MINIMAL DEGREE LIFTINGS IN CHARACTERISTIC 2

LUÍS R. A. FINOTTI

ABSTRACT. In this paper we analyze liftings of hyperelliptic curves over perfect fields in characteristic 2 to curves over rings of Witt vectors. This theory can be applied to construct error-correcting codes, and lifts of points with minimal degrees are likely to yield the best codes, and these are the main focus of the paper. We find upper and lower bounds for their degrees, give conditions to achieve the lower bounds and analyze the existence of lifts of the Frobenius. Finally, we exhibit explicit computations for genus 2 and show codes obtained using this theory.

1. INTRODUCTION

In this paper we analyze liftings of hyperelliptic curves over perfect fields of characteristic 2 to curves over rings of Witt vectors (characteristic 0). As we shall discuss later, these liftings can be used to construct error-correcting codes, and we will focus on particular kinds of liftings that are likely to yield good codes. For reasons that will become quite clear later on, we shall refer to those particular liftings as *minimal degree liftings*.

The case of characteristic $p > 2$ was dealt with in [Fin04], and we shall prove here similar results for $p = 2$. We observe that for concrete applications to coding theory, this case is especially important, since we can obtain *binary* codes, which can be effectively implemented.

As with the case $p > 2$, these minimal degree liftings are also of independent interest, and although we shall keep their applications to coding theory in mind, we will not restrict ourselves only to results that are relevant to this particular aspect. We shall also study, for instance, liftings of the Frobenius and the relations of minimal degree liftings with canonical liftings.

This paper is organized as follows: in section 2 we give a brief introduction to algebraic geometric codes over rings, which was first introduced by Walker in [Wal99]. Our goal in this session is to only give a rough idea of how such codes are obtained and to motivate the introduction of minimal degree liftings.

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

Key words and phrases. hyperelliptic curves, canonical liftings, minimal degree liftings, algebraic geometric codes over rings.

In section 3 we introduce some definitions and notation that will be used throughout this paper and in section 4 we give a precise definition of minimal degree liftings.

In section 5 we discuss liftings of the Frobenius and define the notion of a lift of the Frobenius associated to a lift of points.

With the background established by the previous sections, we are able to state in section 6 the main results of this paper, while leaving the proofs to the later sections.

In section 7 we prove some technical results about Witt vectors and valuations which are then used in the proofs of the main theorems.

Sections 8 and 9 contain the proofs of the upper and lower bounds, respectively, for the degrees of the minimal degree liftings, while section 10 has the proofs of the statements about achieving degrees exactly equal to the lower bounds.

Section 11 contains the proofs of the main results about lifting the Frobenius map to characteristic zero. In particular, it proves that minimal degree liftings satisfying the established lower bounds always have a lift of the Frobenius modulo 8 associated to the corresponding lift of points.

In section 12, we exhibit explicit examples of lifts (modulo 16) of hyperelliptic curves of genus 2 whose degrees are equal to the lower bounds.

Finally, section 13 contains examples of error-correcting codes.

2. Algebraic Geometric Codes over Rings

In this section we follow sections 2 and 3 of [VW00], adapting the notation and some results to the particular cases in which we are interested here.

Let k be a finite field of characteristic p (not necessarily equal to 2) and $\boldsymbol{W}_l(k)$ be the *ring of Witt vectors of length l over k*. Also, let $\boldsymbol{C}/\boldsymbol{W}_l(k)$ be a projective curve with good reduction modulo p, C/k be its reduction modulo p, $\mathcal{P} \stackrel{\text{def}}{=} \{\boldsymbol{P}_1, \ldots, \boldsymbol{P}_n\}$ be a set of $\boldsymbol{W}_l(k)$-rational points of $\boldsymbol{C}$ with distinct reductions modulo p, say $\{P_1, \ldots, P_n\}$, D be a Cartier divisor of $\boldsymbol{C}$ such that no $\boldsymbol{P}_i$ is in the support of D, and $\mathcal{L} \stackrel{\text{def}}{=} \mathcal{L}(D)$ be the sheaf associated to D (as in section II.6 of [Har77]). Observe that one can think of $\mathcal{L}$ as a set of functions on $\boldsymbol{C}$ which are regular on the support of D.

Definition 2.1. Let $\boldsymbol{C}$, $\mathcal{P}$ and $\mathcal{L}$ be as above. We define the *algebraic geometric code over $\boldsymbol{W}_l(k)$ associated to $\boldsymbol{C}$, $\mathcal{P}$ and $\mathcal{L}$*, denoted by $\mathcal{C}_{\boldsymbol{W}_l(k)}(\boldsymbol{C}, \mathcal{P}, \mathcal{L})$, as

$$\mathcal{C}_{\boldsymbol{W}_l(k)}(\boldsymbol{C}, \mathcal{P}, \mathcal{L}) \stackrel{\text{def}}{=} \{(\boldsymbol{f}(\boldsymbol{P}_1), \ldots, (\boldsymbol{f}(\boldsymbol{P}_n)) \;:\; \boldsymbol{f} \in \mathcal{L}\} \subset (\boldsymbol{W}_l(k))^n.$$

The next theorem summarizes some of the main results of [Wal99]:

Theorem 2.2 (Walker)**.** *Let $\boldsymbol{C}$, $\mathcal{P} \stackrel{\text{def}}{=} \{\boldsymbol{P}_1, \ldots, \boldsymbol{P}_n\}$, D, $\mathcal{L}$ and $\mathcal{C} \stackrel{\text{def}}{=} \mathcal{C}_{\boldsymbol{W}_l(k)}(\boldsymbol{C}, \mathcal{P}, \mathcal{L})$ be as above and let g denote the genus of the curve $\boldsymbol{C}$. If $(2g-2) < \deg D < n$, then $\mathcal{C}$ is a linear* *code over $\boldsymbol{W}_l(k)$ which is free as a $\boldsymbol{W}_l(k)$-module. Moreover, $\mathcal{C}$ has rank* $\deg D + 1 - g$ *and minimum Hamming distance at least* $n - \deg D$.

We are particularly interested in codes over $\mathbb{Z}/p^l\mathbb{Z}$, where p is a prime. If $k = \mathbb{F}_p$, the field of p elements, then $\boldsymbol{W}_l(k) \cong \mathbb{Z}/p^l\mathbb{Z}$, and the algebraic geometric codes above are then codes over $\mathbb{Z}/p^l\mathbb{Z}$. On the other hand, if k is a finite field of characteristic p, but $k \neq \mathbb{F}_p$, one can apply the *trace* $\mathrm{tr} : \boldsymbol{W}_l(k) \to \boldsymbol{W}_l(\mathbb{F}_p)$ to each coordinate of all codewords to obtain codes over $\mathbb{Z}/p^l\mathbb{Z}$

When $p = 2$ we can obtain non-linear *binary* codes from codes over $\mathbb{Z}/2^l\mathbb{Z}$ by using the *generalized Gray map*, defined by Carlet in [Car98], which is a map $G : (\mathbb{Z}/2^l\mathbb{Z}) \to \mathbb{F}_2^{2^{l-1}}$ such that the Hamming weight of $G(x - y)$ is equal to the Hamming distance between $G(x)$ and $G(y)$, i.e., G is *distance preserving*. The binary codes are obtained by applying G coordinatewise to the codewords of the $\mathbb{Z}/2^l\mathbb{Z}$-codes.

Since we are mainly interested in these binary codes, whenever $l = 2$ (and $p = 2$) the *Lee weight* for the codes over $\mathbb{Z}/4\mathbb{Z}$ is of interest, instead of the the Hamming weight, since in this case the Lee weight of a codeword over $\mathbb{Z}/4\mathbb{Z}$ is equal to the Hamming weight of the image of this codeword under the generalized Gray map applied coordinatewise. (Observe that for $l = 2$, G is equal to the original *Gray map*, defined by $G(0) = (0, 0)$, $G(1) = (0, 1)$, $G(2) = (1, 1)$ and $G(3) = (1, 0)$.)

A computation (see [VW00]) shows that if $\vec{x} = (x_1, \dots, x_n)$ is a codeword of length n over $\mathbb{Z}/4\mathbb{Z}$, then the Lee weight of $\vec{x}$, denoted by $w_L(\vec{x})$, satisfies

$$w_L(\vec{x}) \geq n - \left| \sum_{j=1}^{n} e^{2\pi i x_j/4} \right|. \tag{2.1}$$

Hence, to find lower bounds to the minimum Lee weight of a code over $\mathbb{Z}/4\mathbb{Z}$, it suffices to find an upper bound for the exponential sum above, and thus, in the case of algebraic geometric codes (with $l = 2$), where the codewords are of the form $(\mathrm{tr}(\boldsymbol{f}(\boldsymbol{P}_1), \dots, \mathrm{tr}(\boldsymbol{f}(\boldsymbol{P}_n))$, with $\boldsymbol{f} \in \mathcal{L}$ and $\mathcal{P} = \{\boldsymbol{P}_1, \dots, \boldsymbol{P}_n\}$, we need to find upper bounds for the absolute value of the exponential sums

$$S_{\boldsymbol{f}} \stackrel{\text{def}}{=} \sum_{j=1}^{n} e^{2\pi i \, \mathrm{tr}(\boldsymbol{f}(\boldsymbol{P}_j))/4},$$

for $\boldsymbol{f} \in \mathcal{L}$.

