. One can prove that the F_i's are in fact in $k[x_0]$, and the G_i's, for $p \neq 2$, can be written as $G_i = y_0 \, H_i$, with $H_i \in k[x_0]$.

The error-correcting codes constructed by Voloch and Walker in [VW00] (using canonical liftings) have parameters that depend on the order of poles of the F_i's and G_i's at the point at infinity O (or equivalently, on the degrees of the F_i's and H_i's). In [Fin02] precise bounds for the orders were found:

Theorem 1.1. *We have*

$$\operatorname{ord}_O F_n \geq -(n+2)p^n + np^{n-1}, \quad \operatorname{ord}_O G_n \geq -(n+3)p^n + np^{n-1}.$$

for all $n \geq 0$. For $p > 2$, those bounds may be written

$$\deg F_n \leq \frac{(n+2)p^n - np^{n-1}}{2}, \quad \deg H_n \leq \frac{(n+3)p^n - np^{n-1} - 3}{2}.$$

Moreover, equality does not occur for $\operatorname{ord}_O F_n$ *(or for* $\deg F_n$*) if, and only if, p divides $(n+1)$, and the equality does not occur for* $\operatorname{ord}_O G_n$ *(or for* $\deg H_n$*) if, and only if, p divides $(n+1)(n+2)/2$.*

On the other hand, one can also use other lifts, different from the canonical, to construct codes. When estimating the paramenter of these codes, lifts with poles of smaller order, or equivalently, smaller degrees, give better bounds. In the cases dealt with in [VW00], only the reduction modulo p^2 of $E/\boldsymbol{W}(k)$ was considered. In that case, using the canonical lift instead of any other, was the best possible choice to keep the degrees small: Proposition 4.2 in [VW00] tells us that if we have any lift of points $\nu : (x_0, y_0) \mapsto ((x_0, F_1), (y_0, G_1))$ from the affine part of the elliptic curve E/k (possibly non-ordinary) to the affine part of the elliptic curve $\boldsymbol{E}/\boldsymbol{W}_2(k)$, satisfying $\operatorname{ord}_O F_1 \geq (-3p+1)$ or $\operatorname{ord}_O G_1 \geq (-4p+1)$, then E is ordinary, $\boldsymbol{E}$ is the canonical lift of E (modulo p^2) and ν is the elliptic Teichmüller lift.

But one can also use lifts modulo higher powers of p to construct codes. Moreover, only the *affine* part of the curve is really relevant. Although one might have expected that the canonical lift and elliptic Teichmüller lift would be again the best choices, it turns out that there are other lifts which yield even smaller degrees. Section 5 of [Fin02] presents a lift of points

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

from the affine part of the elliptic curve

$$E/\mathbb{F}_5 \ : \ y_0^2 = x_0^3 + x_0$$

to the affine part of its canonical lift

$$\boldsymbol{E}/\boldsymbol{W}_3(\mathbb{F}_5) \ : \ \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{x}$$

with $\deg \tilde{F}_2 = 37 < \deg F_2 = 45$ (and $\deg \tilde{H}_2 = \deg H_2 = 56$), where

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

denotes the elliptic Teichmüller lift. (Observe that, in contrast with τ, the lift ν *cannot* be extended to the point at infinity.)

We thus see that there are lifts which yield better bounds for the parameters of codes associated to them, and which therefore possibly give better codes. Since lifts with minimal degrees give us the best bounds, in this paper we study the properties of such lifts.

Similar ideas to those used in the case of elliptic curves can be applied to obtain lifts of *hyperelliptic* curves, and these curves may also be used in the construction of codes. (See [VW99]). Moreover, the results obtained here can be used to develop an algorithm to find the liftings of the curves as well as the lifts of points, and then the associated codes can be effectively constructed.

Throughout this paper, we will restrict ourselves to the case $p > 2$. The case $p = 2$ (for which similar results hold, and more concrete applications to coding theory might exist) requires different techniques and will be dealt with elsewhere.

Since we will be using hyperelliptic curves, throughout this paper we will use the following notation: let k be a perfect field of characteristic $p > 2$ and C be a hyperelliptic curve over k, given by

$$C/k : \quad y_0^2 = f(x_0), \tag{1.1}$$

where f is a monic polynomial of degree $d \geq 3$, with $(f, f') = 1$. (Here f' denotes the derivative of f.) Note that although we write only the affine equation for C, we think of C as a *projective curve*, i.e., the unique smooth compactification of the affine curve given by equation (1.1). We shall refer to the affine curve as the *affine part of* C.

Let also

$$\boldsymbol{C}/\boldsymbol{W}(k): \quad \boldsymbol{y}^2 = \boldsymbol{f}(\boldsymbol{x}), \tag{1.2}$$

where $\boldsymbol{f}$ is a monic polynomial that reduces to f modulo p, i.e., $\boldsymbol{C}$ is a lift of C. (Again, $\boldsymbol{C}$ is a *projective* curve.) Also, let U denote the affine part of C and $\boldsymbol{U}$ the affine part of $\boldsymbol{C}$.

Definition 1.2. Let C and $\boldsymbol{C}$ be as above. A *hyperelliptic lift (of points) from* C *to* $\boldsymbol{C}$ is a regular map $\nu : U(\bar{k}) \to \boldsymbol{U}(\boldsymbol{W}(\bar{k}))$ (so it is a map between the *affine parts only*) given by

$$\nu(x_0, y_0) = ((x_0, F_1, F_2, \dots), (y_0, G_1, G_2, \dots)), \tag{1.3}$$

such that $G_i = y_0 H_i$ and $F_i, H_i \in k[x_0]$ for all i. We also write $F_0 \stackrel{\text{def}}{=} x_0$, $G_0 \stackrel{\text{def}}{=} y_0$, $H_0 \stackrel{\text{def}}{=} 1$.

Observe that saying that ν is hyperelliptic is equivalent to saying that it commutes with the hyperelliptic involutions of C and $\boldsymbol{C}$.

We will be looking for lifts of points whose coordinate functions have poles of small order at infinity. For simplicity we shall refer to "degrees" instead of orders of poles, since we will be dealing with polynomials. But since we have polynomials in x_0 and y_0, to be precise we have to define $\deg x_0 \stackrel{\text{def}}{=} 1$ and $\deg y_0 \stackrel{\text{def}}{=} d/2$, since $y_0^2 = f(x_0)$. (We will deal mostly with polynomials in x_0.)

It also seems that the best way to obtain these small degrees is to proceed coordinate by coordinate, i.e., to first obtain the minimal degree for the second coordinate, and then, with the second coordinate fixed, to obtain minimal degree for the third, and so on.

We will consider here only hyperelliptic lifts of points. Although this assumption greatly simplifies our analysis, it might seem to defeat the purpose of obtaining minimal possible degrees. But, in this spirit of obtaining minimal degrees coordinate by coordinate, Proposition 5.2 will partly justify why this is not entirely bad. Also, the last few paragraphs of section 6 further clarifies this choice.

We may consider two different notions of minimal degree: one in which the curves C and $\boldsymbol{C}$ are fixed a priori, and another in which we only fix C and want to find a curve $\boldsymbol{C}$ which has a hyperelliptic lift of points having minimal degrees among all other choices of curves that reduce to C modulo p. We will make these two notions precise in the following two definitions below.

Definition 1.3. Let C and $\boldsymbol{C}$ be curves given by equations (1.1) and (1.2) respectively. A *minimal degree lift from* C *to* $\boldsymbol{C}/\boldsymbol{W}_2(k)$ *with respect to* $\boldsymbol{x}$ (resp., $\boldsymbol{y}$) is a hyperelliptic lift of points

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

where $\deg F_1$ (resp., $\deg H_1$) is minimal. Inductively, a *minimal degree lift from C to $\boldsymbol{C}/\boldsymbol{W}_{n+1}(k)$ with respect to $\boldsymbol{x}$* (resp., $\boldsymbol{y}$) is a hyperelliptic lift of points

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

whose reduction modulo p^n is a minimal degree lift from C to $\boldsymbol{C}/\boldsymbol{W}_n(k)$, and $\deg F_n$ (resp., $\deg H_n$) is minimal. Also, if we say "minimal degree lift from C to $\boldsymbol{C}/\boldsymbol{W}_{n+1}(k)$" without specifying with respect to what coordinate, we will be referring to the minimal degree lift with respect to $\boldsymbol{x}$.

Definition 1.4. Let C be a hyperelliptic curve given by (1.1). An *absolute minimal degree curve modulo p^2 over C (with respect to $\boldsymbol{x}$)* is a curve $\boldsymbol{C}/\boldsymbol{W}_2(k)$ (given by (1.2)) which reduces to C modulo p, and which satisfies the following property. Let

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

be a minimal degree lift from C to $\boldsymbol{C}$, and let $\tilde{\boldsymbol{C}}/\boldsymbol{W}_2(k)$ be any curve that reduces to C modulo p. Then for any minimal degree lift

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

from C to $\tilde{\boldsymbol{C}}$, we have $\deg \tilde{F}_1 \geq \deg F_1$.

Inductively, an *absolute minimal degree curve modulo p^{n+1} over C (with respect to $\boldsymbol{x}$)* is a curve $\boldsymbol{C}/\boldsymbol{W}_{n+1}(k)$ whose reduction modulo p^n is an absolute minimal degree curve modulo p^n over C, satisfying the following property. Let

$$\nu(x_0, y_0) = ((x_0, F_1, \ldots, F_{n-1}, F_n), (y_0, G_1, \ldots, G_{n-1}, G_n)),$$

be a minimal degree lift from C to $\boldsymbol{C}$, and let $\tilde{\boldsymbol{C}}/\boldsymbol{W}_{n+1}(k)$ be any curve whose reduction modulo p^n is equal to the reduction modulo p^n of $\boldsymbol{C}$. Then, for a minimal degree lift

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

from C to $\tilde{\boldsymbol{C}}$, we have $\deg \tilde{F}_n \geq \deg F_n$. In this case we call the minimal degree lift ν from C to $\boldsymbol{C}$ an *absolute minimal degree lift* of points (modulo p^{n+1}).

We also have the analogous definitions *with respect to $\boldsymbol{y}$*, rather than $\boldsymbol{x}$.

Remark. Note that in Definitions 1.3 and 1.4, the lift of points ν is hyperelliptic, and is therefore only a lift from the affine part of C to the affine part of $\boldsymbol{C}$.

2. Statement of Main Results

We will now describe how this paper is organized and state its main results.

In section 3 we introduce the notation and state some results that will be used in the following sections. In section 4 we deal with liftings of powers of the Frobenius and, as a corollary, we establish a formula for the derivatives of the entries of the $\boldsymbol{x}$-coordinate of the elliptic Teichmüller lift. Namely, we prove:

Theorem 2.1. *Let E be an ordinary elliptic curve and $\boldsymbol{E}$ be its canonical lift. Let $\tau : E(\bar{k}) \to \boldsymbol{E}(\boldsymbol{W}(\bar{k}))$ be the elliptic Teichmüller lift*

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

Then, for $n \geq 1$,

$$\frac{dF_n}{dx_0} = 0$$

if $p = 2$, and

$$\frac{dF_n}{dx_0} = A^{-(p^n-1)/(p-1)}\, y_0^{p^n-1} - x_0^{p^n-1} - \sum_{i=1}^{n-1} F_i^{(p^{n-i}-1)}\, \frac{dF_i}{dx_0}$$

if $p > 2$, where A is the Hasse invariant of E.

We observe that these derivatives allow us to create an algorithm, similar to the one described in the last section of [Fin02], to compute the canonical lift and elliptic Teichmüller lift modulo any power of p, although a generalization of Theorem 5.3 in [Fin02] (restated here as Theorem 3.3), would greatly improve such algorithm.

In section 5 we find upper bounds for the lifts (of hyperelliptic curves) with minimal degrees. We prove the following result:

Proposition 2.2. *Let C/k and $\boldsymbol{C}/\boldsymbol{W}(k)$ be curves given by equations* (1.1) *and* (1.2)*. Then there exists a* unique *minimal degree lift*

$$\nu = ((x_0, F_1, F_2, \dots), (y_0, y_0 H_1, y_0 H_2, \dots)),$$

from C to $\boldsymbol{C}$ with respect to $\boldsymbol{x}$, and we have

$$\deg F_n \leq \frac{dp^n + (d-2)}{2}$$

and

$$\deg H_n \leq \frac{(n(d-2)+d)p^n + n(d-2)p^{n-1} - d}{2},$$

for all $n > 0$.

We also prove the corresponding result for lifts with respect to $\boldsymbol{y}$:

Proposition 2.3. *Let the hypotheses and notation be as in Proposition 2.2, and suppose in addition that p does not divide $(d-1)$. Then, there exists a* unique *minimal degree lift*

$$\nu = ((x_0, F_1, F_2, \dots), (y_0, y_0 H_1, y_0 H_2, \dots)),$$

from C to $\boldsymbol{C}$ with respect to $\boldsymbol{y}$, and we have

$$\deg H_n \leq (d-1)p^n - 1$$

and

$$\deg F_n \leq \frac{(n(d-2)+2)p^n + n(d-2)p^{n-1}}{2},$$

for all $n > 0$.

In section 6 we prove lower bounds for the absolute minimal degree lifts:

Theorem 2.4. *Let*

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

where $n \geq 1$, *be a lift of points (not necessarily hyperelliptic) from the affine part of* C, *given by equation* (1.1), *to the affine part of a lift* $\boldsymbol{C}$, *given by equation* (1.2), *where* $F_i \in k[x_0]$ *with*

$$\deg F_i = \frac{dp^i - (d-2)}{2},$$

for $i = 0, \dots, (n-1)$. *Then,* $\deg F_n \geq (dp^n - (d-2))/2$. *If equality holds, then*

$$\frac{dF_n}{dx_0} = A^{-(p^n-1)/(p-1)} f(x_0)^{(p^n-1)/2} - \sum_{i=0}^{n-1} F_i^{p^{n-i}-1} \frac{dF_i}{dx_0}.$$

where A *is the (necessarily non-zero) coefficient of* x_0^{p-1} *in* $f(x_0)^{(p-1)/2}$.

Thus, Theorem 2.4 gives lower bounds for the absolute minimal degree lifts with respect to $\boldsymbol{x}$. The best one can expect is to have

$$\deg F_n = \frac{dp^n - (d-2)}{2} \tag{2.1}$$

for all $n \geq 1$. It also gives us a necessary condition to achieve these lower bounds: in order for the lower bound to be attained when $n = 1$, it is necessary for $A^{-1} f(x_0)^{(p-1)/2} - x_0^{p-1}$ to be a derivative. For this to occur, the coefficient of x_0^{rp-1} in $f(x_0)^{(p-1)/2}$ must be equal to zero for $r \neq 1$, and the coefficient of x_0^{p-1} must be non-zero. Also the formula for the derivative of F_n helps us to explicitly compute this lift when it exists.

In section 7 we analyze minimal degree lifts in the case of elliptic curves, and prove that, modulo p^3, we can achieve the lower bounds above. (Theorem 7.2.) We also relate the minimal degree lift with the elliptic Teichmüller lift.

In order to describe the results of section 8, we require the following definition:

Definition 2.5. Let C/k and $\boldsymbol{C}/\boldsymbol{W}_n(k)$ be curves such that the reduction modulo p of $\boldsymbol{C}$ is C and for which we have a lift of points $\nu : U(\bar{k}) \to \boldsymbol{U}(\boldsymbol{W}(\bar{k}))$ between the affine parts. Let also $\phi : C \to C^\sigma$ denote the Frobenius map in characteristic p. We say that $\boldsymbol{\phi} : \boldsymbol{U} \to \boldsymbol{U}^\sigma$ is a *lift of the Frobenius associated to* ν if it is a map that makes the diagram

$$\begin{array}{ccc} \boldsymbol{U}(\boldsymbol{W}_n(\bar{k})) & \xrightarrow{\boldsymbol{\phi}} & \boldsymbol{U}^\sigma(\boldsymbol{W}_n(\bar{k})) \\ {\scriptstyle\nu}\big\uparrow & & \big\uparrow{\scriptstyle\nu^\sigma} \\ U(\bar{k}) & \xrightarrow{\phi} & U^\sigma(\bar{k}) \end{array}$$

commute.

It is shown in section 4 that, modulo p^2, any lift of points has an associated lift of the Frobenius. The main result of section 8 gives a necessary and sufficient condition for a lift of the Frobenius modulo p^3 associated to a lift of points to exist. In order to be more precise, we need to establish some further notation.

Definition 2.6. Let $g(x_0, y_0) \in k[x_0, y_0]$ and $\boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}_2(k)$ be the lift of g defined by applying the Teichmüller lift to the coefficients of g, i.e., if λ is a coefficient of some monomial of g, then the corresponding monomial of $\boldsymbol{g}$ has coefficient $(\lambda, 0)$. (We shall refer to such lift as the *Teichmüller lift* of the polynomial g.) We define

$$\psi(g) \stackrel{\text{def}}{=} \psi(\boldsymbol{g}) \stackrel{\text{def}}{=} \text{reduction modulo } p \text{ of } \frac{\boldsymbol{g}^{\sigma}(\boldsymbol{x}^p, \boldsymbol{y}^p) - \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y})^p}{p}.$$

Remark. One can define $\psi(g)$ without lifting g, with a recursive definition: if g is a monomial, define $\psi(g) = 0$; if not let $m(x_0, y_0) = \lambda x_0^i y_0^j$ be a monomial of g, so that $g - m$ has one term less than g. If

$$b(r) \stackrel{\text{def}}{=} \frac{1}{p}\binom{p}{r}, \text{ for } r \in \{1, \dots, (p-1)\},$$

(and hence the $b(r)$'s are integers) then we can define

$$\psi(g) \stackrel{\text{def}}{=} \psi(g - m) - \sum_{r=1}^{p-1} b(r)(g - m)^r\, m^{p-r}.$$

The main result of section 8 may be stated as follows:

Proposition 2.7. *Let C/k and $\boldsymbol{C}/\boldsymbol{W}_3(k)$ be curves given by equations* (1.1) *and* (1.2), *and let*

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

be a hyperelliptic lift with

$$\frac{dF_1}{dx_0} = A^{-1} f(x_0)^{(p-1)/2} - x_0^{p-1},$$

where A is the coefficient of x_0^{p-1} in $f(x_0)^{(p-1)/2}$. Then, there is a lift of the Frobenius associated to ν if, and only if,

$$F_2 - x_0^{p(p-1)}\, F_1 - \psi(F_1) - \left(F_1'\right)^p F_1$$

and

$$G_2 - y_0^{p(p-1)}\, G_1 - \psi(G_1) - \left(\frac{\partial G_1}{\partial x_0}\right)^p F_1 - \left(\frac{\partial G_1}{\partial y_0}\right)^p G_1$$

are both p-th powers, say $P(x_0)^p$ and $Q(x_0, y_0)^p$, respectively. In this case, the lift of the Frobenius is given by

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

where $\boldsymbol{F}_1$ and $\boldsymbol{G}_1$ are the Teichmüller lifts of F_1 and G_1 respectively, and $\boldsymbol{P}$ and $\boldsymbol{Q}$ are lifts of P and Q to $\boldsymbol{W}_3(k)[\boldsymbol{x}]$ and $\boldsymbol{W}_3[\boldsymbol{x}, \boldsymbol{y}]$ respectively.

We then use this proposition in section 9 to prove that minimal degree lifts satisfying the lower bounds in section 6, or more precisely, lifts for which equation (2.1) holds for $i = 1, 2$, have a lift of the Frobenius modulo p^3. (Theorem 9.2.)

In section 10 we use this theory of minimal degree lifts to give examples of *Mochizuki lifts* for curves of genus 2 in characteristic 3: we observe that if the genus of the curve is greater than 1, there is no "canonical lift", i.e., we cannot lift the Frobenius. (See [Ray83].) On the other hand, Mochizuki has developed a theory of canonical liftings of higher genus curves (in [Moc96]), where there exists liftings of the Frobenius with certain singularities at finitely many points, which are referred to as the *supersingular points*. In this paper, a *Mochizuki lift* (modulo p^2) will satisfy the condition of the statement of Proposition 4.10 on pg. 1114 of [Moc96], i.e., the height of the lift of the Frobenius will be less than or equal to one minus the genus of the curve. (We define the height of the lift of the Frobenius precisely on Definition 10.2.) Note that a Mochizuki lift is not unique.

Mochizuki's theory does not have many known examples, and the results obtained in this paper allows us to explicitly find examples for curves of genus 2. More precisely, in sections 10 and 11 we prove:

Theorem 2.8. *Let k be a perfect field of characteristic 3 and C a smooth, proper, geometrically connected curve of genus 2 over k.*

(1) *Any Mochizuki lift of C to $\boldsymbol{W}_2(k)$ determines an absolute minimal degree curve modulo 9 over the affine curve U obtained by removing the supersingular points associated to the Mochizuki lift from C.*
(2) *Suppose that k is algebraically closed. Then if C admits a Mochizuki lift over $\boldsymbol{W}_2(k)$, then C can be given by*

$$y_0^2 = x_0^6 + a_0 x_0^4 + x_0^2 + b_0 x_0 + c_0,$$

where $a_0, b_0, c_0 \in k$, and the supersingular points associated to the Mochizuki lift are the two points at infinity. In particular, if the moduli of C are sufficiently general, then C may be written in that form.
(3) *Suppose that C is given by the equation*

$$y_0^2 = x_0^6 + a_0 x_0^4 + x_0^2 + b_0 x_0 + c_0,$$

where $a_0, b_0, c_0 \in k$. Then one can compute an explicit example of a Mochizuki lift of C modulo 9 (by computing a minimal degree lift). Moreover, the following three conditions are equivalent:
   (a) *this Mochizuki lift is Mochizuki-ordinary;*
   (b) *the Jacobian of the curve C is ordinary;*
   (c) $a_0 \neq 0$.

3. Definitions and Previous Results

In this section we will introduce notation and results from [Fin02] that will be used in the rest of the paper.

First we recall that, for $p \neq 2$, an elliptic curve given by

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

where $f(x)$ is a monic cubic, is ordinary if, and only if, the coefficient of x_0^{p-1} of $f^{(p-1)/2}$ is non-zero. We shall denote this coefficient by A and call it the *Hasse invariant* of E.

We now review some facts about Witt vectors. Let p be a prime, and and for each non-negative integer n consider

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

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:

$$W_n(S_0, \dots, S_n) = W_n(X_0, \dots, X_n) + W_n(Y_0, \dots, Y_n) \tag{3.1}$$

and

$$W_n(P_0, \dots, P_n) = W_n(X_0, \dots, X_n) \cdot W_n(Y_0, \dots, Y_n). \tag{3.2}$$

(See [Ser79].)

If $\boldsymbol{a} = (a_0, a_1, \dots)$ and $\boldsymbol{b} = (b_0, b_1, \dots)$ are Witt vectors,

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

and

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

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

Now, let K be a field of characteristic $p > 0$ and let $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation of the field K. (In the applications below, we will choose K to be the function field of a curve over k and v to be the order of vanishing at a point.) For $e, r \geq 0$, define:

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

and

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

(So, $U(e) = \bigcap_{r \geq 0} U_r(e)$.)

Lemma 3.1. *The sets $U(e)$ and $U_r(e)$ are subgroups of $\boldsymbol{W}(K)^\times$.*

Proof. The proof that $U(e)$ is a group can be found in [Fin02] (Lemma 2.2) and can be easily adapted to prove that the same is true of $U_r(e)$. $\square$

A careful examination of the proof of Lemma 2.2 in [Fin02] also gives us the following lemma:

Lemma 3.2. *Let $\boldsymbol{s}, \boldsymbol{t} \in U_{r-1}(e)$. Then, the $(r+1)$-th coordinate of $\boldsymbol{s} \cdot \boldsymbol{t}$ is given by*

$$t_0^{p^r} s_r + s_0^{p^r} t_r + \dots,$$

where all the omitted terms have valuation greater than or equal to $p^n(v(s_0\, t_0) - en)$.

Proof. The $(r+1)$-th coordinate of $\boldsymbol{s} \cdot \boldsymbol{t}$ is given by

$$\bar{P}_r(s_0, \dots, s_r, t_0, \dots, t_r) = t_0^{p^r} s_r + s_0^{p^r} t_r + \dots,$$

where the omitted terms are monomials in $s_0, \dots, s_{r-1}, t_0, \dots, t_{r-1}$.

The proof of Lemma 2.2 in [Fin02] bounds each monomial appearing in

$$\bar{P}_r(s_0, \dots, s_r, t_0, \dots, t_r).$$

In this case, we don't have the bounds for the s_r and t_r, but the bounds for $s_0, \dots, s_{r-1}$ and $t_0, \dots, t_{r-1}$ are enough to bound the valuations of the omitted terms. $\square$

The next theorem gives an important characterization of the canonical lift modulo p^3. It is also helpful in the explicit computation of such lifts.

Theorem 3.3. *Suppose that $p \neq 2, 3$ and that $\boldsymbol{E}/\boldsymbol{W}_3(k)$ is an elliptic curve whose reduction modulo p is E/k. Suppose also that there exists a lift of points*

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

between the affine parts of E and $\boldsymbol{E}$, such that, modulo p^2, E and τ are the canonical lift and elliptic Teichmüller lift respectively. Then E and τ are also the canonical lift and the elliptic Teichmüller lift modulo p^3 if, and only if,

$$\deg\left(x_0^{p^2} F_2 - \frac{3}{4} F_1^{2p}\right) \leq \frac{5p^2 - 1}{2}.$$

If this inequality holds, then it is in fact an equality.