In fact, more generally, if $p^l \neq 4$, one can use *Euclidean weights* instead of the Lee weight: given $x \in \mathbb{Z}/p^l\mathbb{Z}$, the Euclidean weight of x is given by

$$w_E(x) \stackrel{\text{def}}{=} \sqrt{2 - 2\cos\left(\frac{2\pi x}{p^l}\right)},$$

and if $\vec{x} = (x_1, \dots, x_n)$, then

$$w_E^2(\vec{x}) \stackrel{\text{def}}{=} \sum_{j=1}^{n} w_E^2(x_j).$$

When $p^l = 4$, ones has that $w_L(x) = 1/2\, w_E^2(x)$. But, in general, we have that

$$w_E^2(\vec{x}) \geq 2n - 2 \left| \sum_{j=1}^{n} e^{2\pi i x_j / p^l} \right|,$$

and if $\vec{x}$ is a codeword of the form $(\mathrm{tr}(\boldsymbol{f}(\boldsymbol{P}_1), \dots, \mathrm{tr}(\boldsymbol{f}(\boldsymbol{P}_n))$, as above, but with arbitrary p and l, then to find a lower bound to the Euclidean weight of the code, it suffices to find an upper bound for the absolute value of

$$S_{\boldsymbol{f}} \stackrel{\text{def}}{=} \sum_{j=1}^{n} e^{2\pi i \, \mathrm{tr}(\boldsymbol{f}(\boldsymbol{P}_j))/p^l}, \tag{2.2}$$

for $\boldsymbol{f} \in \mathcal{L}$.

Let then k be a finite field of characteristic p, C/k and $\boldsymbol{C}/\boldsymbol{W}_l(k)$ be curves as before and U and $\boldsymbol{U}$ be open subsets of C and $\boldsymbol{C}$, respectively, such that U is the reduction modulo p of $\boldsymbol{U}$. Also, let ν be a *lift of points* on U, i.e., a map $\nu : U(\bar{k}) \to \boldsymbol{U}(\boldsymbol{W}_l(\bar{k}))$ that is a section of the reduction modulo p. So, if $\nu(P) = \boldsymbol{P}$ and $\boldsymbol{f}$ is a function regular in $\boldsymbol{P}$, then $\boldsymbol{f}(\boldsymbol{P}) = \boldsymbol{f} \circ \nu(P)$, and $\boldsymbol{f} \circ \nu = (f_0, f_1, \dots, f_{l-1})$, where each $f_i \in k(C)$, for $i = 0, \dots, l-1$, and $k(C)$ denotes the function field of C. Since $\boldsymbol{f}$ is regular at $\boldsymbol{P}$, all the f_i's are regular at P.

So, fix a function $\boldsymbol{f}$ and let

$$\mathcal{P} = \{\boldsymbol{P}_1, \dots, \boldsymbol{P}_n\} = \{\nu(P) : P \in U(k) \text{ and } \boldsymbol{f} \text{ is regular at } \nu(P)\}. \tag{2.3}$$

In this situation, Voloch and Walker found an upper bound for the exponential sum (2.2), more precisely, Theorem 3.1 of [VW00] states:

Theorem 2.3 (Voloch-Walker)**.** *Let $k = \mathbb{F}_q$ be the field of q elements with characteristic p, $\boldsymbol{f}$ be a function on the curve $\boldsymbol{C}/\boldsymbol{W}_l(k)$ and $\mathcal{P}$ be as in equation* (2.3)*. Let also $\{Q_1, \dots, Q_s\}$ be the set of poles (in $C(\bar{k})$) of the coordinates of $\boldsymbol{f} \circ \nu$, and v_{Q_i} be the valuation of $k(C)$ given by the order of vanishing at Q_i. Finally, let g be the genus of the curve C and assume that $\boldsymbol{f} \circ \nu$ is not of the form $\sigma(\boldsymbol{g}) - \boldsymbol{g} + \boldsymbol{c}$ for any $\boldsymbol{g} \in \boldsymbol{W}_l(k(C))$ and $\boldsymbol{c} \in \boldsymbol{W}_l(k)$, where $\sigma(g_0, \dots, g_l) \stackrel{\text{def}}{=} (g_0^p, \dots, g_l^p)$. Then*

$$|S_{\boldsymbol{f}}| \leq \left(2g - 1 + \sum_{j=1}^{s} \max_{0 \leq i \leq (l-1)} \{-p^{l-1-i}\, v_{Q_j}(f_i)\} \, [k(Q_j) : k] \right) q^{1/2}, \tag{2.4}$$

where $k(Q_j)$ is the minimal field of definition of Q_j.

Hence to have a larger bound for the Euclidean weight of the algebraic geometric codes over $\mathbb{Z}/p^l\mathbb{Z}$, and hence larger Lee weight when $p^l = 4$, we need to have a smaller value for $|S_{\boldsymbol{f}}|$, and thus we want the coordinate functions of $\boldsymbol{f} \circ \nu$ to have *small order of poles* at the Q_i's, and in order to have the best possible bounds, we look for lifts of points ν that yield minimal order of poles. This will be the motivation for our definition of *minimal degree liftings*.

3. Conventions and Definitions

Before we state the main results, we need to establish some notation and review a few previous results.

Throughout this paper, k will be a perfect field of characteristic 2. (For the applications to coding theory k will be a finite field, but the theoretical results hold in the more general case of perfect fields.) Also let

$$C/k \;:\; y_0^2 + g(x_0)\, y_0 = f(x_0), \tag{3.1}$$

be a (non-singular and projective) hyperelliptic curve over k, where $f(x_0)$ is a monic polynomial of *odd* degree (as a polynomial in x_0), which we shall denote by d, and $g(x_0)$ has degree (as a polynomial in x_0) less than or equal to $(d-1)/2$. Therefore, C has genus $(d-1)/2$, there is only one point at infinity, which we shall denote by P_∞, and the polynomials $g(x_0)$ and $(f'(x_0) + g'(x_0)\, y_0)$ have no common zeros on C (since C is non-singular).

Let ω denote the holomorphic differential

$$\omega \stackrel{\text{def}}{=} \frac{dy_0}{f'(x_0) + g'(x_0)\, y_0} = \frac{dx_0}{g(x_0)} \tag{3.2}$$

which has no zeros at the affine part of C and a zero of order $(2d-2)-(d+1) = (d-3)$ at P_∞.

Also observe that, by the Riemann-Roch Theorem, or more precisely, by [Sil85] Corollary II.5.5(b), every hyperelliptic curve over k of genus $(d-1)/2$, for any odd number d, can be put in that form.

Also, let

$$\boldsymbol{C}/\boldsymbol{W}(k) \;:\; \boldsymbol{y}^2 + \boldsymbol{g}(\boldsymbol{x})\, \boldsymbol{y} = \boldsymbol{f}(\boldsymbol{x}) \tag{3.3}$$

be a hyperelliptic curve over the ring of Witt vectors $\boldsymbol{W}(k)$, where $\boldsymbol{f}$ is a monic polynomial of degree d (i.e., same degree as f), the degree of $\boldsymbol{g}$ is less than or equal to $(d-1)/2$, and such that the reductions of $\boldsymbol{f}$ and $\boldsymbol{g}$ modulo 2 are f and g respectively (i.e, C is the reduction modulo 2 of $\boldsymbol{C}$).

Note that since C is non-singular, $\boldsymbol{C}$ is also non-singular, and so $2\boldsymbol{y} + \boldsymbol{g}(\boldsymbol{x})$ and $\boldsymbol{f}'(\boldsymbol{x}) - \boldsymbol{g}'(\boldsymbol{x})\, \boldsymbol{y}$ have no common zeros on $\boldsymbol{C}$. And, similarly as done with C, let $\boldsymbol{P}_\infty$ denote the point at infinity of $\boldsymbol{C}$ and let $\boldsymbol{\omega}$ denote the holomorphic differential

$$\boldsymbol{\omega} \stackrel{\text{def}}{=} \frac{d\boldsymbol{y}}{\boldsymbol{f}'(\boldsymbol{x}) - \boldsymbol{g}'(\boldsymbol{x})\,\boldsymbol{y}} = \frac{d\boldsymbol{x}}{2\boldsymbol{y} + \boldsymbol{g}(\boldsymbol{x})}.$$

We shall often identify $\boldsymbol{C}$ with its *Greenberg transform* $G(\boldsymbol{C})$, which is an infinite dimensional scheme over k, defined in the following manner: writing $\boldsymbol{x} = (x_0, x_1, \dots)$ and $\boldsymbol{y} = (y_0, y_1, \dots)$, where the x_i's and y_i's are variables, one can expand both sides of equation (3.3) using the addition and multiplication of Witt vectors. The equations (on the x_i's and y_i's) obtained by comparing the coordinates of the Witt vectors in both sides of this expansion are the equations that define $G(\boldsymbol{C})$.

As mentioned in section 2, in our construction of codes we shall use lifts of points between open sets of C and $\boldsymbol{C}$. For us these open sets will always be the *affine parts* of C and $\boldsymbol{C}$. So, let U and $\boldsymbol{U}$ denote the affine parts of C and $\boldsymbol{C}$ respectively. We then define:

Definition 3.1. A *lift of points* from C/k to $\boldsymbol{C}/\boldsymbol{W}(k)$ is a regular map

$$\nu : U(\bar{k}) \to \boldsymbol{U}(\boldsymbol{W}(\bar{k})) \approx G(\boldsymbol{U})(\bar{k})$$

which is a section of the reduction modulo 2. (Hence, in this paper, we consider lifts of points between the *affine* parts only.)

In terms of the Greenberg transform, a lift of points

$$\nu : U(\bar{k}) \to \boldsymbol{U}(\boldsymbol{W}(\bar{k}))$$

can be written as

$$\nu(x_0, y_0) = (x_0, F_1(x_0, y_0), F_2(x_0, y_0), \dots, y_0, G_1(x_0, y_0), G_2(x_0, y_0), \dots), \tag{3.4}$$

where, since this map cannot have any poles in the affine part of C, we have in fact that $F_i, G_i \in k[x_0, y_0]$. Also, we will write $F_0 \stackrel{\text{def}}{=} x_0$ and $G_0 \stackrel{\text{def}}{=} y_0$.

Remember that we are after lifts ν that will yield minimal order of poles for the coordinates of compositions of ν with functions in $\boldsymbol{C}$. In our applications our divisor D (as in section 2) will be a positive multiple of $\boldsymbol{P}_\infty$, and hence the functions in $\mathcal{L}(D)$ are polynomials in $\boldsymbol{W}(k)[\boldsymbol{x}, \boldsymbol{y}]$. Therefore, to have the best lower bound for the minimum Euclidean (or Lee weight, if $p^l = 4$), we need to have lifts ν such that the coordinate functions of

$$\boldsymbol{x} \circ \nu = (x_0, F_1, F_2, \dots)$$

and

$$\boldsymbol{y} \circ \nu = (y_0, G_1, G_2, \dots)$$

have minimal order of poles at P_∞.

Observe that in both [Fin02] and [Fin04] we referred to "degrees" as degrees as polynomials in x_0. To say that the F_i's and G_i's have minimal degrees as polynomials is the same as to say that these functions have minimal order of poles at P_∞. This was convenient in those papers since we mostly dealt with polynomials in a single variable, namely with $k[x_0]$. The case of characteristic 2 is rather different and we will have to deal with polynomials in two variables, and so we will adopt a different convention here.

Definition 3.2. Let h be a function in the $k(C)$. Then the *degree* of h, denoted by $\deg h$, is defined as the number of poles of h counted with multiplicity. (Note that this is the same as to define $\deg h \stackrel{\text{def}}{=} [k(C) : k(h)]$, by [Sil85] Proposition II.2.6(a).)

Hence, $\deg x_0 = 2$ and $\deg y_0 = d$. Whenever we need to refer to the degree of some function as a polynomial, we shall explicitly say so.

So our goal is to obtain lifts of points ν whose coordinate functions F_i's and G_i's have minimal degrees.

4. Minimal Degree Liftings

As in [Fin04], we have a few different choices when dealing with minimal degree liftings. First, one can choose which coordinate is to have its degrees minimized, i.e., one can either minimize the degrees of the F_i's (as in equation (3.4)) or of the G_i's. In general, one cannot minimize both at the same time. Secondly, one can either assume that the curves C and $\boldsymbol{C}$ are fixed a priori, and then find lifts of points between (the affine parts of) *those* curves with minimal possible degrees (for the chosen coordinate), or we can assume that only C is fixed, and then find a lift $\boldsymbol{C}$ of C which has a lift of points with minimal degrees (for the chosen coordinate) among all lifts of points from C to any other lift $\tilde{\boldsymbol{C}}$.

We will make these notions precise in the following two definitions below.

Definition 4.1. Let C and $\boldsymbol{C}$ be curves given by equations (3.1) and (3.3) respectively. A *minimal degree lifting from C to $\boldsymbol{C}/\boldsymbol{W}_2(k)$ with respect to $\boldsymbol{y}$* (resp., $\boldsymbol{x}$) is a lift of points $\nu : U(\bar{k}) \to \boldsymbol{U}(\boldsymbol{W}_2(\bar{k}))$, with

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

where $\deg G_1$ (resp., $\deg F_1$) is minimal.

Inductively, a *minimal degree lifting from C to $\boldsymbol{C}/\boldsymbol{W}_{n+1}(k)$ with respect to $\boldsymbol{y}$* (resp., $\boldsymbol{x}$) is a lift of points $\nu : U(\bar{k}) \to \boldsymbol{U}(\boldsymbol{W}_{n+1}(\bar{k}))$, with

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

where the reduction modulo 2^n is a minimal degree lifting from C to $\boldsymbol{C}/\boldsymbol{W}_n(k)$, and $\deg G_n$ (resp., $\deg F_n$) is minimal.

Definition 4.2. Let C be a hyperelliptic curve given by (3.1). An *absolute minimal degree curve modulo* 4 *over* C *with respect to* $\boldsymbol{y}$ is a curve $\boldsymbol{C}/\boldsymbol{W}_2(k)$ (given by (3.3)) which reduces to C modulo 2, and which satisfies the following property. Let

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

be a minimal degree lifting from C to $\boldsymbol{C}$ with respect to $\boldsymbol{y}$, and let $\tilde{\boldsymbol{C}}/\boldsymbol{W}_2(k)$ be any curve that reduces to C modulo 2. Then for any minimal degree lifting with respect to $\boldsymbol{y}$

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

from C to $\tilde{\boldsymbol{C}}$, we have $\deg \tilde{G}_1 \geq \deg G_1$.

Inductively, an *absolute minimal degree curve modulo* 2^{n+1} *over* C *with respect to* $\boldsymbol{y}$ is a curve $\boldsymbol{C}/\boldsymbol{W}_{n+1}(k)$ whose reduction modulo 2^n is an absolute minimal degree curve modulo 2^n over C with respect to $\boldsymbol{y}$, satisfying the following property. Let

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

be a minimal degree lifting with respect to $\boldsymbol{y}$ from C to $\boldsymbol{C}$, and let $\tilde{\boldsymbol{C}}/\boldsymbol{W}_{n+1}(k)$ be any curve whose reduction modulo 2^n is equal to the reduction modulo 2^n of $\boldsymbol{C}$. Then, for a minimal degree lifting with respect to $\boldsymbol{y}$

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

from C to $\tilde{\boldsymbol{C}}$, we have $\deg \tilde{G}_n \geq \deg G_n$. In this case we call the minimal degree lift ν from C to $\boldsymbol{C}$ an *absolute minimal degree lift (of points) with respect to* $\boldsymbol{y}$ (modulo 2^{n+1}).

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

In contrast with the case of $p > 2$, where liftings with respect to $\boldsymbol{x}$ and $\boldsymbol{y}$ had very similar properties, here these two liftings are quite different. One will notice that the lifting with respect to $\boldsymbol{y}$ in this case has properties very similar to the properties we have when $p > 2$, but for the $\boldsymbol{x}$ coordinates, the cases $p = 2$ and $p > 2$ are quite different.

One of the author's first motivations to deal with minimal degree liftings was to try to lower the degrees of the *elliptic Teichmüller lift*, which is a special lift of points in the case of ordinary elliptic curves (i.e., genus 1 or $d = 3$), which we shall now briefly describe.

Let k be a perfect field of characteristic $p > 0$. (We do not assume that $p = 2$ for this part.) 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 $\boldsymbol{W}(k)$, called the *canonical lifting* of E, and a map $\tau : E(\bar{k}) \to \boldsymbol{E}(\boldsymbol{W}(\bar{k}))$ (not only between the affine parts, but for the whole projective curves), 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 lifting of E^σ (the elliptic curve obtained by applying σ to the coefficients of the equation that defines E) is $\boldsymbol{E}^\sigma$;

(3) τ is an injective group homomorphism and a section of the reduction modulo p;

(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

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

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 interesting applications, such as counting rational points in ordinary elliptic curves, as in Satoh's [Sat00], and counting torsion points of curves of genus $g \geq 2$, as in Poonen's [Poo01]. Also, one can clearly use ordinary elliptic curves and the elliptic Teichmüller lift in the construction of codes described in section 2, and, in fact, the codes constructed by Voloch and Walker in [VW00] were obtained this way.

In order to improve the bounds for the codes that would be obtained using the Teichmüller lift

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

we would need to reduce the degrees of the F_i's and G_i's. Proposition 4.2 in [VW00] states that the degrees of F_1 and G_1 cannot be improved. On the other hand, the degrees of the F_i's and G_i's for $i \geq 2$ can almost always be improved. If $p \geq 3$, then one can choose to either reduce the degrees of the F_i's *without increasing* the degrees of the G_i's, or the other way around. On the other hand, for $p = 2$, we can still reduce the degrees of the G_i's without increasing the degrees of the F_i's, but we *cannot* reduce the degrees of the F_i's without increasing the degrees of the G_i's. In fact, in this case, the degrees of the G_i's increase considerably. Hence, it seemed more natural to first consider minimal degree liftings in characteristic 2 with respect to $\boldsymbol{y}$ instead of $\boldsymbol{x}$.

5. Lifts of the Frobenius

In this section we briefly discuss lifts of the Frobenius. We probably should start by observing that the question of whether or not such lift exists is of purely theoretical interest and has no application to the explicitly construction of codes or apparent relation with how good the obtained codes are.

Let C be a hyperelliptic curve given by equation (3.1). Let, as before, σ denote the Frobenius of k (now of characteristic 2), and C^σ be the curve given by the zeros of the equation defined by applying σ to the coefficients of the equation that defines C. Then, the relative Frobenius is a morphism

$$\phi : C \to C^\sigma$$

defined by $\phi(x_0, y_0) \stackrel{\text{def}}{=} (x_0^2, y_0^2)$.

Certainly in characteristic zero one does not have a naturally defined analogue of the Frobenius map. On the other hand, we can look for liftings of C for which we have a lift of the Frobenius. More precisely, if σ denote also the Frobenius in $\boldsymbol{W}(k)$, can one find a curve $\boldsymbol{C}$, given by an equation as in (3.3) for which there is a morphism

$$\boldsymbol{\phi} : \boldsymbol{C} \to \boldsymbol{C}^\sigma,$$

such that the reduction modulo 2 gives the Frobenius of C (as in the case of ordinary elliptic curves)? In general, the answer is no. Raynaud showed in [Ray83] that curves of genus greater than one have no lift of the Frobenius. Moreover, only *ordinary* elliptic curves have lifts of the Frobenius. On the other hand, for (smooth) *affine* curves over $\boldsymbol{W}_n(k)$ with good reduction, there is *always* a lifting of the Frobenius. (Although not entirely immediate, a proof of this result in the case of plane curves can be obtained by using Lemma 8.1 and a slightly modified version of Lemma 11.1.)