Proof. This is Theorem 5.3 from [Fin02]. $\square$

4. Liftings of the Frobenius

In [VW00] and [Fin02], the derivatives of F_1 and F_2 (from the elliptic Teichmüller lift) were computed. In order to do this, the reduction modulo p of $1/p\, \boldsymbol{\phi}^*(d\boldsymbol{x}/\boldsymbol{y})$ and $(1/p\, \boldsymbol{\phi}^*)^2(d\boldsymbol{x}/\boldsymbol{y})$ were computed, where $\boldsymbol{\phi}$ denotes the lift of the Frobenius. The main goal of this section is to obtain more general results that will allow us to deduce the general formula for the derivative of F_n from the elliptic Teichmüller lift stated in Theorem 2.1, and to give similar results for hyperelliptic curves.

Theorem 4.1. *Let k be a perfect field of characteristic $p > 0$ and*

$$U/k \ : \ g(x_0, y_0) = 0$$

be an affine *curve in $\mathbb{A}^2$. Let*

$$\boldsymbol{U}/\boldsymbol{W}_{n+1}(k) \ : \ \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}) = 0$$

be an affine curve with reduction U, i.e., $\boldsymbol{g}$ reduces to g modulo p. If we have a lift of points $\nu : U(\bar{k}) \to \boldsymbol{U}(\boldsymbol{W}_{n+1}(\bar{k}))$ given by

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

with $F_i, G_i \in k[x_0, y_0]$, then we have a lift $\boldsymbol{\phi}^n : \boldsymbol{U} \to \boldsymbol{U}^{\sigma^n}$ of the p^n-th power Frobenius $\phi^n : U \to U^{\sigma^n}$ associated to ν (as in Definition 2.5) given by

$$\boldsymbol{\phi}^n(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\text{def}}{=} (\boldsymbol{x}^{p^n} + p\boldsymbol{F}_1^{p^{n-1}} + \dots + p^n \boldsymbol{F}_n, \boldsymbol{y}^{p^n} + p\boldsymbol{G}_1^{p^{n-1}} + \dots + p^n \boldsymbol{G}_n),$$

where $\boldsymbol{F}_i, \boldsymbol{G}_i \in \boldsymbol{W}_{n+1}(k)[\boldsymbol{x}, \boldsymbol{y}]$, and $\boldsymbol{F}_i$ (resp., $\boldsymbol{G}_i$) is a lift of $F_i \in k[x_0, y_0]$ (resp., G_i).

Proof. We need to prove that the map $\boldsymbol{\phi}^n$ above is well defined. It suffices to show that the map is well defined for the Greenberg transforms $G(\boldsymbol{U})$ and $G(\boldsymbol{U}^{\sigma^n})$. Writing $\boldsymbol{x} = (x_0, \dots, x_n)$ and $\boldsymbol{y} = (y_0, \dots, y_n)$,

$$\boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}) = (g_0(x_0, y_0), g_1(x_0, x_1, y_0, y_1), \dots, g_n(x_0, \dots, x_n, y_0, \dots, y_n)).$$

So, $G(\boldsymbol{U})$ is the defined as the common zeros of the equations $g_0, \dots, g_n$ in $\mathbb{A}^{2n+2}$. (Note that $g_0 = g$.) Since ν is a (well defined) lift, we have that

$$\nu^* g_1, \dots, \nu^* g_n \equiv 0 \pmod{(g_0)}. \tag{4.1}$$

(Observe that,

$$\nu^* g_i = g_i(x_0, F_1, \dots F_i, y_0, G_1, \dots, G_i),$$

for $i = 0, \dots n$.)

If $\boldsymbol{v} = (v_0, \dots, v_n)$ is a Witt vector of length $n+1$, then $p^i \boldsymbol{v}^{p^{n-i}}$ is the Witt vector whose the $(i+1)$-th coordinate is $v_0^{p^n}$ and whose other coordinates are zero. So, the map $\boldsymbol{\phi}^n$ defined in the statement is such that

$$\boldsymbol{\phi}^n = ((x_0^{p^n}, F_1^{p^n}, \dots, F_n^{p^n}), (y_0^{p^n}, G_1^{p^n}, \dots, G_n^{p^n})). \tag{4.2}$$

To prove that $\boldsymbol{\phi}^n$ is well defined, it suffices to prove that the coordinates of $\boldsymbol{g}^{\sigma^n}(\boldsymbol{\phi}^n(\boldsymbol{x},\boldsymbol{y}))$ are congruent to zero modulo I, where $I \stackrel{\text{def}}{=} (g_0,\dots,g_n)$. But, by equation (4.2),

$$\boldsymbol{g}^{\sigma^n}(\boldsymbol{\phi}^n(\boldsymbol{x},\boldsymbol{y})) = ((\nu^* g_0)^{p^n}, (\nu^* g_1)^{p^n}, \dots, (\nu^* g_n)^{p^n}),$$

and so, by equation (4.1), $\boldsymbol{\phi}^n$ is well defined.

Therefore, for any point $(\boldsymbol{x},\boldsymbol{y}) = ((x_0,\dots,x_n),(y_0,\dots,y_n)) \in \boldsymbol{U}(\boldsymbol{W}_{n+1}(\bar{k}))$, $\boldsymbol{\phi}^n(\boldsymbol{x},\boldsymbol{y}) = \nu^{\sigma^n} \circ \phi^n(x_0,y_0)$, and so the diagram

$$\begin{array}{ccc} \boldsymbol{U}(\boldsymbol{W}_{n+1}(\bar{k})) & \xrightarrow{\boldsymbol{\phi}^n} & \boldsymbol{U}^{\sigma^n}(\boldsymbol{W}_{n+1}(\bar{k})) \\ {\scriptstyle \nu}\uparrow & & \uparrow{\scriptstyle \nu^{\sigma^n}} \\ U(\bar{k}) & \xrightarrow{\phi^n} & U^{\sigma^n}(\bar{k}) \end{array}$$

commutes. $\square$

Corollary 4.2. *With the same hypotheses as Theorem 4.1, we have that the reduction modulo p of*

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

is $dF_n + F_{n-1}^{p-1} dF_{n-1} + \cdots + F_1^{p^{n-1}-1} dF_1 + x_0^{p^n-1} dx_0$.

Proof. Using the formula for $\boldsymbol{\phi}^n$ from the Theorem 4.1, we have

$$\left(\frac{1}{p^n}\,\boldsymbol{\phi}^n\right)^* d\boldsymbol{x} = \frac{1}{p^n} d\left(\boldsymbol{x}^{p^n} + p\boldsymbol{F}_1^{p^{n-1}} + \cdots + p^n \boldsymbol{F}_n\right) =$$

$$= d\boldsymbol{F}_n + \boldsymbol{F}_{n-1}^{p-1} d\boldsymbol{F}_{n-1} + \cdots + \boldsymbol{F}_1^{p^{n-1}-1} d\boldsymbol{F}_1 + \boldsymbol{x}^{p^n-1} d\boldsymbol{x},$$

which reduces to $dF_n + F_{n-1}^{p-1} dF_{n-1} + \cdots + F_1^{p^{n-1}-1} dF_1 + x_0^{p^n-1} dx_0$. $\square$

We now want to apply the previous corollary in the case of canonical liftings of elliptic curves to prove Theorem 2.1. But, in order to do use the corollary, we need to show that, modulo p^n, the n-th power of the lift of the Frobenius of the canonical lift is equal to the lift defined in Theorem 4.1. We need the following lemma:

Lemma 4.3. *Let C be a curve, $\boldsymbol{C}$ be a lift of C and $\boldsymbol{\phi} : \boldsymbol{U} \to \boldsymbol{U}^{\sigma}$ be* any *lift of the Frobenius between the affine parts. Then, if we set $\boldsymbol{x} = (x_0, x_1, \dots)$ and $\boldsymbol{y} = (y_0, y_1, \dots)$, the reductions of $(\boldsymbol{\phi}^*)^n(\boldsymbol{x})$ and $(\boldsymbol{\phi}^*)^n(\boldsymbol{y})$ modulo p^{n+1} depend only on x_0 and y_0.*

Proof. We prove the lemma by induction on n.

For any lift of the Frobenius $\boldsymbol{\phi}$,

$$\boldsymbol{\phi}^*(\boldsymbol{x}) = \boldsymbol{x}^p + p\boldsymbol{F}(\boldsymbol{x},\boldsymbol{y})$$

for some polynomial $\boldsymbol{F}(\boldsymbol{x},\boldsymbol{y}) \in \boldsymbol{W}(k)[\boldsymbol{x},\boldsymbol{y}]$. Modulo p^2, $p\boldsymbol{F}(\boldsymbol{x},\boldsymbol{y}) = (0, F(x_0,y_0)^p)$, where $F \in k[x_0,y_0]$ is the reduction modulo p of $\boldsymbol{F}$, and $\boldsymbol{x}^p = (x_0^p, 0)$. Thus, the lemma holds for $n=1$ and $\boldsymbol{\phi}^*(\boldsymbol{x})$, and the same method may be use to show that it also holds for $\boldsymbol{\phi}^*(\boldsymbol{y})$.

Now assume that the lemma holds for $(\boldsymbol{\phi}^*)^n(\boldsymbol{x})$ and $(\boldsymbol{\phi}^*)^n(\boldsymbol{y})$. We have

$$(\boldsymbol{\phi}^*)^{n+1}(\boldsymbol{x}) = (\boldsymbol{\phi}^*)^n((\boldsymbol{\phi}^*)(\boldsymbol{x})) = ((\boldsymbol{\phi}^*)^n(\boldsymbol{x}))^p + p\boldsymbol{F}((\boldsymbol{\phi}^*)^n(\boldsymbol{x}), (\boldsymbol{\phi}^*)^n(\boldsymbol{y})).$$

Since modulo p^{n+2}, both $\boldsymbol{a}^p$ and $p\boldsymbol{a}$ depend only on $\boldsymbol{a}$ modulo p^{n+1}, using the induction hypothesis one easily sees that the lemma holds for $(\boldsymbol{\phi}^*)^{n+1}(\boldsymbol{x})$, and in the analogous way, for $(\boldsymbol{\phi}^*)^{n+1}(\boldsymbol{y})$. $\square$

Proposition 4.4. *Let C be a curve, and suppose that $\boldsymbol{C}$ is a lift of C. Let*

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

be a lift of points between the affine parts and assume that there exists a lift of the Frobenius between affine parts associated to ν, say $\boldsymbol{\phi} : \boldsymbol{U} \to \boldsymbol{U}^\sigma$. Then, modulo p^{n+1}, $\boldsymbol{\phi}^n$ is equal to the map defined in Theorem 4.1, i.e.,

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

where $\boldsymbol{F}_i, \boldsymbol{G}_i \in \boldsymbol{W}_{n+1}(k)[\boldsymbol{x},\boldsymbol{y}]$, and $\boldsymbol{F}_i$ (resp., $\boldsymbol{G}_i$) is a lift of $F_i \in k[x_0,y_0]$ (resp., G_i).

Proof. We again work with the Greenberg transforms. Let $\pi : G(\boldsymbol{C})(\bar{k}) \to C(\bar{k})$ be the reduction modulo p (or the projection in the first coordinates). By Lemma 4.3, $\boldsymbol{\phi}^n(\boldsymbol{x},\boldsymbol{y})$ modulo p^{n+1} depends only on x_0 and y_0, and thus $\boldsymbol{\phi}^n \equiv \boldsymbol{\phi}^n \circ \ \nu \circ \pi \pmod{p^{n+1}}$. Since the diagram

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

commutes, $\boldsymbol{\phi}^n \circ \nu = \nu^{\sigma^n} \circ \phi^n$, and so $\boldsymbol{\phi}^n \equiv \nu^{\sigma^n} \circ \phi^n \circ \pi \pmod{p^{n+1}}$, or

$$\boldsymbol{\phi}^n \equiv ((x_0^p, F_1^p, \dots, F_n^p), (y_0^p, G_1^p, \dots, G_n^p)) \pmod{p^{n+1}}.$$

By looking at the proof of Theorem 4.1 (more precisely, equation (4.2)), one easily sees that the reduction modulo p^{n+1} of $\boldsymbol{\phi}^n$ is this case coincides with the map defined in that theorem. $\square$

Now we can prove Theorem 2.1.

Proof of Theorem 2.1. Assume first that $p > 2$. The reduction modulo p of

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

is a holomorphic differential. Thus, if ω denotes the reduction modulo p of

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

then ω is also holomorphic, and so, there is a $\lambda \in k$ such that $\omega = \lambda\, dx_0/y_0$. Applying the n-th power of the Cartier operator $\mathcal{C}$ to ω, we get

$$\mathcal{C}^n(\omega) = \mathcal{C}^n(\lambda\, dx_0/y_0) = \lambda^{p^{-n}} A^{(p^{-1}+\cdots+p^{-n})} \frac{dx_0}{y_0}.$$

On the other hand, since $(1/p\,\boldsymbol{\phi})^*$ is the "inverse" of the Cartier operator, $\mathcal{C}^n(\omega) = dx_0/y_0$. Therefore, $\lambda = A^{-(p^n-1)/(p-1)}$, and

$$\omega = A^{-(p^n-1)/(p-1)} \frac{dx_0}{y_0}.$$

But Proposition 4.4 tells us that we can use the Corollary 4.2 in this case, and we then get

$$\omega = \frac{\sum_{i=0}^{n} F_i^{p^{n-i}-1} dF_i}{y_0^{p^n}}$$

(with $F_0 \stackrel{\text{def}}{=} x_0$). Comparing these two expressions for ω we obtain the formula for dF_n/dx_0.

The case $p = 2$ is analogous. We just need to use the invariant differential

$$\frac{d\boldsymbol{x}}{2\boldsymbol{y} + \boldsymbol{x}}$$

instead of $d\boldsymbol{x}/\boldsymbol{y}$. Then we obtain

$$\mathcal{C}^n(\omega) = \mathcal{C}^n\left(\lambda \frac{dx_0}{x_0}\right) = \lambda^{p^{-n}} \frac{dx_0}{x_0},$$

and thus $\lambda = 1$. So,

$$\omega = \frac{dx_0}{x_0}.$$

On the other hand, by Corollary 4.2,

$$\omega = \frac{\sum_{i=0}^{n} F_i^{p^{n-i}-1} dF_i}{x_0^{p}}.$$

Comparing the two expressions for ω in the case $n = 1$, gives that $dF_1/dx_0 = 0$. Inductively, one can deduce then that $dF_n/dx_0 = 0$ for all n. $\square$

5. Minimal Degrees

We first try to justify why assuming that our lifts of points are all hyperelliptic lifts does not greatly compromise our goal of finding lifts of points with small order of poles at infinity (i.e., small degrees).

We will need the following lemma:

Lemma 5.1. *Every monomial of $\bar{P}_n$ (as defined in section 3) has even degree.*

Proof. Lemma 2.1 of [Fin02] states that the monomials $\prod X_i^{a_i} \prod Y_j^{b_j}$ of $\bar{P}_n$ are such that

$$\sum a_i\, p^i = \sum b_j\, p^j = p^n.$$

Since $p \equiv 1 \pmod 2$, we have

$$\sum a_i \equiv \sum b_j \equiv 1 \pmod 2,$$

and hence, the degree of a such monomial, namely $\sum a_i + \sum b_j$, is even. $\square$

Proposition 5.2. *Suppose that we have a lift of points*

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

where $n \geq 1$, from the affine part of the hyperelliptic curve C/k, given by equation (1.1)*, to the affine part of some lift $\boldsymbol{C}/\boldsymbol{W}_{n+1}(k)$, given by equation* (1.2)*. Also, assume that ν is hyperelliptic modulo p^n and write $F_n = F_{n,1} + y_0\, F_{n,2}$ and $G_n = G_{n,1} + y_0\, G_{n,2}$, with $F_{n,1}, F_{n,2}, G_{n,1}, G_{n,2} \in k[x_0]$. Then, the map*

$$\tilde{\nu} = ((x_0, F_1, \dots, F_{n-1}, F_{n,1}), (y_0, G_1, \dots, G_{n-1}, y_0\, G_{n,2})),$$

defines a hyperelliptic lift whose degrees are not larger than those of ν.

Proof. Writing $\boldsymbol{x} = (x_0, x_1, \dots)$ and $\boldsymbol{y} = (y_0, y_1, \dots)$, one can expand (1.2) using the multiplication and addition of Witt vectors. The equality of the coordinates on both sides of this expansion gives the equations that determine the Greenberg transform. In particular, comparing the $(n+1)$-th coordinates, we have:

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

where neither x_n nor y_n appear in any of the omitted terms. Since ν defines a lift, we have:

$$2y_0^{p^n} G_n + \cdots = f'(x_0)^{p^n} F_n + \dots. \tag{5.1}$$

The omitted terms on the right hand side of (5.1) involve only $x_0, F_1, \dots, F_{n-1} \in k[x_0]$, and therefore form a polynomial in $k[x_0]$. The omitted terms on the left hand side of (5.1) come from $\bar{P}_n(y_0, G_1, \dots, G_n, y_0, G_1, \dots, G_n)$, and by Lemma 5.1, each one has an even number of G_i's. Replacing each G_i by $y_0\, H_i$, we can factor an even power of y_0 in each monomial, and it will be multiplying a polynomial in $k[x_0]$. But since $y_0^2 = f(x_0)$, this factored term is also a polynomial in $k[x_0]$. Hence, all the omitted terms of (5.1) are polynomials in $k[x_0]$.

Thus, equation (5.1) implies that

$$2y_0^{p^n} (y_0\, G_{n,2}) + \cdots = f'(x_0)^{p^n} F_{n,1} + \dots$$

(with the same omitted terms as equation (5.1)) and

$$2f(x_0)^{(p^n-1)/2} G_{n,1} = f'(x_0)^{p^n} F_{n,2}.$$

Thus, taking $F_{n,2} = G_{n,1} = 0$ also gives us a well defined hyperelliptic lift of points, with degrees not greater than the degrees of F_n and G_n. $\square$

So, remembering that we want to obtain minimal degrees coordinate by coordinate, this shows that the last coordinate of the lift of points can always be made hyperelliptic if the previous coordinates already are, and in particular, modulo p^2, we can always have a hyperelliptic lift with minimal degrees.

Note also that in principle we could have lifts ν and $\tilde{\nu}$, say $\nu = ((x_0, F_1, F_2), (y_0, G_1, G_2))$ and $\tilde{\nu} = (x_0, \tilde{F}_1, \tilde{F}_2), (y_0, \tilde{G}_1, \tilde{G}_2))$ such that $\deg F_1 < \deg \tilde{F}_1$ but $\deg F_2 > \deg \tilde{F}_2$, and so our minimal lift (or even absolute minimal lift) might not have the minimal degree among all possible F_2's if we don't impose restrictions on the degree of F_1. But in general one expects that if $\deg F_1 < \deg \tilde{F}_1$, then also $\deg F_2 < \deg \tilde{F}_2$.

We now introduce a useful lemma, that will be essential for the proofs of Propositions 2.2 and 2.3:

Lemma 5.3. *Let $a, b, c \in k[x_0]$, with $\deg(a) = n$, $\deg(b) = m$, $\deg(c) = r$. 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 $\deg(u) \leq m - 1$ and $\deg(v) \leq s - m$ such that $au + bv = c$.*

Proof. We follow the same idea of Lemma IV.1 in [VW99]. 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 $\deg(u) \leq m - 1 < \deg(b)$, which implies $u = z = 0$. Thus $\ker \psi = \{0\}$. 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 can now prove the main results of this section.

Proof of Proposition 2.2. We will work in $U_r((d-2)(p+1)/p)$, where the valuation is defined by $v(x_0) \stackrel{\text{def}}{=} -2$, $v(y_0) \stackrel{\text{def}}{=} -d$, $v(\alpha) \stackrel{\text{def}}{=} 0$, for $\alpha \in k^\times$, $v(0) \stackrel{\text{def}}{=} \infty$, and extended in the natural way to $k[x_0, y_0]$. (In other words, if d is odd, v is the order of vanishing at the point at infinity, and if d is even, v is twice the order of vanishing at one of the points at infinity.)

We prove the theorem by constructing the F_n's and H_n's inductively. The case $n = 0$ is trivial. Now suppose we have constructed ν up to the n-th coordinate. We construct F_n and H_n in the following way: observe that $(x_0, F_1, \ldots, F_{n-1})$ and $(y_0, y_0 H_1, \ldots, y_0 H_{n-1})$ are both in the group $U_{n-1}((d-2)(p+1)/p)$, by the induction hypothesis.

We have in the $(n+1)$-th coordinate of the equation of $G(\boldsymbol{C})/k$,

$$-f'(x_0)^{p^n} x_n + 2\, y_0^{p^n}\, y_n = \dots,$$

and, since ν will be a lift, we need

$$-f'(x_0)^{p^n} F_n + 2\, f(x_0)^{(p^n+1)/2} H_n = \dots, \tag{5.2}$$

where no omitted term involves either F_n or H_n. (Here we view F_n and H_n as "unknowns", rather than as polynomials.)

By Lemmas 3.1 and 3.2, all the omitted terms in (5.2) have valuations greater than or equal to $-(n(d-2)+2d)p^n - n(d-2)p^{n-1}$. Let c denote these omitted terms. By the same argument as the one used in the proof of Proposition 5.2, c is a polynomial in x_0. Let $a \stackrel{\text{def}}{=} -f'(x_0)^{p^n}$ and $b \stackrel{\text{def}}{=} 2f(x_0)^{(p^n+1)/2}$. Then, by Lemma 5.3, there are polynomials u and v, with valuations greater than or equal to $-dp^n - (d-2)$ and $-(n(d-2)+d)p^n - n(d-2)p^{n-1} + d$ respectively, such that $au + bv = c$. Thus, we can define $F_n \stackrel{\text{def}}{=} u$, and $H_n \stackrel{\text{def}}{=} v$.

The fact that $\deg F_n$ is minimal comes from the uniqueness in Lemma 5.3. We cannot have a $\tilde{F}_n$ with degree less than the degree of F_n, unless we allow $\deg \tilde{H}_n > ((n(d-2)+d)p^n + n(d-2)p^{n-1} - d)/2$. But in this case the degree of the left hand side of the equation

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

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

Observe that if we have a supersingular elliptic curve E, by Proposition 4.2 in [VW00], the minimal lift from E to *any* lift $\boldsymbol{E}$ is such that $\deg F_1 \geq (3p+1)/2$, i.e., in this case the upper bound in Proposition 2.2 cannot be improved.

With the same approach, one can prove Proposition 2.3.

Proof of Proposition 2.3. The proof follows the exact same idea as the proof of Proposition 2.2: again we will work in $U((d-2)(p+1)/p)$ and we just apply Lemma 5.3 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. $\square$

Propositions 2.2 and 2.3 have obvious applications to elliptic curves, by taking $d = 3$. But by Theorem 1.1, we can see that taking E ordinary and $\boldsymbol{E}$ its canonical lift, we can have $\deg F_1 \leq (3p-1)/2$, $\deg H_1 \leq 2p-2$, and so have degrees smaller than the upper bounds found in Proposition 2.2. This (together with the results to be obtained in section 6) gives the motivation for the following proposition, with better bounds for $\deg H_n$:

Proposition 5.4. *Let C/k and $\boldsymbol{C}/\boldsymbol{W}(k)$ be curves given by equations* (1.1) *and* (1.2)*, and suppose that the minimal degree lift of points*

$$\nu = ((x_0, F_1, F_2, \dots), (y_0, y_0H_1, y_0H_2, \dots)),$$

is such that

$$\deg F_1 \leq \frac{dp - (d-2)}{2}$$

and

$$\deg H_1 \leq \frac{(2d-2)p - (d-2) - d}{2}.$$

Then, we must have

$$\deg F_n \leq \frac{dp^n + (d-2)}{2}$$

and

$$\deg H_n \leq \frac{(n(d-2)+d)p^n - n(d-2)p^{n-1} - d}{2},$$

for all $n > 0$.

Proof. The idea is that the restrictions on F_1 and H_1 allow us to work on $U_r((d-2)(p-1)/p)$ instead of $U_r((d-2)(p+1)/p)$. Inductively, the term c (as in the proof of Proposition 2.2) will have degree less than or equal to $(n(d-2)+2d)p^n - n(d-2)p^{n-1})/2$, and we just apply Lemma 5.3 again. □

6. Lower Bounds

The main goal of this section is to prove Theorem 2.4. F. Voloch proved the particular case of this theorem where $p = 3$, $d = 6$ and $n = 1$, and it is possible to generalize his proof. The proof given below is somewhat shorter.

Proof of Theorem 2.4. By Theorem 4.1, we have a lift $\boldsymbol{\phi}^n$ of the p^n-th power Frobenius ϕ^n. Let $\boldsymbol{U}$ denote the affine part of $\boldsymbol{C}$ and U denote the affine part of C . Then, by Corollary 4.2, the reduction modulo p of $(1/p^n\, \boldsymbol{\phi}^n)^*(d\boldsymbol{x}/\boldsymbol{y})$ is given by

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

Since $d\boldsymbol{x}/\boldsymbol{y}$ is regular in $\boldsymbol{U}$, ω must be regular on U. In particular, it is regular at the points with $y_0 = 0$, and since

$$\omega = \frac{2}{f(x_0)^{(p^n-1)/2}} \left(\sum_{i=0}^{n} F_i^{(p^{n-i}-1)} \frac{dF_i}{dx_0} \right) \frac{dy_0}{f'(x_0)},$$

we have that

$$\sum_{i=0}^{n} F_i^{(p^{n-i}-1)} \frac{dF_i}{dx_0} = g(x_0)\, f(x_0)^{(p^n-1)/2},$$

for some $g(x_0) \in k[x_0]$. (Remember that since the curve is non-singular, $(f, f') = 1$.) Therefore, $\deg F_n \geq (dp^n - (d-2))/2$ and if we have equality, necessarily $\lambda_n \stackrel{\text{def}}{=} g(x_0) \in k^\times$.