As one can see from [Bui96] and [Fin04], lifts of points and lifts of the Frobenius are somewhat related. (For example, Theorem 4.1 in [Fin04] states that having a lift of points modulo p^{n+1} gives a lift of the n-th power of the Frobenius modulo p^{n+1}.) To make this connection between lifts of points and lifts of the Frobenius more precise, we introduce the following definition:

Definition 5.1. Let C/k and $\boldsymbol{C}/\boldsymbol{W}_n(k)$ be curves given by equations (3.1) and (3.3) respectively and $\nu : U(\bar{k}) \to \boldsymbol{U}(\boldsymbol{W}(\bar{k}))$ be a lift of points 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

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

commute.

Note that a lift of the Frobenius associated to a lift of points is, in principle, only a map between the *affine parts* of $\boldsymbol{C}$ and $\boldsymbol{C}^{\sigma}$. Clearly, in the case of ordinary elliptic curves, the lift of the Frobenius associated to the elliptic Teichmüller lift can be extended to the whole curve.

So, one can ask about the existence of lifts of the Frobenius that are associated to particular lifts of points. For instance, for (projective) curves of genus greater than one in characteristic $p > 2$, Mochizuki showed in [Moc96] that (in most cases) there is a lift of the Frobenius in an *open subset* of the curve associated to a lift of points which has "small" degrees. In section 12, we show that some special examples of minimal degree liftings (in characteristic 2) have lifts of the Frobenius associated to them, at least modulo 8. Also, it is worth noting that in characteristic $p > 2$ we also often have lifts of the Frobenius associated to minimal degree liftings, and for $p = 3$, the Mochizuki liftings are in fact minimal degree liftings. (See [Fin04].)

6. Statements of Main Results

In this section we state the main results of this paper, while leaving the corresponding proofs for the later sections.

This first proposition, proved in section 8, gives upper bounds for the minimal degrees of the lifts of points with respect to $\boldsymbol{y}$ in the most general situation.

Proposition 6.1. *Let C and $\boldsymbol{C}$ be as in equations* (3.1) *and* (3.3) *respectively. Then, the minimal degree lifting from C to $\boldsymbol{C}$ with respect to $\boldsymbol{y}$,*

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

satisfies

$$\deg G_1 \leq 4(d-1) + (d-2),$$
$$\deg F_1 \leq \max\{4, 2\deg g + (d-2)\},$$

and for $n \geq 2$,

$$\deg G_n \leq 2^{n+1}(d-1) + (d-2),$$
$$\deg F_n \leq 2^n \left(2 + \frac{n\,3(d-2)}{2}\right).$$

The next proposition, also proved in section 8, improves the upper bounds for the degrees of the F_n's in Proposition 6.1, by the addition of extra conditions on the degrees of F_1 and G_1, which, as we shall soon see in Proposition 6.9, are often satisfied.

Proposition 6.2. *Let C and $\boldsymbol{C}$ be as in equations* (3.1) *and* (3.3) *respectively, and assume that the minimal degree lift of points with respect to $\boldsymbol{y}$ modulo* 4 *is such that*

$$\begin{aligned}\deg G_1 &\leq 2\left(d + \frac{5(d-2)}{8}\right),\\ \deg F_1 &\leq 2\left(2 + \frac{5(d-2)}{8}\right).\end{aligned}$$

Then, the minimal degree lift of points from C to $\boldsymbol{C}$ with respect to $\boldsymbol{y}$,

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

satisfies, for $n \geq 2$,

$$\begin{aligned}\deg G_n &\leq 2^{n-1}(d-1) + (d-2),\\ \deg F_n &\leq 2^n\left(2 + \frac{n\,5(d-2)}{8}\right).\end{aligned}$$

As mentioned in section 4, if one now tries to minimize the degrees with respect to $\boldsymbol{x}$, the degrees in the $\boldsymbol{y}$ coordinate tend to increase considerably.

Although this seems to ruin the possible obtained codes, one should notice that if the Cartier divisor in question, as in section 2, is of the form $D = n\boldsymbol{P}_\infty$, with $n < d$, then the functions in $\mathcal{L}(D)$ are all powers of $\boldsymbol{x}$, and hence the G_i's are irrelevant to the code. Hence, it does make sense to consider such lifts.

Proposition 6.3. *Let C and $\boldsymbol{C}$ be as in equations* (3.1) *and* (3.3) *respectively. Then, the minimal degree lift of points from C to $\boldsymbol{C}$ with respect to $\boldsymbol{x}$,*

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

satisfies, for $n \geq 1$,

$$\begin{aligned}\deg F_n &\leq 2^n \deg g + d - 2,\\ \deg G_n &\leq 2^n(d + ne_n),\end{aligned}$$

where

$$e_n \stackrel{\text{def}}{=} \max\left\{0, \deg g + \frac{d-6}{2}\right\} + (d - \deg g)\sum_{j=1}^{n}\frac{1}{j}.$$

In the same spirit as Proposition 6.2, Proposition 6.4 improves the bounds on the degrees of the G_n's in Proposition 6.3 by adding assumptions to the degrees of F_1 and G_1, which again will often be satisfied as a consequence of Proposition 6.9.

Proposition 6.4. *Let C and $\boldsymbol{C}$ be as in equations* (3.1) *and* (3.3) *respectively, with* $\deg g \leq (3d+2)/4$*. If the minimal degree lift of points from C to $\boldsymbol{C}$ with respect to $\boldsymbol{x}$,*

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

is such that

$$\deg F_1 \leq d+2 \quad \text{and} \quad \deg G_1 \leq 3d-2,$$

then, for $n \geq 2$,

$$\begin{aligned} \deg F_n &\leq 2^n \deg g + d - 2, \\ \deg G_n &\leq 2^n (d + n e_n), \end{aligned}$$

where

$$e_n \stackrel{\text{def}}{=} \frac{d-2}{2} - (d - \deg g) + (d - \deg g) \sum_{j=1}^{n} \frac{1}{j}.$$

The next theorem gives lower bounds for the degrees of the G_n's.

Theorem 6.5. *Let C and $\boldsymbol{C}$ be as in equations* (3.1) *and* (3.3)*, and ν, as in equation* (3.4)*, be a lift of points between U and $\boldsymbol{U}$, the affine parts of C and $\boldsymbol{C}$ respectively. Assume that*

$$\deg G_i = 2^{i+1}(d-1) - (d-2)$$

for $i = 0, \dots, (n-1)$. Then,

$$\deg G_n \geq 2^{n+1}(d-1) - (d-2). \tag{6.1}$$

Moreover, if the equality holds, then:

1. *the coefficient of x_0 in g, say λ, is non-zero;*
2. *$g' = \lambda$;*
3. *$dG_n = \lambda^{-(2^n-1)}(f' + g'y_0)^{2^n-1}\, dy_0 + \sum_{i=0}^{n-1} G_i^{2^{n-i}-1}\, dG_i$.*

Thus, the above theorem implies that when trying to minimize the degrees of the G_n's, the best one can expect is to obtain $\deg G_n = 2^{n+1}(d-1) - (d-2)$ for $n \geq 1$.

Theorem 6.5 above is somewhat similar to Theorem 2.4 in [Fin04]: both give lower bounds for the degrees of lifts of points and a necessary condition on the equation of the curve to achieve those bounds. (In fact, the ideas behind the proofs are the same.) In the case of [Fin04], computations show that the obtained condition seems to be also sufficient, at least for $n = 1, 2$. The next proposition, proved in section 10, shows that this is not the case here.

Proposition 6.6. *Let C and $\boldsymbol{C}$ be curves defined by equations* (3.1) *and* (3.3) *and*

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

be a lift of points between their affine parts such that $\deg G_1 = (3d-2)$*. Then* $\deg g = 2$ *(i.e.,* as polynomial in x_0*, $g(x_0)$ has degree one) and $F_1 \in k[x_0]$ with* $\deg F_1 \leq 2$ *(i.e.,* as polynomial in x_0*, F has degree at most one).*

Hence, to achieve the lower bound, besides having $g' \in k^{\times}$, it is also necessary to have $\deg g = 2$. On the other hand, those two conditions do *seem* to be sufficient, as we shall see in Theorem 6.13 and in the computation of section 12.

One can also use the same approach used to prove Theorem 6.5 to find lower bounds for the degrees of the F_n's. But, in this case, one obtains the trivial bound $\deg F_n \geq 0$. Although the bound itself is useless, the proof again gives us a necessary conditions to have the equality, and, as we shall see in Proposition 6.8, one can indeed often obtain equality.

Theorem 6.7. *Let C and $\boldsymbol{C}$ be as in equations* (3.1) *and* (3.3)*, and ν, as in equation* (3.4)*, be a lift of points between U and $\boldsymbol{U}$, the affine parts of C and $\boldsymbol{C}$ respectively. Then, if $dF_1 = 0$, then either $g = \lambda$ or $g = \lambda x_0$, for some $\lambda \in k^{\times}$. In particular, this restriction on g has to hold if* $\deg F_1 = 0$.

Furthermore, one can prove:

Proposition 6.8. *Let C be a curve given by equation* (3.1) *with $g \in k^{\times}$. Then, for any lifting $\boldsymbol{C}$ of C, there exists a lift of points*

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

such that

$$\begin{aligned} &\deg F_n = 0, \\ &\deg G_n \leq 2^n \left(d + n \left(-\frac{1}{2} + d \cdot \sum_{j=1}^{n} \frac{1}{j} \right) \right). \end{aligned}$$

(The proof of Theorem 6.7 is given in section 9, while the proof of Proposition 6.8 is given in section 10.)

Also, as we shall see in Proposition 6.9 below, if $g = x_0$, one can also obtain $\deg F_1 = 0$, but in this case, not always one can have $\deg F_2 = 0$: for example, as we shall state in Theorem 6.13, the ordinary elliptic curve $y_0^2 + x_0 y_0 = x_0^3 + a_0$ has no lift modulo 8 with $\deg F_2 = 0$. So, the condition $g = \lambda x_0$ in Theorem 6.7 is not sufficient.

The next proposition, also proved in section 10, shows that if we have $g = x_0$, one can achieve the lower bounds for both F_1 and G_1 modulo 4. Observe that, by Theorem 6.7, it is not enough to have $\deg g = 2$, even though such a curve is isomorphic to a curve with $g = x_0$: the degrees of a lift of points depends on the *equation* of the curve in question, not on its isomorphism class. On the other hand, having $g = \lambda x_0$, for any $\lambda \in k^\times$, instead of $g = x_0$ does yield same degrees.

Proposition 6.9. *Let C be a curve defined by equation (3.1). If $g = x_0$, then there exists a lifting of C, say $\boldsymbol{C}$ (defined by (3.3)), for which we have a lift of points*

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

between the affine parts of C and $\boldsymbol{C}$ with $\deg G_1 = (3d - 2)$ and $F_1 \in k$. Hence, $\boldsymbol{C}$ is an absolute minimal degree curve over C with respect to both $\boldsymbol{x}$ and $\boldsymbol{y}$, and ν is an absolute minimal degree lift of points.

It is worth noticing that the proof is actually constructive, giving us a method to obtain the curve $\boldsymbol{C}$ and lift of points ν (modulo 4), which can then be used in the construction of the error-correcting codes.

Also note that, with the above proposition, when $g = x_0$ one can use Propositions 6.2 and 6.4 instead of 6.1 and 6.3 to bound the degrees of the later F_i's and G_i's.

Observe that, in the case of minimal degree liftings with respect to $\boldsymbol{y}$, although we have $\deg F_1 = 0 < 2(2 + 5(d - 2)/8)$ and $\deg G_1 = 3d - 2 < 2(d + 5(d - 2)/8)$, the bounds from Proposition 6.2 cannot be improved. The reason for that comes from the condition $e \geq (d - 2)(1 + 1/2^r)/r$ in Lemma 8.2, which is, in fact, the key part of the proof of Propositions 6.1 and 6.2. Very roughly, the reason for that is that the degrees of G_2 and F_2 might have to reach the stated upper bounds just to match the degrees of the terms that do not involve F_1 or G_1 in the third coordinate of the Greenberg transform.

In the case of minimal degree liftings with respect to $\boldsymbol{x}$, note that, since we have $\deg g = 2$, Proposition 6.3 gives, for $n \geq 2$,

$$\deg G_n \leq 2^n \left(d + n \left(\frac{d - 2}{2} + (d - 2) \sum_{j=1}^{n} \frac{1}{j} \right) \right),$$

while Proposition 6.4 gives

$$\deg G_n \leq 2^n \left(d + n \left(-\frac{(d - 2)}{2} + (d - 2) \sum_{j=1}^{n} \frac{1}{j} \right) \right),$$

The next proposition, proved in section 11, will give a necessary and sufficient condition for the existence of a lift of the Frobenius (between affine parts of hyperelliptic curves, as in section 5) associated to a lift of points modulo 8 (for a hyperelliptic curve C given by equation (3.1)). Note, though, that the existence of a lift modulo 4 is guaranteed by

Theorem 4.1 in [Fin04]. Before we can give a precise statement, we need the following definition.

Definition 6.10. Let $h(x_0, y_0) \in k[x_0, y_0]$ and $\boldsymbol{h}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}_2(k)$ be the lift of h defined by applying the Teichmüller lift to the coefficients of h, i.e., if λ is a coefficient of some monomial of h, then the corresponding monomial of $\boldsymbol{h}$ has coefficient $(\lambda, 0)$. (We shall refer to such lift as the *Teichmüller lift* of the polynomial h.) We define

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

Note that when $p = 2$, $\Psi(h(x_0, y_0))$ is just the sum of all possible products of pairs of distinct monomials of h.

Proposition 6.11. *Let C/k and $\boldsymbol{C}/\boldsymbol{W}_3(k)$ be curves given by equations (3.1) and (3.3), and let*

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

be a lift of points. There is a lift of the Frobenius between the affine parts associated to ν if, and only if,

$$F_2 + x_0^2 F_1 + F_1^2 + \Psi(F_1) + \left(\frac{\partial F_1}{\partial x_0}\right)^2 F_1 + \left(\frac{\partial F_1}{\partial y_0}\right)^2 G_1$$

and

$$G_2 + y_0^2 G_1 + G_1^2 + \Psi(G_1) + \left(\frac{\partial G_1}{\partial x_0}\right)^2 F_1 + \left(\frac{\partial G_1}{\partial y_0}\right)^2 G_1$$

are both squares, say $P(x_0, y_0)^2$ and $Q(x_0, y_0)^2$, respectively. In this case, the lift of the Frobenius given by

$$\boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}^2 + 2\boldsymbol{F}_1 + 4\boldsymbol{P}, \boldsymbol{y}^2 + 2\boldsymbol{G}_1 + 4\boldsymbol{Q}),$$

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, respectively, to $\boldsymbol{W}_3[\boldsymbol{x}, \boldsymbol{y}]$.

Observe that Proposition 6.11 is similar to Proposition 2.7 in [Fin04], which deals with the case $p > 2$. On the other hand Proposition 6.11 is more general, since here there are no restrictions on the lift ν as there was in [Fin04]. But, in fact, one could easily make Proposition 2.7 of [Fin04] more general following the same ideas from the proof of the above proposition.

The next theorem, also proved in section 11, shows that if a lift has the degrees of either the F_n's or the G_n's satisfying the lower bounds given by Theorems 6.7 and 6.5, then there is a lift of the Frobenius modulo 8.

Theorem 6.12. *Let C and $\boldsymbol{C}$ be given by equations* (3.1) *and* (3.3) *respectively. Let*

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

be a lift of points such that

$$\begin{aligned} dF_1 &= (h\, g + x_0)\, dx_0, \\ dF_2 &= (h^3\, g^3 + x_0^3)\, dx_0 + F_1\, dF_1, \end{aligned}$$

for some $h \in k(C)$. Then there is a lift of the Frobenius (modulo 8) between the affine parts of C and $\boldsymbol{C}$ associated to ν. In particular, if $\deg F_n = 0$ or if $\deg G_n = 2^{n+1}(d-1) - (d-2)$ (i.e., the degrees of either the F_n's or the G_n's are equal to the lower bounds) for $n = 1, 2$, then there is a lift of the Frobenius modulo 8.

We note that the last sentence of the theorem, at least for the case when $\deg G_n = 2^{n+1}(d-1) - (d-2)$, is not totally trivial at this points, but will follow from some later results.

Finally, it might also be worth mentioning the case of elliptic curves (i.e., $d = 3$), to relate minimal degrees liftings and canonical liftings. One has:

Theorem 6.13. *Let C be an elliptic curve, i.e., a curve given by equation* (3.1) *with $d = 3$. Then:*

(1) *C is ordinary if, and only if,* $\deg g = 2$.
(2) *If C is not ordinary, then there is no lift of points satisfying the lower bounds for the G_i's from Theorem 6.5.*
(3) *If C is ordinary, then, modulo* 16, *the absolute minimal degree curve over C with respect to $\boldsymbol{y}$ is the canonical lifting of C (hence it's unique), the minimal degree lift of points is also unique and it satisfies the lower bounds of Theorem 6.5. (Hence, by Theorem 6.12, there is a lift of the Frobenius modulo* 8 *associated to the lift of points.)*
(4) *If C is ordinary, then there is no lift of points with* $\deg F_2 = 0$. *But, modulo* 16, *its absolute minimal degree curve over C with respect to $\boldsymbol{x}$ is the canonical lifting, and, although* $\deg F_2 > 0$ *and* $\deg G_2 > 15$, *there is still a lift of the Frobenius modulo* 8 *associated to this lift.*

So, as in the case of $p > 2$, it seems that minimal degree curves and canonical liftings are closely related.

Item 1 of the theorem is a well known fact: see, for instance, section V.4 of [Sil85]. Item 2 is an immediate consequence of Theorem 6.5 (more precisely, the condition $g' \in k^{\times}$) and item 1.

Items 3 and 4 can be proved by explicit computations, which are too long to be presented here, but are perfectly feasible with the use of a computer.

7. Witt Vectors and Valuations

In this section we obtain the results that we shall need to deal with Witt vectors. Although the proofs are rather technical and sometimes tedious, the results are necessary for the proofs of the main results.

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

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

the corresponding *Witt polynomial*. Then, there exist polynomials

$$S_n, P_n \in \mathbb{Z}[X_0, \dots, X_n, Y_0, \dots, Y_n]$$

satisfying:

$$W_n(S_0, \dots, S_n) = W_n(X_0, \dots, X_n) + W_n(Y_0, \dots, Y_n)$$

and

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

(See [Ser79].)

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

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

and

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

We may write, to simplify the notation,

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

and

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

Since the entries of our Witt vectors are in characteristic p, we can use the polynomials $\bar{S}_n, \bar{P}_n \in \mathbb{F}_p[X_0, \dots, X_n, Y_0, \dots, Y_n]$, that are the reductions of S_n, P_n modulo p, to give us the sum and product of Witt vectors.

We now introduced some technical lemmas that we shall need later on.