We now need to prove that $\lambda_n = A^{-(p^n-1)/(p-1)}$. First observe that, whether $n = 1$ or $n > 1$, we must have the equality for the degree of F_1, and thus we must have that

$$\frac{dF_1}{dx_0} = \lambda_1 f(x_0)^{(p-1)/2} - x_0^{p-1}.$$

for some $\lambda_1 \in k^\times$. But since the right hand side is a derivative in characteristic p, it cannot have a term in x_0^{p-1}, and hence $\lambda_1 = A^{-1}$, where A is the (necessarily non-zero) coefficient of x_0^{p-1} in $f(x_0)^{(p-1)/2}$.

Now, to prove that in general $\lambda_n = A^{-(p^n-1)/(p-1)}$, we proceed by induction: suppose that $\lambda_{n-1} = A^{-(p^{n-1}-1)/(p-1)}$, i.e., (with a computation analogous to the one above for ω in the case $n-1$)

$$\frac{1}{y_0^{p^{n-1}}} \left(\sum_{i=0}^{n-1} F_i^{(p^{n-1-i}-1)} \frac{dF_i}{dx_0} \right) dx_0 = A^{-(p^{n-1}-1)/(p-1)} \frac{dx_0}{y_0}. \tag{6.1}$$

Since

$$\omega = \frac{1}{y_0^{p^n}} \left(\sum_{i=0}^{n} F_i^{(p^{n-i}-1)} \frac{dF_i}{dx_0} \right) dx_0 = \lambda_n \frac{dx_0}{y_0},$$

applying the Cartier operator to both sides of the second equality of the equation above, we obtain

$$\frac{1}{y_0^{p^{n-1}}} \left(\sum_{i=0}^{n-1} F_i^{(p^{n-1-i}-1)} \frac{dF_i}{dx_0} \right) dx_0 = \lambda_n^{1/p} A^{1/p} \frac{dx_0}{y_0}.$$

Comparing with equation (6.1), we obtain the formula for λ_n. □

We observe here that the condition that $A^{-1} f(x_0)^{p-1} - x_0^{p-1}$ is a derivative, which is necessary to achieve these lower bounds, also seems to be *sufficient* to obtain $\deg F_1 = (dp - (d-2))/2$, i.e., if $A^{-1} f(x_0)^{(p-1)/2} - x_0^{p-1}$ is a derivative, then there is *some* lift $\boldsymbol{C}$ of C (modulo p^2) for which we can obtain a hyperelliptic lift of points satisfying $\deg F_1 = (dp - (d-2))/2$. (In another words, the absolute minimal degree lift modulo p^2 of C satisfying the above condition, has $\deg F_1$ equal to the lower bound of Theorem 2.4.) Note that if $\boldsymbol{C}$ is fixed from the beginning, one might not be able to obtain F_1 with such small degree.

For the case $d = 3$ (i.e., elliptic curves), one can always find ν and $\boldsymbol{C}$ such that $\deg F_1 = (dp - (d-2))/2$: the condition for this case is equivalent to saying that the elliptic curve is ordinary, and choosing $\boldsymbol{C}$ to be the canonical lift of C, we have the elliptic Teichmüller lift with $\deg F_1$ satisfying the lower bound. Also we have done several computations with hyperelliptic curves and they always had liftings of points satisfying the lower bound.

The condition also seems to be sufficient to obtain the lower bound for $\deg F_2$ as well, but not as many examples were tried in this case. But again, it is true for elliptic curves, as we will prove in section 7.

Also, observe that if we achieve the lower bound for $n = 1$, we can use Proposition 5.4 to bound the degrees instead of Proposition 2.2, getting better bounds for $\deg H_n$.

If these lower bounds can be achieved, the assumption that ν is hyperelliptic does not affect the fact that the degrees are minimal, meaning that we cannot have smaller degrees even if we drop this assumption. Indeed, by induction assume we can obtain a lift with F_n (not necessarily a polynomial in x_0) having degree less than or equal to $(dp^n - (d-2))/2$, while assuming also that, for $i = 0, \ldots, (n-1)$, $F_i \in k[x_0]$ with $\deg F_i = (dp^i - (d-2))/2$ and $G_i = y_0\, H_i$, with $H_i \in k[x_0]$. Let us write $F_n = F_{n,1} + y_0\, F_{n,2}$ and $G_n = G_{n,1} + y_0\, G_{n,2}$, with $F_{n,1}, F_{n,2}, G_{n,1}, G_{n,2} \in k[x_0]$. As in the proof of Proposition 5.2, we have in the $(n+1)$-th coordinate of the Greenberg transform:

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

with no x_n or y_n in the omitted terms, and this implies that

$$2f(x_0)^{(p^n-1)/2} G_{n,1} = f'(x_0)^{p^n} F_{n,2}.$$

Hence, if $F_{n,2} \neq 0$, then it is a multiple of $f(x_0)^{(p^n-1)/2}$, and thus the term $y_0\, F_{n,2}$ has degree greater than or equal to $dp^n/2$ (remember that we defined $\deg y_0 = d/2$) and then so does F_n, what is a contradiction to the initial assumption on the degree of F_n.

7. Minimal Degrees for Elliptic Curves

In this section we will study absolute minimal degree lifts and curves modulo p^3 of *ordinary* elliptic curves only and in characteristic $p \neq 2, 3$. (For $p = 2, 3$, the elliptic Teichmüller lift is also *the* (we have uniqueness) absolute minimal lift modulo p^3.)

As observed before, modulo p^2, Proposition 4.2 of [VW00] tells us that the choice of curve that gives the minimal possible degree for F_1 is the canonical lift itself, the minimal degree map is the elliptic Teichmüller lift and the degree of F_1 is *exactly* $(3p-1)/2$. Moreover, if E is not ordinary, then necessarily $\deg F_1 = (3p+1)/2$.

The next proposition is the key step in obtaining the results modulo p^3. It was stated as a conjecture (and proved, with the help of a computer, for $p \leq 877$) in the author's doctoral thesis [Fin01] and was later proved in general by J. Tate in [Tat02].

Proposition 7.1 (Tate). *Let $\tau = ((x_0, F_1), (y_0, G_1))$ be the elliptic Teichmüller lift from an ordinary elliptic curve*

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

to its canonical lift. Let $q(x_0)$ and $r(x_0)$ be the quotient and remainder of the division of F_1^2 by $x_0^p\, f(x_0)^{(p+1)/2}$, i.e.,

$$F_1^2 = (x_0^p\, f(x_0)^{(p+1)/2}) q(x_0) + r(x_0), \quad \deg r(x_0) \leq \frac{5p+1}{2}.$$

Then, in fact $\deg r(x_0) \leq (5p-1)/2$.

Proof. See [Tat02] for a proof of this proposition. □

In this section, since we are dealing with elliptic curves, we will write

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

for the elliptic Teichmüller lift and

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

for the minimal lift.

Theorem 7.2. *An absolute minimal degree lift*

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

of an ordinary elliptic curve E is such that $\deg \tilde{F}_2 = (3p^2 - 1)/2$ and the corresponding absolute minimal degree curve $\boldsymbol{E}$ is its canonical lift (modulo p^3). (So, up to isomorphism, the absolute minimal degree curve in this case is unique and satisfies the lower bound of section 6.) Moreover,

$$\frac{d\tilde{F}_2}{dx_0} = \frac{dF_2}{dx_0}.$$

Proof. We first prove that the minimal degree lift from E to its canonical lift $\boldsymbol{E}$ is such that $\deg \tilde{F}_2 = (3p^2 - 1)/2$. We will actually give a way to construct the absolute minimal degree lift from the elliptic Teichmüller lift: if

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

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

$$F_2 = f(x_0)^{(p^2+1)/2}\, q_1(x_0) + r_1(x_0) \quad (\deg r_1 \leq (3p^2 + 1)/2).$$

Now define $\tilde{F}_2 \stackrel{\text{def}}{=} r_1(x_0)$ and $\tilde{G}_2 \stackrel{\text{def}}{=} G_2 - y_0(f'(x_0)^{p^2} q_1(x_0))/2$. Then, we have

$$2y_0^{p^2} \tilde{G}_2 - f'(x_0)^{p^2} \tilde{F}_2 = 2y_0^{p^2} G_2 - f'(x_0)^{p^2} F_2,$$

and thus, by equation (5.1),

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

is another lift from E to its canonical lift, and since $\deg \tilde{F}_2 \leq (3p^2 + 1)/2$, by Proposition 2.2, it is the minimal lift.

We now have to prove that $\deg \tilde{F}_2 = (3p^2 - 1)/2$. Let $d(x_0) \stackrel{\text{def}}{=} x_0^{p^2} F_2 - 3/4\, F_1^{2p}$. Theorem 3.3 tells us that $\deg d(x_0) = (5p^2 - 1)/2$. Also, by Proposition 7.1,

$$\frac{3}{4} F_1^2 = (x_0^p\, f(x_0)^{(p+1)/2}) q(x_0) + r(x_0), \quad \text{with } \deg r(x_0) \leq (5p - 1)/2. \tag{7.1}$$

We can then write

$$\begin{aligned} x_0^{p^2} F_2 &= x_0^{p^2} f(x_0)^{(p^2+p)/2} q(x_0)^p + (r(x_0)^p + d(x_0)) \\ &= x_0^{p^2} f(x_0)^{(p^2+1)/2} \left(f(x_0)^{(p-1)/2} q(x_0)^p \right) + (r(x_0)^p + d(x_0)), \end{aligned} \tag{7.2}$$

with $\deg (r(x_0)^p + d(x_0)) = (5p^2 - 1)/2$, and thus it is the remainder of the division of $x_0^{p^2} F_2$ by $x_0^{p^2} f(x_0)^{(p^2+1)/2}$. We see then that $x_0^{p^2}$ divides this remainder and $\tilde{F}_2 = r_1(x_0) = (r(x_0)^p + d(x_0)) / x_0^{p^2}$, which implies that $\deg \tilde{F}_2 = (3p^2 - 1)/2$.

Hence, by Theorem 2.4, this has to be the absolute minimal degree lift, and

$$\frac{d\tilde{F}_2}{dx_0} = A^{-p-1} f(x_0)^{(p^2-1)/2} - x_0^{p^2-1} - F_1^{p-1} \frac{dF_1}{dx_0} = \frac{dF_2}{dx_0}.$$

(One could also deduce that $d\tilde{F}_2/dx_0 = dF_2/dx_0$ from equation (7.2), since it implies that

$$\begin{aligned} F_2 &= f(x_0)^{(p^2+p)/2} q(x_0)^p + \frac{r(x_0)^p + d(x_0)}{x_0^{p^2}} \\ &= f(x_0)^{(p^2+p)/2} q(x_0)^p + \tilde{F}_2, \end{aligned}$$

and taking derivatives would give us the result.)

Now, we prove that if we can obtain $\deg \tilde{F}_2 = (3p^2 - 1)/2$, then $\boldsymbol{E}$ must be the canonical lift of E. So assume we have a lift of E to some curve $\boldsymbol{E}$ (not necessarily the canonical lift) with $\deg \tilde{F}_2 = (3p^2 - 1)/2$. Let

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

(with the $q(x_0)$ from equation (7.1)) and

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

Then,

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

is another lift, since

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

But then, by hypothesis,

$$x_0^{p^2} \tilde{\tilde{F}}_2 - \frac{3}{4} F_1^{2p} = x_0^{p^2} \tilde{F}_2 + \left(x_0^p \, q(x_0) \, f(x_0)^{(p+1)/2} \right)^p - \frac{3}{4} F_1^{2p} = x_0^{p^2} \tilde{F}_2 - r(x_0)^p$$

has degree less than or equal to $(5p^2 - 1)/2$. Theorem 3.3 then tells us that $\boldsymbol{E}$ is the canonical lift modulo p^3, $\tilde{\tilde{F}}_2$ and $\tilde{\tilde{G}}_2$ are F_2 and G_2 from the elliptic Teichmüller lift.

□

Thus, modulo p^3, the absolute minimal degree curve over an ordinary elliptic curve is the same as its canonical lift.

So, we can modify the algorithm described in the section 6 of [Fin02] to compute this absolute minimal lift and the canonical lift of an elliptic curve over a perfect field of characteristic $p \geq 5$. The function (written for the package Magma) available at

`http://www.math.ucsb.edu/~finotti/can_lifts.html`

that computes the canonical lift and elliptic Teichmüller lift, also gives you an option to compute this absolute minimal degree lift instead of the elliptic Teichmüller lift.

8. A Necessary and Sufficient Condition to Lift the Frobenius

In sections 9 and 10 we will deal with liftings of the Frobenius modulo p^3, and so in this section we prove Proposition 2.7, which will allow us to obtain such liftings.

Lemma 8.1. *Let*

$$\boldsymbol{g}(\boldsymbol{x},\boldsymbol{y}) = \sum_{i,j} \boldsymbol{a}_{i,j}\, \boldsymbol{x}^i \boldsymbol{y}^j \in \boldsymbol{W}_2(k)[\boldsymbol{x},\boldsymbol{y}],$$

and suppose that

$$\boldsymbol{g}(\boldsymbol{x},\boldsymbol{y}) = (g_0(x_0,y_0), g_1(x_0,x_1,y_0,y_1)),$$

Then, if

$$\boldsymbol{a}_{i,j} = (a_{i,j,0}, a_{i,j,1})$$

we have

$$g_1(x_0,x_1,y_0,y_1) = x_1 \left(\frac{\partial g_0}{\partial x_0}\right)^p + y_1 \left(\frac{\partial g_0}{\partial y_0}\right)^p + \psi(g_0) + \sum_{i,j} a_{i,j,1}\, x_0^{pi} y_0^{pj}.$$

(Here ψ is the function defined in Definition 2.6.)