Lemma 7.1. *The monomials $\prod X_i^{a_i} \prod Y_j^{b_j}$ (disregarding the coefficient) occurring in $\bar{P}_n$ satisfy*

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

Proof. This is Lemma 2.1 in [Fin02]. $\square$

Let K be a field of characteristic $p > 0$ and $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation on K. (In the applications, K will be the function field of our curve and $v = \mathrm{ord}_{P_\infty}$.) Then, for any positive integer r and positive real number e, we 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, $U(e) = \bigcap_{r \geq 0} U_r(e)$.) Also, for any $v_0 \in \mathbb{R}$, let

$$M_r(v_0, e) \stackrel{\text{def}}{=} \{ \boldsymbol{s} = (s_0, s_1, \dots) \in \boldsymbol{W}(K) \;\mid\; v(s_n) \geq p^n(v_0 - ne), \text{ for } n \leq r \}$$

and $M(v_0, e) \stackrel{\text{def}}{=} \bigcap_{r \geq 0} M_r(v_0, e)$

We then have the following lemmas:

Lemma 7.2. *The sets $U(e)$ and $U_r(e)$ are subgroups of $\boldsymbol{W}(K)^\times$.*

Proof. This is Lemma 3.1 in [Fin04]. □

Lemma 7.3. *Let k be a subfield of K for which every non zero element has valuation zero. (E.g., $\mathbb{F}_p$ or the field of constants in the case where K is a function field of a curve.) Then, the set $M_r(v_0, e)$ is a $\boldsymbol{W}(k)$-submodule of $\boldsymbol{W}(K)$. In particular, so is $M(v_0, e)$.*

Proof. We first show that $M_r(v_0, e)$ is closed under addition for all non-negative integers r.

Let $\boldsymbol{s} = (s_0, s_1, \dots), \boldsymbol{t} = (t_0, t_1, \dots) \in M_r(v_0, e)$. Then,

$$\boldsymbol{s} + \boldsymbol{t} = (S_0(\boldsymbol{s}, \boldsymbol{t}), S_1(\boldsymbol{s}, \boldsymbol{t}), \dots),$$

where $S_n \in \mathbb{Z}[X_0, \dots, X_n, Y_0, \dots, Y_n]$ is defined recursively by

$$S_n = (X_n + Y_n) + \frac{1}{p}(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p) + \cdots + \frac{1}{p^n}(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}). \tag{7.1}$$

It is enough to prove that every monomial in S_n, for $n = 0, \dots, r$, has valuation, when computed at $(\boldsymbol{s}, \boldsymbol{t})$, greater than or equal to $p^n(v_0 - ne)$.

Observe that the valuations of the coefficients of the monomials of S_n are zero, since, in characteristic $p > 0$, they are roots of unity. Hence, we shall disregard the coefficients of the monomials.

We proceed by induction on n. For $n = 0$, $S_0(\boldsymbol{s}, \boldsymbol{t}) = s_0 + t_0$, and since $v(s_0), v(t_0) \geq v_0$, the statement clearly holds.

So, assume that, for $0 \leq m < n \leq r$, the valuations of the monomials of S_m when evaluated at $(\boldsymbol{s}, \boldsymbol{t})$ are less than or equal to $p^m(v_0 - me)$ and let $\prod X_i^{a_i} \prod Y_j^{b_j}$ be a monomial (with the coefficient dropped) that appears in S_n.

By equation (7.1), this monomial comes from $S_m^{p^{n-m}}$, or it is either of the form $X_i^{p^{n-i}}$ or $Y_j^{p^{n-j}}$.

The monomials of $S_m^{p^{n-m}}$ are products of p^{n-m} monomials of S_m, and therefore, by the induction hypothesis, they have valuation, when computed at $(\boldsymbol{s}, \boldsymbol{t})$, greater or equal to $p^{n-m}p^m(v_0 - me) \geq p^n(v_0 - ne)$.

If the monomial is either $X_i^{p^{n-i}}$ or $Y_j^{p^{n-j}}$, then the corresponding valuations are $p^{n-i}v(s_i) \geq p^n(v_0 - ie)$ and $p^{n-j}v(t_j) \geq p^n(v_0 - je)$, respectively. In either case, the monomials have valuation greater than or equal to $p^n(v_0 - ne)$. Therefore, $M_r(v_0, e)$ is closed under addition.

Now let $\boldsymbol{c} = (c_0, c_1, \dots) \in \boldsymbol{W}(k)$ and $\boldsymbol{s} \in M_r(v_0, e)$. Note that either $v(c_i) = 0$ or $c_i = 0$.

The $(n+1)$-th coordinate of $\boldsymbol{c} \cdot \boldsymbol{s}$, for $0 \leq n \leq r$, is given by $\bar{P}_n(\boldsymbol{c}, \boldsymbol{s})$. Let $\prod X_i^{a_i} \prod Y_j^{b_j}$ be a monomial (disregarding the coefficient) in $\bar{P}_n$. If $c_i = 0$, for some fixed i for which $a_i \neq 0$, then

$$v\left(\prod c_i^{a_i} \prod s_j^{b_j}\right) = v(0) > p^n(v_0 - ne).$$

If $c_i \neq 0$ for all i such that $a_i \neq 0$, then, by Lemma 7.1,

$$\begin{aligned} v\left(\prod c_i^{a_i} \prod s_j^{b_j}\right) &= \sum a_i v(c_i) + \sum b_j v(s_j) \\ &= \sum b_j v(s_j) \geq \sum b_j p^j (v_0 - je) \\ &\geq p^n(v_0 - ne). \end{aligned}$$

Therefore, $v(\bar{P}_n(\boldsymbol{c}, \boldsymbol{s})) \geq p^n(v_0 - ne)$, and so $\boldsymbol{c} \cdot \boldsymbol{s} \in M_r(v_0, e)$.

□

Lemma 7.4. *Let k be a field of characteristic $p > 0$ and $\boldsymbol{h}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}(k)[\boldsymbol{x}, \boldsymbol{y}]$. If we let $\boldsymbol{x} = (x_0, x_1, \dots)$ and $\boldsymbol{y} = (y_0, y_1, \dots)$ and expand $\boldsymbol{h}(\boldsymbol{x}, \boldsymbol{y})$ as Witt vector (as we do with Greenberg transforms), then the $(n+1)$-th coordinate of this expansion is of the form*

$$x_n \left(\frac{\partial h}{\partial x_0}(x_0, y_0)\right)^{p^n} + y_n \left(\frac{\partial h}{\partial y_0}(x_0, y_0)\right)^{p^n} + \dots,$$

where $h(x_0, y_0)$ is the reduction modulo p of $\boldsymbol{h}(\boldsymbol{x}, \boldsymbol{y})$ and the omitted terms depend only on x_i and y_i, for $i = 0, \dots (n-1)$.

Proof. The lemma clearly holds for $\boldsymbol{h}(\boldsymbol{x}, \boldsymbol{y})$ equal to either $\boldsymbol{x}$, $\boldsymbol{y}$ or a constant (in $\boldsymbol{W}(k)$). So, it suffices to show that if the lemma holds for $\boldsymbol{h}_1$ and $\boldsymbol{h}_2$, then it must also hold for their sum and product.

We first show that it holds for $\boldsymbol{h}_1 + \boldsymbol{h}_2$: just observed that the $(n+1)$-th coordinate is given by the polynomial S_n (as in equation (7.1)), and so, in the $(n+1)$-th coordinate of

$\boldsymbol{h}_1 + \boldsymbol{h}_2$, we have

$$\left(x_n \left(\frac{\partial h_1}{\partial x_0} \right)^{p^n} + y_n \left(\frac{\partial h_1}{\partial y_0} \right)^{p^n} + \dots \right) + \left(x_n \left(\frac{\partial h_2}{\partial x_0} \right)^{p^n} + y_n \left(\frac{\partial h_2}{\partial y_0} \right)^{p^n} + \dots \right) + \dots$$
$$= \left(x_n \left(\frac{\partial (h_1 + h_2)}{\partial x_0} \right)^{p^n} + y_n \left(\frac{\partial (h_1 + h_2)}{\partial y_0} \right)^{p^n} + \dots \right) + \dots,$$

where no omitted term involves x_n or y_n. Thus, it works for the sum.

For the product, remember that

$$\bar{P}_n = (X_0^{p^n} Y_n + X_1^{p^{n-1}} Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) + \dots,$$

where no omitted term involves either X_n or Y_n. (See, for instance, formula (3) in [Fin02].) Hence, the $(n+1)$-th coordinate of $\boldsymbol{h}_1 \cdot \boldsymbol{h}_2$ is given by

$$h_2^{p^n} \left(x_n \left(\frac{\partial h_1}{\partial x_0} \right)^{p^n} + y_n \left(\frac{\partial h_1}{\partial y_0} \right)^{p^n} + \dots \right) + h_1^{p^n} \left(x_n \left(\frac{\partial h_2}{\partial x_0} \right)^{p^n} + y_n \left(\frac{\partial h_2}{\partial y_0} \right)^{p^n} + \dots \right) + \dots$$
$$= \left(x_n \left(\frac{\partial (h_1 \cdot h_2)}{\partial x_0} \right)^{p^n} + y_n \left(\frac{\partial (h_1 \cdot h_2)}{\partial y_0} \right)^{p^n} + \dots \right) + \dots,$$

where no omitted term involves x_n or y_n. Therefore, it also works for the product.

□

The next lemma will be quite useful when analyzing the equations that define the Greenberg transform of a curve over $\boldsymbol{W}(k)$, in particular in the construction of lifts of points.

Lemma 7.5. *Let K and k be as in Lemma 7.3, $\boldsymbol{s}, \boldsymbol{t} \in U_{r-1}(e)$ and $\boldsymbol{h}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}(k)[\boldsymbol{x}, \boldsymbol{y}]$. Furthermore, let $-v_0$ be the* weighted *degree of $\boldsymbol{h}$, where the weight of $\boldsymbol{x}$ is defined to be $-v(s_0)$ and the weight of $\boldsymbol{y}$ is defined to be $-v(t_0)$. Then, on the $(r+1)$-th coordinate of $\boldsymbol{h}(\boldsymbol{s}, \boldsymbol{t})$, we have*

$$s_r \left(\frac{\partial h}{\partial x_0}(s_0, t_0) \right)^{p^r} + t_r \left(\frac{\partial h}{\partial y_0}(s_0, t_0) \right)^{p^r} + \dots, \tag{7.2}$$

where all the omitted terms do not involve s_n or t_n and have valuation less than or equal to $p^r(v_0 - re)$.