Sketch of the Proof. First we observe that, with the same notation as section 3,

$$\bar{S}_1(X_0,X_1,Y_0,Y_1) = X_1 + Y_1 + \psi(X_0 + Y_0)$$

and

$$\bar{P}_1(X_0,X_1,Y_0,Y_1) = X_1\, Y_0^p + X_0^p\, Y_1.$$

Then, one can easily prove that the formula is true for $\boldsymbol{g}$ equal to powers of $\boldsymbol{x}$ and $\boldsymbol{y}$, then for monomials, and finally for an arbitrary polynomial, by an induction on the number of terms. $\square$

Lemma 8.2. *Let $\boldsymbol{C}$ be a hyperelliptic curve with reduction C (given by equations* (1.2) *and* (1.1) *respectively) and*

$$\nu = ((x_0, F_1), (y_0, y_0 H_1))$$

a hyperelliptic lift of points. If

$$\frac{dF_1}{dx_0} = A^{-1} f(x_0)^{(p-1)/2} - x_0^{p-1},$$

then

$$2\,f\,H_1' + f'\,H_1 - A^{-1}\,(f')^p + f^{(p-1)/2}\,f' = 0.$$

Proof. By Lemma 8.1, when expanding the equation (1.2) as Witt vectors and comparing the second coordinates we have

$$2\,y_0^p\,y_1 = x_1\,(f')^p + \psi(f) + \dots,$$

where the omitted terms are p-th powers. Since ν is a lift, we have,

$$2\,f^{(p+1)/2}\,H_1 = F_1(f')^p + \psi(f) + \dots,$$

and so this is an equality of polynomials in x_0. Taking derivatives, one obtains

$$f'\,f^{(p-1)/2}\,H_1 + 2\,f^{(p+1)/2}\,H_1' = A^{-1}\,f^{(p-1)/2}\,(f')^p - f^{p-1}\,f',$$

and dividing both terms by the common factor $f^{(p-1)/2}$, we obtain the differential equation for H_1 from the statement. □

We also need the following simple lemma:

Lemma 8.3. *Let $P(X,Y)$ be a polynomial in two variables. 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 $P(X,Y)$. □

We finally prove Proposition 2.7, which can be quite useful when dealing with explicit computations.

Proof of Proposition 2.7. We first prove that the condition is necessary. Assume we have a lift of $\boldsymbol{\phi}$ associated to ν. By Theorem 4.1, it must have the form

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

for some $\boldsymbol{P},\boldsymbol{Q} \in \boldsymbol{W}_3(k)[\boldsymbol{x},\boldsymbol{y}]$.

Let δ be the p-derivation associated to $\boldsymbol{\phi}$ (as in [Bui96]):

$$\delta\boldsymbol{u} \stackrel{\text{def}}{=} \frac{\boldsymbol{\phi}^*\boldsymbol{u}^\sigma - \boldsymbol{u}^p}{p}.$$

We then have

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

and, using Lemma 8.3,

$$\begin{aligned}\delta^2 \boldsymbol{x} &= \frac{(\boldsymbol{F}_1 + p\boldsymbol{P})^\sigma \circ \boldsymbol{\phi} - (\boldsymbol{F}_1 + p\boldsymbol{P})^p}{p} \\ &= \frac{\boldsymbol{F}_1^\sigma(\boldsymbol{x}^p) - \boldsymbol{F}_1^p}{p} + \frac{d\boldsymbol{F}_1{}^\sigma}{d\boldsymbol{x}}(\boldsymbol{x}^p) \cdot \boldsymbol{F}_1 + \boldsymbol{P}^\sigma(\boldsymbol{x}^p) + p \cdot (\dots).\end{aligned} \tag{8.1}$$

But, by Lemma 2.6 of [Bui96], the reduction modulo p of $\delta^2\boldsymbol{x}$ must be equal to $F_2 - x_0^{p(p-1)} F_1$. Since the reduction modulo p of $\boldsymbol{P}^\sigma(\boldsymbol{x}^p)$ is clearly a p-th power, say P^p, and $\boldsymbol{F}_1$ is the Teichmüller lift of F_1,

$$F_2 - x_0^{p(p-1)}\, F_1 = \psi(F_1) + \left(F_1'\right)^p F_1 + P^p. \tag{8.2}$$

An analogous computation with $\delta^2\boldsymbol{y}$, gives

$$G_2 - y_0^{p(p-1)}\, G_1 = \psi(G_1) + \left(\frac{\partial G_1}{\partial x_0}\right)^p F_1 + \left(\frac{\partial G_1}{\partial y_0}\right)^p G_1 + Q^p,$$

and hence, the condition is necessary.

We now prove the converse, more precisely, that $\boldsymbol{\phi}$ is well defined and that the diagram

$$\begin{array}{ccc} \boldsymbol{U}(\boldsymbol{W}_3(\bar{k})) & \xrightarrow{\ \boldsymbol{\phi}\ } & \boldsymbol{U}^\sigma(\boldsymbol{W}_3(\bar{k})) \\ {\scriptstyle\nu}\big\uparrow & & \big\uparrow{\scriptstyle\nu^\sigma} \\ U(\bar{k}) & \xrightarrow{\ \phi\ } & U^\sigma(\bar{k}) \end{array} \tag{8.3}$$

commutes, where U and $\boldsymbol{U}$ are the affine parts of C and $\boldsymbol{C}$ respectively. It suffices to prove it for the Greenberg transform. Defining

$$\boldsymbol{g} \stackrel{\text{def}}{=} \boldsymbol{y}^2 - \boldsymbol{f}(\boldsymbol{x}),$$

we write

$$\boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}) = (g_0(x_0, y_0), g_1(x_0, x_1, y_0, y_1), g_2(x_0, x_1, x_2, y_0, y_1, y_2)).$$

Then, to prove that $\boldsymbol{\phi}$ is well defined, it suffices to prove that $\boldsymbol{\phi}^* g_i^\sigma \in I$, for $i = 0, 1, 2$, where $I \stackrel{\text{def}}{=} (g_0, g_1, g_2)$.

By Theorem 4.1, we have that $\boldsymbol{\phi}^* g_0^\sigma, \boldsymbol{\phi}^* g_1^\sigma \in I$. So we just need to show that $\boldsymbol{\phi}^* g_2^\sigma \in I$.

One has

$$\boldsymbol{x}^p = (x_0, x_1, x_2)^p = (x_0^p, 0, x_0^{p^2(p-1)} x_1^p).$$

Also, by Lemma 8.1

$$p\boldsymbol{F}_1 = (0, F_1^p, \left(x_1 (F_1')^p + \psi(F_1)\right)^p).$$

Hence,

$$\boldsymbol{x}^p + p\boldsymbol{F}_1 + p^2\boldsymbol{P} = (x_0^p, F_1^p, F_2^p + \mathfrak{X}_2^p)\,, \tag{8.4}$$

where,

$$\mathfrak{X}_2 \stackrel{\text{def}}{=} (x_1 - F_1)\left(x_0^{p-1} + F_1'\right)^p,$$

and in a similar manner,

$$\boldsymbol{y}^p + p\boldsymbol{G}_1 + p^2\boldsymbol{Q} = (y_0^p, G_1^p, G_2^p + \mathcal{Y}_2^p) \tag{8.5}$$

where

$$\mathcal{Y}_2 \stackrel{\text{def}}{=} (x_1 - F_1)\left(y_0\, H_1'\right)^p + (y_1 - G_1)\left(y_0^{p-1} + H_1\right)^p.$$

Note that

$$g_2^\sigma = 2y_0^{p^2} y_2 - ((f')^\sigma(x_0))^{p^2} x_2 + \dots,$$

where no omitted term depends on either x_2 or y_2. Hence

$$\boldsymbol{\phi}^* g_2^\sigma = 2y_0^{p^3}(G_2 + \mathcal{Y}_2)^p - f'(x_0)^{p^3}(F_2 + \mathcal{X}_2)^p + \dots. \tag{8.6}$$

Since

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

is a lift,

$$2y_0^{p^3} G_2^p - f'(x_0)^{p^3} F_2^p + \dots \equiv 0 \pmod{(g_0)},$$

where the omitted terms are the same as the ones in formula (8.6). Therefore

$$\boldsymbol{\phi}^* g_2^\sigma \equiv 2y_0^{p^3} \mathcal{Y}_2^p - f'(x_0)^{p^3} \mathcal{X}_2^p \pmod{I},$$

and it suffices to prove that

$$2y_0^{p^2} \mathcal{Y}_2 - f'(x_0)^{p^2} \mathcal{X}_2 \equiv 0 \pmod{I},$$

or,

$$(x_1 - F_1)\left(-A^{-1}\,(f')^p\, f^{(p-1)/2} + 2\, f^{(p+1)/2}\, H_1'\right)^p \\ + (y_1 - G_1)\, 2\, y_0^p \left(f^{p-1} + f^{(p-1)/2}\, H_1\right)^p \equiv 0 \pmod{I}.$$

Factoring $f^{(p^2-p)/2}$, it is enough to prove

$$(x_1 - F_1)\left(-A^{-1}\,(f')^p + 2\, f\, H_1'\right)^p + (y_1 - G_1)\, 2\, y_0^p \left(f^{(p-1)/2} + H_1\right)^p \equiv 0 \pmod{I}. \tag{8.7}$$

Using Lemma 8.2, equation (8.7) becomes

$$\left(H_1 + f^{(p-1)/2}\right)^p \left((x_1 - F_1)(-f')^p + (y_1 - G_1)(2\, y_0)^p\right) \equiv 0 \pmod{I}.$$

But $g_1, \nu^* g_1 \equiv 0 \pmod{I}$, and then

$$g_1(x_0, x_1, y_0, y_1) - g_1(x_0, F_1, y_0, G_1) = (x_1 - F_1)(-f')^p + (y_1 - G_1)(2\, y_0)^p \equiv 0 \pmod{I},$$

what finishes the proof that $\boldsymbol{\phi}$ is well defined.

Finally, equations (8.4) and (8.5) show the diagram (8.3) commutes. $\square$

The proof of the proposition above also gives us the following corollary:

Corollary 8.4. *Let C/k and $\boldsymbol{C}/\boldsymbol{W}_3(k)$ be curves given by equations* (1.1) *and* (1.2)*, and suppose that we can lift the Frobenius for the affine part of $\boldsymbol{C}$. Let*

$$\nu \stackrel{\text{def}}{=} ((x_0, F_1, F_2), (y_0, G_1, G_2))$$

be the lift of points, and also assume that $F_i \in k[x_0]$. Then,

$$\frac{dF_2}{dx_0} = \left(\frac{dF_1}{dx_0}\right)^{p+1} + \left(\frac{dF_1}{dx_0}\right)^{p} x_0^{p-1} + \left(x_0^{p(p-1)} - F_1^{p-1}\right)\frac{dF_1}{dx_0}.$$

In particular, if $dF_1/dx_0 = \lambda\, y_0^{p-1} - x_0^{p-1}$ for some $\lambda \in k^{\times}$, then

$$\frac{dF_2}{dx_0} = \lambda^{p+1}\, y_0^{p^2-1} - x_0^{p^2-1} - F_1^{p-1}\frac{dF_1}{dx_0}.$$

Proof. By Proposition 2.7, the first coordinate of the lift of the Frobenius has the form

$$\boldsymbol{x}^p + p\boldsymbol{F}_1 + p^2\boldsymbol{P}$$

where $\boldsymbol{F}_1$ is a lift of F_1 to $\boldsymbol{W}_3(k)[\boldsymbol{x}]$ and $\boldsymbol{P}$ is some polynomial. Equation (8.2) also holds in this case. Observing that

$$\frac{d\psi(\boldsymbol{F}_1)}{dx_0} = x_0^{p-1}\left(\frac{dF_1}{dx_0}\right)^{p} - F_1^{p-1}\frac{dF_1}{dx_0}, \tag{8.8}$$

if we take derivatives of equation (8.2) we obtain the formula for dF_2/dx_0 in the statement. □

9. Minimal Lifts and the Frobenius

By Theorem 4.1, the existence of a lift from C to $\boldsymbol{C}/\boldsymbol{W}_2(k)$ is enough to give a lift of the Frobenius ϕ on the affine part of C. On the other hand, the existence of a lift from C to $\boldsymbol{C}/\boldsymbol{W}_3(k)$ merely guarantees a lift of ϕ^2. Of course, in the case of elliptic curves, the canonical lift always has a lift of ϕ associated to τ for any power of p. So, one could ask if there is also a lift of the Frobenius (between the affine parts) associated to the minimal lift, at least modulo p^3.

Theorem 9.2 below gives a precise answer to this question. But we first need the following lemma:

Lemma 9.1. *Let*

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

be a lift of points from the affine part of C, given by equation (1.1)*, to the affine part of a lift $\boldsymbol{C}$, given by equation* (1.2)*, with*

$$\frac{dF_i}{dx_0} = A^{-(p^i-1)/(p-1)} f(x_0)^{(p^i-1)/2} - \sum_{j=0}^{i-1} F_j^{p^{i-j}-1}\,\frac{dF_j}{dx_0},$$

for $i = 1, \dots, n$, where A denotes the coefficient of x_0^{p-1} in $f^{(p-1)/2}$. Then

$$dG_i = \left(A^{-(p^i-1)/(p-1)} (f')^{p^i-1} - y_0^{p^i-1}\right) dy_0 - \sum_{j=1}^{i-1} G_j^{p^{i-j}-1} dG_j.$$

Proof. We fix some $i \in \{1, \ldots, n\}$, and work modulo p^{i+1}. Then, by Corollary 4.2, the reduction modulo p of $(1/p^i \boldsymbol{\phi}^i)^*(d\boldsymbol{x}/\boldsymbol{y})$ is given by

$$\omega \stackrel{\text{def}}{=} \frac{1}{y_0^{p^i}} \left(\sum_{j=0}^{i} F_j^{(p^{i-j}-1)} \frac{dF_j}{dx_0} \right) dx_0 = A^{-(p^i-1)/(p-1)} \frac{dx_0}{y_0}.$$

On the other hand, since $d\boldsymbol{x}/\boldsymbol{y} = 2d\boldsymbol{y}/\boldsymbol{f}'$, and by the analogous to Corollary 4.2 for $d\boldsymbol{y}$, we have that

$$\omega = 2 \left(\frac{dG_i + \sum_{j=0}^{i-1} G_j^{p^{i-j}-1} dG_j}{(f')^{p^i}} \right).$$

Since $dx_0/y_0 = 2dy_0/(f')$, comparing the two expressions for ω we obtain the formula for dG_i in the statement. $\square$

Theorem 9.2. *Let*

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

be a hyperelliptic lift of points from C, given by equation (1.1), to a lift $\boldsymbol{C}$, given by equation (1.2), where again we write $G_i = y_0 H_i$ with $H_i \in k[x_0]$. If

$$\frac{dF_i}{dx_0} = A^{-(p^i-1)/(p-1)} f(x_0)^{(p^i-1)/2} - \sum_{j=0}^{i-1} F_j^{p^{i-j}-1} \frac{dF_j}{dx_0},$$

for $i = 1, 2$, where A denotes the coefficient of x_0^{p-1} in $f^{(p-1)/2}$, then there is a lift of the Frobenius modulo p^3. In particular, if the minimal degree lift of C satisfies the lower bounds in Theorem 2.4, namely $\deg F_1 = (dp - (d-2))/2$ and $\deg F_2 = (dp^2 - (d-2))/2$, there is a lift of the Frobenius modulo p^3.

Proof. We use Proposition 2.7. So, it suffices to prove that

$$\frac{d}{dx_0} \left(F_2 - x_0^{p(p-1)} F_1 - \psi(F_1) - \left(F_1'\right)^p F_1 \right) = 0 \tag{9.1}$$

and

$$d \left(G_2 - y_0^{p(p-1)} G_1 - \psi(G_1) - \left(\frac{\partial G_1}{\partial x_0} \right)^p F_1 - \left(\frac{\partial G_1}{\partial y_0} \right)^p G_1 \right) = 0 \tag{9.2}$$

By using equation (8.8), the equality in (9.1) is easily verified.

The proof of equation (9.2) is also a straightforward calculation, but requires a little more work. First we observe that

$$d\psi(G_1) = \left(\frac{\partial G_1}{\partial x_0} \right)^p x_0^{p-1} dx_0 + \left(\frac{\partial G_1}{\partial y_0} \right)^p y_0^{p-1} dy_0 - G_1^{p-1} dG_1.$$

So, the left-hand-side of equation (9.2) becomes

$$dG_2 - y_0^{p(p-1)} dG_1 - \left(\frac{\partial G_1}{\partial x_0}\right)^p x_0^{p-1} dx_0 + \left(\frac{\partial G_1}{\partial y_0}\right)^p y_0^{p-1} dy_0 \\ - G_1^{p-1} dG_1 - \left(\frac{\partial G_1}{\partial x_0}\right)^p (A^{-1} f^{(p-1)/2} - x_0^{p-1}) dx_0 - \left(\frac{\partial G_1}{\partial y_0}\right)^p dG_1.$$

Using Lemma 9.1, $dx_0 = (2y_0/f')\, dy_0$ and $G_1 = y_0\, H_1$, one sees that the expression above is equal to

$$\left(A^{-1}(f')^p - f^{(p-1)/2}\, f' - f'\, H_1 - 2\, f\, H_1'\right)^p \frac{A^{-1}}{f'} dy_0,$$

which, by Lemma 8.2, is equal to zero. □

With the help of this theorem, we can prove the following proposition that deals with the case of minimal degree lifts of elliptic curves.

Proposition 9.3. *Let*

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

be the minimal lift from E (ordinary) to $\boldsymbol{E}/\boldsymbol{W}_3(k)$, such that, modulo p^2, $\boldsymbol{E}$ is the canonical lift and ν gives us the Teichmüller lift. We have a lift of the Frobenius associated to ν if, and only if, $\deg \tilde{F}_2 = (3p^2 - 1)/2$ *(and then ν is the absolute minimal degree lift and $\boldsymbol{E}$ is the canonical lift also modulo p^3).*

Proof. Assume that we have a lift of $\boldsymbol{\phi}$ associated to ν. So

$$\tilde{F}_2 - x_0^{p(p-1)}\, F_1 - \psi(F_1) - \left(F_1'\right)^p F_1$$

is a p-th power by Proposition 2.7, and thus cannot have a term of degree $(3p^2 + 1)/2$. Since all terms in the above equation, except possibly $\tilde{F}_2$, have degrees less than or equal to $(3p^2 - 1)/2$, $\deg \tilde{F}_2 \leq (3p^2 - 1)/2$, and hence ν is the absolute minimal degree lift.

The converse is a trivial consequence of the Theorem 9.2.

□

10. Mochizuki Lifts

As mentioned in section 2, curves of genus $g > 1$ do not have lifts of the Frobenius (see [Ray83]), but Mochizuki showed in [Moc96] that a *Mochizuki-ordinary* (defined in section 11) curve of genus g admits a lift of the Frobenius with certain singularities. Although the theory is completely developed (over almost two hundred pages), few examples are known of Mochizuki lifts. In this section we give an example of a minimal degree lift that is also a Mochizuki lift. (Observe that Mochizuki lifts are supposed to have a lift of points with "small" degrees.)

We first observe that the number of singularities of Mochizuki lifts has to be equal to $(g-1)(p-1)$: indeed, Corollary 4.9, Proposition 4.10 and Definition 4.11 of [Moc96] on pg. 1116 and 1117, tell us that for the lifting of the Frobenius $\boldsymbol{\phi}$,

$$\mathrm{ht}(\boldsymbol{\phi}) = -p(g-1) + \deg(C-U) = (1-g)$$

where $\mathrm{ht}(\boldsymbol{\phi})$ denotes the *height* of $\boldsymbol{\phi}$ (which we will discuss in more detail below) and U is the open set on which we can lift the Frobenius. (Note that we have no marked points!) Thus, $\deg(C-U) = (p-1)(g-1)$.

Finding an explicit example of a Mochizuki lift was Voloch's motivation for proving Theorem 2.4 for $p=3$, $d=6$ and $n=1$: genus 2 curves are necessarily hyperelliptic, and if the two supersingular points form a set that is invariant under the hyperelliptic involution, we can assume that those points are at infinity. But Mochizuki's theory is indeed invariant with respect to the hyperelliptic involution. Roughly, this is true because the hyperelliptic involution can be deformed along with an arbitrary deformation of the curve. Hence, in the genus 2 case, the supersingular points can always be put at infinity.

Note that the genus 2 case is the only one for which we can try to relate Mochizuki's theory and minimal degree lifts, since for the former we have $(p-1)(g-1)$ singularities and for the latter either 1 (if d is odd) or 2 (if d is even).

We will now establish the connection with Mochizuki's theory, as outlined to the author by the referee of this paper. We will consider a genus 2 curve

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

where k is a perfect field of characteristic 3 and $\deg f = 6$, and assume it admits a Mochizuki lift

$$\boldsymbol{C}/\boldsymbol{W}_2(k) : \boldsymbol{y}^2 = \boldsymbol{f}(\boldsymbol{x}),$$

with supersingular points at infinity. As in [Bui96], the lift of the Frobenius defines a lift of points (between the affine parts) $\nu(x_0, y_0) = ((x_0, F_1), (y_0, G_1))$. (The lift of the Frobenius is then a lift of the Frobenius associated to ν.)

Definition 10.1. Let $\boldsymbol{\xi}_P$ be a local Frobenius defined in a neighborhood of the point in $\boldsymbol{P} \in \boldsymbol{C}$ with reduction P. Let $\boldsymbol{t}$ be a local parameter at $\boldsymbol{P}$ and let δ_P be the reduction modulo p of the rational function

$$\frac{1}{p}(\boldsymbol{\xi}_P^*(\boldsymbol{t}^\sigma) - \boldsymbol{\phi}^*(\boldsymbol{t}^\sigma)).$$

Then, the *local height of* $\boldsymbol{\phi}$ at P, denoted by $\mathrm{ht}_P(\boldsymbol{\phi})$, is zero if δ_P is regular at P, and equal to the order of the pole of δ_P at P otherwise. (As in [Moc96], pg. 1116.)

By Definition 4.7 and Proposition 4.8 in [Moc96], pg. 1116, we can define:

Definition 10.2. The *height of the lift of the Frobenius*, denoted by $\mathrm{ht}(\boldsymbol{\phi})$, is given by

$$\mathrm{ht}(\boldsymbol{\phi}) \stackrel{\text{def}}{=} \left(\sum_{P \in C} [k(P) : k] \ \mathrm{ht}_P(\boldsymbol{\phi}) \right) - p(g-1), \tag{10.1}$$

where $\mathrm{ht}_P(\boldsymbol{\phi})$ is the local height at P and $k(P)$ is the minimal field of definition of P over k.

We now compute the local heights. Since $\boldsymbol{\phi}$ is regular on the affine part of C, the non-zero local heights can only occur at the points at infinity, say P_1 and P_2. So, for $i = 1, 2$, we have that $\boldsymbol{t} = 1/\boldsymbol{x}$ is a local parameter at $\boldsymbol{P}_i$, the points at infinity of $\boldsymbol{C}$. Hence

$$\boldsymbol{\xi}^*_{P_i}(\boldsymbol{t}^\sigma) = \boldsymbol{t}^3 + 3 \cdot \dots = \frac{1}{\boldsymbol{x}^3} + 3 \cdot \dots,$$

where the omitted terms are regular at $\boldsymbol{P}_i$. On the other hand,

$$\boldsymbol{\phi}^*(\boldsymbol{t}^\sigma) = \frac{1}{\boldsymbol{\phi}^*(\boldsymbol{x})} = \frac{1}{\boldsymbol{x}^3 + 3\boldsymbol{F}_1 + 9 \cdot \dots},$$

where $\boldsymbol{F}_1$ is a lift of F_1. So,

$$\frac{1}{3}(\boldsymbol{\xi}^*_{P_i}(\boldsymbol{t}^\sigma) - \boldsymbol{\phi}^*(\boldsymbol{t}^\sigma)) = \frac{\boldsymbol{F}_1 + 3 \cdot \dots}{\boldsymbol{x}^3(\boldsymbol{x}^3 + 3\boldsymbol{F}_1 + 9 \cdot \dots)} + \cdots$$

where the omitted terms after the plus sign are regular at $\boldsymbol{P}_i$. So

$$\delta_{P_i} = \frac{F_1}{x_0^6} + \dots,$$

where the omitted terms are regular at P_i, and hence

$$\mathrm{ht}_{P_i}(\boldsymbol{\phi}) = \deg F_1 - 6.$$

Thus, equation (10.1), in this case ($p = 3$ and $g = 2$), gives us

$$\mathrm{ht}(\boldsymbol{\phi}) = 2 \deg F_1 - 15.$$

Remember that for us a Mochizuki lift has height less than or equal to $(1 - g) = -1$, and in this case this implies that $\deg F_1 \leq 7$. Hence by Theorem 2.4, it determines an absolute minimal degree lifting, which proves item 1 of Theorem 2.8.

Theorem 2.4 also tells us that if $\deg F_1 = 7$ then the coefficient of x_0^2 in $f(x_0)$, say A, is non-zero. If we assume that k is algebraically closed (or work on some finite extension of k) we may assume that $A = 1$, and so we will consider f given by equations of the form

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

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, using the fact the k is algebraically closed, or extending k), allows us to consider f given by

$$f(x_0)=x_0^6+a_0x_0^4+x_0^2+b_0x_0+c_0,$$

which proves all but the last sentence of item 2 of 2.8. The last sentence follows from Corollary 3.8 on pg. 1048 of [Moc96], which implies that curves whose moduli are sufficiently general admit Mochizuki lifts.