Proof. By Lemma 7.4, the $(n+1)$-th coordinate of $\boldsymbol{h}(\boldsymbol{s}, \boldsymbol{t})$ indeed is as in equation (7.2). So, all that is left to do is to prove the statement about the valuation of the omitted terms.

For every monomial $\boldsymbol{x}^i \boldsymbol{y}^j$ of $\boldsymbol{h}$, disregarding the coefficient, the term $\boldsymbol{s}^i \boldsymbol{t}^j \in U_{r-1}(e)$. But since the weighted degree of $\boldsymbol{h}$ is $-v_0$, which implies that $i\, v(s_0) + j\, v(t_0) \geq v_0$, we have, by Lemma 7.3, that $\boldsymbol{h}(\boldsymbol{s}, \boldsymbol{t}) \in M_{r-1}(v_0, e)$.

By the same reasoning, if $\boldsymbol{s}$ and $\boldsymbol{t}$ were in $U_r(e)$ instead of in $U_{r-1}(e)$, then $\boldsymbol{h}(\boldsymbol{s}, \boldsymbol{t})$ would be in $M_r(v_0, e)$, and the bounds would clearly hold. But the proof of Lemma 7.3 bounds the valuation of *each* monomial appearing in the sum of two elements of $M_n(v_0, e)$ and in the product of an element of $\boldsymbol{W}(k)$ with an element of $M_n(v_0, e)$. So, this would bound the valuation of every monomial appearing in the $(r+1)$-th coordinate of $\boldsymbol{h}(\boldsymbol{s}, \boldsymbol{t})$ by $p^r(v_0 - e)$. In our case, we are only missing the bounds for the valuations of s_r and t_r, but we could still bound the valuation of every monomial that does not involve those two terms in exactly the same way. Hence, since by Lemma 7.4 no omitted term in equation (7.2) involves t_n or s_n, we can bound the valuations of the omitted terms by $p^r(v_0 - e)$.

□

The following lemma will be helpful when dealing with the second coordinate of the Greenberg transforms of curves.

Lemma 7.6. *Let*

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

and suppose that

$$\boldsymbol{h}((x_0, x_1), (y_0, y_1)) = (h_0(x_0, y_0), h_1(x_0, x_1, y_0, y_1)).$$

Then, if

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

we have

$$h_1(x_0, x_1, y_0, y_1) = x_1 \left(\frac{\partial h_0}{\partial x_0}\right)^p + y_1 \left(\frac{\partial h_0}{\partial y_0}\right)^p + \Psi(h_0) + \sum_{i,j} a_{i,j,1}\, x_0^{pi} y_0^{pj},$$

where Ψ is as in Definition 6.10.

Proof. This is Lemma 8.1 in [Fin04]. □

8. Proofs of the Upper Bounds

In this section we prove the upper bounds for the minimal degree lifting with respect to both $\boldsymbol{x}$ and $\boldsymbol{y}$. More precisely, we prove here Propositions 6.1, 6.2, 6.3 and 6.4.

The following lemma is an adaptation of Lemma IV.1 from [VW99] to our case, and it is the main tool to obtain the upper bounds for the degrees of the lifts of points.

Lemma 8.1. *Let C be a curve given by equation (3.1), and $R \stackrel{\text{def}}{=} \mathcal{O}(U)$ be the ring of regular functions on the affine part of C. Let also $a, b, c \in R$ with $(a, b) = 1$, $\deg a \leq n$, $\deg b = m$ and $\deg c \leq r$. Also, assume that $n + m + (d-2) \leq r$. Then, there exist $u, v \in R$ such that $au + bv = c$ with $\deg u \leq (m + (d-2))$ and $\deg v \leq (r - m)$.*

Proof. Since $m + n + (d-2) \leq r$, the map

$$\psi : \mathcal{L}((m + (d-2))P_\infty) \oplus \mathcal{L}((r-m)P_\infty) \to \mathcal{L}(rP_\infty),$$

defined by $\psi(u,v) \stackrel{\text{def}}{=} au + bv$ is well defined. Hence, to prove the lemma, it suffices to show that ψ is surjective.

Since the genus of C is $(d-1)/2$ and $(m+d-2)$, $(r-m)$ and r are all greater than $(d-2)$, by the Riemann-Roch Theorem, or more precisely, Corollary II.5.5(c) of [Sil85], the dimensions of the k-vector spaces above are

$$\begin{aligned} \ell((m+d-2)P_\infty) &= m + (d-2) - (d-1)/2 + 1, \\ \ell((r-m)P_\infty) &= (r-m) - (d-1)/2 + 1, \\ \ell(rP_\infty) &= r - (d-1)/2 + 1. \end{aligned}$$

On the other hand, since a and b are relatively prime, $(u,v) \in \ker\psi$ if, and only if, $u = bz$ and $v = -az$, for some $z \in R$.

Therefore, with the restrictions on the degrees of u and v, and since $n+m+(d-2) \leq r$, we have that $\ker(\psi) \cong \mathcal{L}((d-2)P_\infty)$. Observing that $\ell((d-2)P_\infty) = d-2-(d-1)/2+1$, the dimension of our domain minus the dimension of the kernel is equal the dimension of the co-domain, and hence our map is surjective.

□

The next lemma is the main step for the proofs of Propositions 6.1 and 6.2.

Lemma 8.2. *Let C and $\boldsymbol{C}$ be as in equations* (3.1) *and* (3.3) *respectively, and let*

$$\bar{\nu}(x_0, y_0) = ((x_0, F_1, \ldots, F_{r-1}), (y_0, G_1, \ldots, G_{r-1}))$$

be a lift of points such that $\bar{\nu}^*\boldsymbol{x}, \bar{\nu}^*\boldsymbol{y} \in U_{r-1}(e)$, with $e \geq (d-2)(1+1/2^r)/r$. Then, $\bar{\nu}$ can be completed to a lift

$$\nu(x_0, y_0) = ((x_0, F_1, \ldots, F_{r-1}, F_r, \ldots), (y_0, G_1, \ldots, G_{r-1}, G_r, \ldots)),$$

where $\nu^*\boldsymbol{x}, \nu^*\boldsymbol{y} \in U(e)$. Moreover,

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

for all $n \geq r$.

Proof. We shall inductively construct the F_n's and G_n's for $n \geq r$. So, assume we have $(x_0, F_1, \ldots, F_{n-1}), (y_0, G_1, \ldots, G_{n-1}) \in U_{n-1}(e)$ for some $n \geq r$. We shall find $F_n, G_n \in \mathcal{O}(U)$ such that

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

is a lift of points with $(x_0, F_1, \ldots, F_{n-1}, F_n), (y_0, G_1, \ldots, G_{n-1}, G_n) \in U_n(e)$.

By Lemma 7.4, in the $(n+1)$-th coordinate of the Greenberg transform, one has

$$y_n g^{2^n} + x_n (f' + g' y_0)^{2^n} = \ldots, \tag{8.1}$$

where no omitted term depends on x_n or y_n. Thus, to produce a lift modulo p^{n+1}, we need to find F_n and G_n such that

$$G_n g^{2^n} + F_n (f' + g' y_0)^{2^n} = \ldots, \tag{8.2}$$

where the omitted terms here are obtained by substituting x_i by F_i and y_i by G_i, for $i = 1, \ldots, (n-1)$, in equation (8.1). (Note that the equality in equation (8.2) is equality in $k(C)$, not in $k[x_0, y_0]$.)

We shall apply Lemma 8.1 with $a \stackrel{\text{def}}{=} g^{2^n}$, $b \stackrel{\text{def}}{=} (f' + g' y_0)^{2^n}$ and c as the omitted terms in (8.2). By Lemma 7.5, c has degree less than or equal to $2^n(2d + ne)$. By assumption C is non-singular, and hence $((f' + g' y_0), g) = 1$. Furthermore, since $e \geq (d-2)(1 + 1/2^r)/r \geq (d-2)(1+1/2^n)/n$ and $\deg g \leq (d-1)$, we have $2^n(2d + ne) \geq \deg a + \deg b + (d-2)$, and thus we can indeed apply Lemma 8.1, which gives us G_n and F_n such that

$$\deg G_n \leq 2^{n+1}(d-1) + (d-2), \quad \deg F_n \leq 2^n(2 + ne).$$

Therefore, clearly $(x_0, F_1, \ldots, F_n) \in U_n(e)$, and using again the bound on e, one can easily verify that $2^{n+1}(d-1) + (d-2) \leq 2^n(d + ne)$, yielding that $(y_0, G_1, \ldots, G_n) \in U_n(e)$. □

With the above lemma in hand, we can now prove Proposition 6.1.

Proof of Proposition 6.1. If one applies Lemma 8.2 with $r = 1$, one obtains the existence of a lift such that

$$\deg G_n \leq 2^{n+1}(d-1) + (d-2), \qquad \deg F_n \leq 2^n(2 + n3(d-2)/2)$$

for all $n \geq 1$. So, we need to show that we can improve that bound on the degree of F_1 to have it as in the statement.

We take, then, a closer look at the construction of F_1 and G_1. We need in this case F_1 and G_1 to satisfy

$$G_1 g^2 + F_1 (f' + g' y_0)^2 = \ldots,$$

where the omitted terms are the terms independent of x_1 and y_1 in the second coordinate of the Greenberg transform of C. We apply Lemma 8.1 again, with $a = g^2$, $b = (f' + g' y_0)^2$ and c as the omitted terms. In this case, observe that, by Lemma 7.5, $\deg c \leq 2(2d + e)$ for any $e > 0$, and hence $\deg c \leq 4d$. So, to apply the lemma, we take $r \stackrel{\text{def}}{=} \max\{4d, 2\deg g + 4(d-1) + (d-2)\}$.