Now, let C be given by an equation of the form

$$y_0^2=f(x_0)=x_0^6+a_0x_0^4+x_0^2+b_0x_0+c_0.$$

We want to compute a Mochizuki lift of such curve. But as remarked above, this has to have $\deg F_1=7$ and hence is an absolute minimal degree lift, and thus Theorem 2.4 gives the a formula for the derivative of F_1. Using an algorithm similar to the one described in section 6 of [Fin02], we obtain an absolute minimal degree curve

$$\boldsymbol{C}/\boldsymbol{W}_2(k)\,:\,\boldsymbol{y}^2=\boldsymbol{x}^6+\boldsymbol{a}\boldsymbol{x}^4+\boldsymbol{x}^2+\boldsymbol{b}\boldsymbol{x}+\boldsymbol{c},$$

and an absolute minimal degree lift $\nu(x_0,y_0)=((x_0,F_1),(y_0,y_0H_1))$. If $a_0\neq 0$ (the case when the curve is not Mochizuki-ordinary, as we shall see in the next section), we obtain

$$\begin{aligned}F_1=x_0^7+\frac{b_0}{a_0^2}\,x_0^6+2\,a_0\,x_0^5+&\\
&\frac{a_0^4\,c_0^2+2\,a_0^4+2\,a_0^3\,b_0^2+2\,a_0^3\,c_0+2\,a_0^2\,b_0^2\,c_0+2\,a_0^2\,c_0^2+a_0^2+b_0^4}{a_0^2}\,x_0^3\\
&\qquad+2\,b_0\,x_0^2+c_0\,x_0+\frac{a_0^4\,b_0+2\,a_0^3\,b_0\,c_0+a_0^2\,b_0+b_0}{a_0^5}\end{aligned}$$

$$H_1=(2\,a_0^3+a_0)\,x_0^4+2\,a_0\,b_0\,x_0^3+(2\,a_0^2+1)\,x_0^2+(2\,a_0^2\,b_0+b_0)\,x_0+2\,a_0^2\,c_0+b_0^2$$

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

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

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

For $a_0=0$ we have:

$$F_1=x_0^7+2\,b_0\,x_0^6+(2\,b_0^4+2\,b_0^2\,c_0+2\,c_0^2+1)\,x_0^3+2\,b_0\,x_0^2+c_0\,x_0$$

$$H_1=x_0^2+b_0\,x_0+b_0^2$$

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

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

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

Since we could obtain $\deg F_1 = 7$, Proposition 4.10 on pg. 1117 of [Moc96] tells us that we indeed computed a Mochizuki lift. (Note that Theorem 4.1 allows us to explicitly compute the lift of the Frobenius.) Hence we proved all but the last sentence of item 3 of Theorem 2.8, which we prove in the next section.

One can now proceed to compute a minimal degree lifting modulo 27. (Note we do not have an analogue to Proposition 4.10 on pg. 1117 of [Moc96] modulo p^3.) We again can achieve the lower bound given by Theorem 2.4, namely $\deg F_2 = 25$. So, Theorem 9.2 tells us that *there exists a lift of the Frobenius* also modulo 27. The formulas for F_2, H_2, $\boldsymbol{P}$ and $\boldsymbol{Q}$ (the latter two as in the statement of Proposition 2.7) are too long to be given here, but can be easily computed with the help of a computer using the analogue to the modified algorithm for elliptic curves described in the end of section 6 of [Fin02] and Proposition 2.7.

11. Ordinariness

We finally prove the last sentence of item 3 in Theorem 2.8, namely that given a curve

$$C/k \ : \ y_0^2 = x_0^6 + a_0 x_0^4 + x_0^2 + b_0 x_0 + c_0, \tag{11.1}$$

where k is a perfect field of characteristic 3, then its Mochizuki lift being Mochizuki-ordinary (or *hyperbolic-ordinary*, as Mochizuki refers to it in [Moc96]), and its Jacobian being an ordinary Abelian variety, are both equivalent to a_0 being non-zero. Usually, when one simply says that C is *ordinary*, we understand that its Jacobian is ordinary. (Mochizuki refers to this usual notion of ordinariness as *parabolic-ordinariness.*) It is not true in general that these two notions are the same, as happens in this particular case.

We first show that $a_0 \neq 0$ if, and only if, then the Jacobian of C is an ordinary Abelian variety. We recall that the Jacobian of C is ordinary if, and only if, the restriction of the Cartier operator to global differentials on the curve

$$\mathcal{C}|_{\Gamma(C,\Omega_{C/k})} : \Gamma(C, \Omega_{C/k}) \to \Gamma(C, \Omega_{C/k})$$

is surjective. Let $\omega_0 \stackrel{\text{def}}{=} dx_0/y_0$ and $\omega_1 \stackrel{\text{def}}{=} x_0\, \omega_0$. One has

$$\begin{aligned} \mathcal{C}(\omega_1) &= a_0^{1/3}\omega_1 + b_0^{1/3}\omega_0, \\ \mathcal{C}(\omega_0) &= \omega_0, \end{aligned}$$

and so, $\mathcal{C}|_{\Gamma(C,\Omega_{C/k})}$ is surjective if, and only if, $a_0 \neq 0$.

We now briefly recall what it means to say that a Mochizuki lift of C is Mochizuki-ordinary. Let $T_{C^\sigma/k}$ and $T_{C/k}$ denote the relative tangent bundles of C^σ/k and C/k respectively, and let

$$H_{\mathcal{E}} : \phi^*(T_{C^\sigma/k}) \to T_{C/k}$$

be the *square Hasse invariant* of an indigenous bundle $(\mathcal{E}, \nabla_{\mathcal{E}})$ ([Moc96], Proposition 2.6(1), pg. 1032).

Dualizing $H_{\mathcal{E}}$ yields

$$H_{\mathcal{E}}^{\vee} : \Omega_{C/k} \to \phi^*(\Omega_{C^\sigma/k}) \cong \Omega_{C/k}^{\otimes 3}.$$

Tensoring with $\Omega_{C/k}$ gives a map

$$\mathrm{id} \otimes H_{\mathcal{E}}^{\vee} : \Omega_{C/k}^{\otimes 2} \to \Omega_{C/k} \otimes \phi^*(\Omega_{C^\sigma/k}),$$

and now pushing forward by ϕ yields

$$\phi_*(\mathrm{id} \otimes H_{\mathcal{E}}^{\vee}) : \phi_*(\Omega_{C/k}^{\otimes 2}) \to \phi_*(\Omega_{C/k}) \otimes \Omega_{C^\sigma/k}. \tag{11.2}$$

Next we recall that there is a *Cartier isomorphism* (see [Kat70])

$$\tilde{\mathcal{C}} : H^1(\phi_* \Omega_{C/k}^{\bullet}) \to \Omega_{C^\sigma/k},$$

related to the Cartier operator $\mathcal{C}$ as follows: if we also denote by $\tilde{\mathcal{C}}$ the map between $\phi_*(\Omega_{C/k})$ and $\Omega_{C^\sigma/k}$ (having the exact differentials as its kernel) that induces $\tilde{\mathcal{C}} : H^1(\phi_*\Omega_{C/k}^{\bullet}) \to \Omega_{C^\sigma/k}$, then for all $\omega \in \Gamma(C, \phi_*(\Omega_{C/k}))$ one has $\tilde{\mathcal{C}}(\omega) = \mathcal{C}(\omega)^\sigma$. The Cartier isomorphism induces a map

$$\tilde{\mathcal{C}} \otimes \mathrm{id} : \phi_*(\Omega_{C/k}) \otimes \Omega_{C^\sigma/k} \to \Omega_{C^\sigma/k}^{\otimes 2} \tag{11.3}$$

The composition of the maps given by equations (11.2) and (11.3) induces a map on global sections

$$\mathcal{V} : \Gamma(C, \Omega_{C/k}^{\otimes 2}) \to \Gamma(C^\sigma, \Omega_{C^\sigma/k}^{\otimes 2}),$$

called the *Verschiebung*. (This is the analogue of the map $\Phi_{\mathcal{E}}^{\omega}$ on pg. 1037 of [Moc96].) Now, by Definition 3.1 on pg. 1044 and Proposition 2.12 on pg. 1037 of [Moc96], the curve the Mochizuki lift of C/k is Mochizuki-ordinary if $\mathcal{V}$ is surjective.

We now prove that if C/k is given by (11.1), then $\mathcal{V}$ is surjective if, and only if, $a_0 \neq 0$. This proof was also outlined by the referee (and was further clarified to the author by S. Mochizuki).

To understand $\mathcal{V}$, we first look at the square Hasse invariant $H_{\mathcal{E}}$. This map (and its dual) is determined by the "multiplication" by a quadratic differential θ_0 on C/k. By Proposition 2.6 on pg. 1032 of [Moc96], the divisor of zeros of such a quadratic differential is the *double supersingular locus* of C/k, i.e., its support is the set of points where the lift of the Frobenius is not defined. In our case, these points are the points at infinity, and hence θ_0 has to be a non-zero constant multiple of ω_0^2, and we can assume that $\theta_0 = \omega_0^2$. Hence,

$$H_{\mathcal{E}}^{\vee}((\lambda_1 x_0 + \lambda_0)\omega_0) = (\lambda_1 x_0 + \lambda_0)\omega_0^\sigma \approx (\lambda_1 x_0 + \lambda_0)\omega_0^3, \tag{11.4}$$

where "$\approx$" is the identification via the isomorphism between $\phi^*(\Omega_{C^\sigma/k})$ and $\Omega_{C/k}^{\otimes 3}$.

Let $\theta_1 \stackrel{\text{def}}{=} x_0\,\theta_0$ and $\theta_2 \stackrel{\text{def}}{=} x_0^2\,\theta_0$. Then, equation (11.4) implies that the map induced by (11.2) on global sections is given by

$$\lambda_2\theta_2 + \lambda_1\theta_1 + \lambda_0\theta_0 \mapsto (\lambda_2 x_0^2 + \lambda_1 x_0 + \lambda_0)\omega_0 \otimes \omega_0^\sigma.$$

Hence

$$\mathcal{V}(\lambda_2\theta_2 + \lambda_1\theta_1 + \lambda_0\theta_0) = \tilde{\mathcal{C}}((\lambda_2 x_0^2 + \lambda_1 x_0 + \lambda_0)\omega_0) \otimes \omega_0^\sigma.$$

Therefore,

$$\begin{aligned}\mathcal{V}(\theta_0) &= \theta_0^\sigma,\\ \mathcal{V}(\theta_1) &= a_0\theta_1^\sigma + b_0\theta_0^\sigma,\\ \mathcal{V}(\theta_2) &= \theta_2^\sigma + c_0\theta_0^\sigma,\end{aligned}$$

which clearly is surjective if, and only if, $a_0 \neq 0$.

This shows that the two notions of ordinariness are the same in the present situation and finishes the proof of Theorem 2.8.

Acknowledgement. The author would like to thank J. F. Voloch, J. Tate and S. Mochizuki for most valuable discussions and A. Agboola for his insightful comments. Also, the referee's comments were of great importance to the connections with Mochizuki's theory. The author acknowledges the use of the packages Magma and Mathematica in computations mentioned in the text. Finally, part of this work was done with the financial support from CAPES (Brazil).

References

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

[Deu41] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[Fin01] L. R. A. Finotti. *Canonical and Minimal Degree Liftings of Curves*. PhD thesis, University of Texas at Austin, 2001.

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

[Kat70] N. M. Katz. Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin. *Inst. Hautes Études Sci. Publ. Math.*, (39):175–232, 1970.

[LST64] J. Lubin, J-P. Serre, and J. Tate. Elliptic curves and formal groups. *Proc. of Woods Hole summer institute in algebraic geometry*, 1964. Unpublished. Available at http://www.ma.utexas.edu/users/voloch/lst.html.

[Moc96] S. Mochizuki. A theory of ordinary p-adic curves. *Publ. Res. Inst. Math. Sci.*, 32:957–1152, 1996.

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

[Ray83] M. Raynaud. Around the Mordell conjecture for function fields and a conjecture of Serge Lang. *Lecture Notes in Math.*, 1016:1–19, 1983.

[Sat00] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

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

[Tat02] J. Tate. On a conjecture of Finotti. *Bull. Braz. Math. Soc. (N.S.)*, 33(2):225–229, 2002.

[Vol97] J. F. Voloch. Torsion points of $y^2 = x^6 + 1$. *unpublished manuscript*, 1997. available at http://www.ma.utexas.edu/users/voloch/oldpreprint.html.

[VW99] J. F. Voloch and J. L. Walker. Codes over rings from curves of higher genus. *IEEE Trans. Inform. Theory*, 45:1768–1776, 1999.

[VW00] J. F. Voloch and J. L. Walker. Euclidean weights of codes from elliptic curves over rings. *Trans. Amer. Math. Soc.*, 352(11):5063–5076, 2000.

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

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