This way we obtain F_1 and G_1 such that $\deg G_1 \leq 4(d-1)+(d-2)$ and

$$\deg F_1 \leq r - 4(d-1) = \max\{4, 2\deg g + (d-2)\} < 2(2+3(d-2)/2),$$

and hence, $(x_0, F_1), (y_0, G_1) \in U_1(3(d-2)/2)$.

Finally, Lemma 8.2, with $r = 2$ and $e = 3(d-2)/2$, finishes the proof.

□

Example 8.3. Consider the ordinary elliptic curve

$$E/k : y_0^2 + x_0 y_0 = x_0^3 + 1.$$

Then, the map

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

with

$$\begin{aligned}
F_1 &\stackrel{\text{def}}{=} x_0 y_0 \\
F_2 &\stackrel{\text{def}}{=} 1 + x_0^3 + x_0^5 + x_0^7 + x_0^8 + x_0^9 + x_0^{10} + (x_0 + x_0^5 + x_0^7) y_0 \\
G_1 &\stackrel{\text{def}}{=} x_0 + x_0^3 y_0 \\
G_2 &\stackrel{\text{def}}{=} 1 + x_0 + x_0^2 + x_0^3 + x_0^6 + (1 + x_0^5 + x_0^6 + x_0^7) y_0
\end{aligned}$$

is a minimal degree lifting from E to

$$\boldsymbol{E}/\boldsymbol{W}_3(k) : \boldsymbol{y}^2 + \boldsymbol{x}\boldsymbol{y} = \boldsymbol{x}^3 + (1, 0, 1)$$

with respect to $\boldsymbol{y}$. Notice that, in contrast with the case of characteristic $p > 2$, we cannot obtain a minimal degree lift of points that is *hyperelliptic*, i.e., that commutes with the hyperelliptic involutions of C and $\boldsymbol{C}$. Also, observe the the degrees are equal to the upper bounds given by Proposition 6.1.

On the other hand, $\boldsymbol{E}$ is *not* the absolute minimal degree curve over E, since the curve is ordinary and the canonical lifting with the elliptic Teichmüller lift would give us smaller degrees.

Again, in contrast with the case of $p > 2$, or, more precisely, with Proposition 2.3 in [Fin04], note that if we have one particular lift of points ν satisfying the bound in Proposition 6.1, this is not necessarily a *minimal* degree lift of points with respect to $\boldsymbol{y}$. This happens because we have a non-trivial kernel for the map ψ defined in the proof of Lemma 8.1.

On the other hand, since we know exactly what that kernel is, it is fairly easy to obtain a minimal degree lift of points with respect to $\boldsymbol{y}$ in every step of the procedure of finding the G_n's and F_n's: after a pair (G_n, F_n) is found, any other pair

$$\tilde{G}_n \stackrel{\text{def}}{=} G_n + z\,(f' + g' y_0)^{2^n},$$
$$\tilde{F}_n \stackrel{\text{def}}{=} F_n + z\,g^{2^n},$$

with $\deg z \leq (d-2)$, defines another lift also satisfying the bounds from Proposition 6.1. Observe that since $\deg z < d$, we must have $z \in k[x_0]$, and so $\deg z$ is even. Hence if $\deg G_n$ is even and greater than or equal to $2^n \deg g$, then the degree of G_n can always be lowered, and if either $\deg G_n$ is odd or less than or equal to $2^n \deg g$, then it is a minimal degree lift with respect to $\boldsymbol{y}$.

Something else worth noting is that the smaller $\deg g$ is, the smaller is the bound for $\deg F_1$. Also, as stated in Theorem 6.5, having $g = x_0$ (and so $\deg g = 2$) in fact yields smaller degrees also for G_1.

Lemma 8.2 tells us that having smaller degrees for first coordinates of a lift of points allows us to obtains lifts with smaller degrees for the remaining F_n's. Proposition 6.2, which is the analogue to Proposition 5.4 in [Fin04] and an immediate consequence of Lemma 8.2, illustrates this point in a particular case.

Proof of Proposition 6.2. Just apply Lemma 8.2 with $e = 5(d-2)/8$ and $r = 2$.

□

To prove Propositions 6.3 and 6.4, we first introduce a lemma analogous to Lemma 8.2. As we can see in its statement, in contrast with the case with Lemma 8.2, the degrees of the G_n's increase in such a way that there is no positive e for which the obtained $(y_0, G_1, G_2, \dots)$ is in $U(e)$.

Lemma 8.4. *Let C and $\boldsymbol{C}$ be as in equations* (3.1) *and* (3.3) *respectively, and let*

$$\bar{\nu}(x_0, y_0) = ((x_0, F_1, \dots, F_{r-1}), (y_0, G_1, \dots, G_{r-1}))$$

be a lift of points such that $\bar{\nu}^*\boldsymbol{x}, \bar{\nu}^*\boldsymbol{y} \in U_{r-1}(e_{r-1})$, with $e_{r-1} \geq (\deg g + (d-2)/2^r - 2)/r$. Then, $\bar{\nu}$ can be extended to a lift

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

with $\nu^*\boldsymbol{x}, \nu^*\boldsymbol{y} \in U(e_n)$, where $e_n = e_{r-1} + (d - \deg g)\sum_{j=r}^{n} 1/j$. Moreover,

$$\deg F_n \leq 2^n \deg g + (d-2),$$

for all $n \geq r$.

Proof. We again construct inductively the desired F_i's and G_i's. So, assume we have $(F_0, \ldots, F_{n-1}), (G_0, \ldots, G_{n-1}) \in U_{n-1}(e_{n-1})$. By Lemma 7.5, to extend this map to the next coordinate, we have to find F_n and G_n such that

$$F_n(f' + g'y_0)^{2^n} + G_n g^{2^n} = \ldots,$$

where the omitted terms (coming from the $(n+1)$-th coordinate of the Greenberg transform) have degree less than or equal to $2^n(2d + ne_{n-1})$.

Since

$$e_{n-1} \geq e_{r-1} \geq (\deg g + (d-2)/2^r - 2)/r \geq (\deg g + (d-2)/2^n - 2)/n, \tag{8.3}$$

we have $2^n(2d + ne_{n-1}) \geq 2^{n+1}(d-1) + 2^n \deg g + (d-2)$, and thus we can apply Lemma 8.1. We then obtain F_n and G_n such that

$$\begin{aligned} \deg F_n &\leq 2^n \deg g + (d-2) \\ \deg G_n &\leq 2^n(2d + ne_{n-1}) - 2^n \deg g = 2^n \left(d + n \left(\frac{d - \deg g}{n} + e_{n-1} \right) \right) \\ &= 2^n(d + ne_n). \end{aligned}$$

Finally, inequality (8.3) implies that $\deg F_n \leq 2^n \deg g + (d-2) \leq 2^n(2 + ne_n)$, and hence $\nu^*\boldsymbol{x}, \nu^*\boldsymbol{y} \in U(e_n)$.

□

We can now prove Propositions 6.3 and 6.4.

Proof of Proposition 6.3. We just apply Lemma 8.4, with $r = 1$ and $e_0 = \max\{0, \deg g + (d-6)/2\}$.

□

Proof of Proposition 6.4. The bounds on $\deg F_1$ and $\deg G_1$ imply that $(x_0, F_1), (y_0, G_1) \in U_1((d-2)/2)$. Since $\deg g \leq (3d+2)/4$, we have $e_1 \geq (\deg g + (d-2)/4 - 2)/2$. The proposition then immediately follows from Lemma 8.4.

□

9. Proofs of the Lower Bounds

In this section we prove the lower bounds (and the necessary conditions to achieve those lower bounds) for the minimal degree liftings with respect to both $\boldsymbol{x}$ and $\boldsymbol{y}$. More precisely, we prove Theorems 6.5 and 6.7 .

Proof of Theorem 6.5. If we work modulo 2^{n+1}, or equivalently, truncate the lift ν at the $(n+1)$-th coordinate, Theorem 4.1 in [Fin04] tells us that there exists a lift of ϕ^n, the 2^n-th power Frobenius of C associated to ν. We shall denote such lift by (bold-face) $\boldsymbol{\phi}^n$.

Furthermore, Theorem 4.1 in [Fin04] also tells us that $\boldsymbol{\phi}^n$ can be written as

$$\boldsymbol{\phi}^n(\boldsymbol{x}, \boldsymbol{y}) = \left(\sum_{i=0}^{n} 2^i \boldsymbol{F}_i^{2^{n-i}}, \sum_{i=0}^{n} 2^i \boldsymbol{G}_i^{2^{n-i}} \right), \tag{9.1}$$

where $\boldsymbol{F}_i, \boldsymbol{G}_i \in \boldsymbol{W}_{n+1}(k)[\boldsymbol{x}, \boldsymbol{y}]$ are lifts of $F_i, G_i \in k[x_0, y_0]$. Hence, if

$$\boldsymbol{\omega}_n \stackrel{\text{def}}{=} \frac{d\boldsymbol{x}}{2\boldsymbol{y} + \boldsymbol{g}^{\sigma^n}(\boldsymbol{x})} = \frac{d\boldsymbol{y}}{(\boldsymbol{f}')^{\sigma^n}(\boldsymbol{x}) - (\boldsymbol{g}')^{\sigma^n}(\boldsymbol{x})\, \boldsymbol{y}}, \tag{9.2}$$

then $(1/2^n\, \boldsymbol{\phi}^n)^* \boldsymbol{\omega}_n$ reduces, modulo 2, to

$$\omega_n \stackrel{\text{def}}{=} \frac{\sum_{i=0}^{n} G_i^{2^{n-i}-1} dG_i/dy_0}{(f' + g'\, y_0)^{2^n}}\, dy_0 = \frac{\sum_{i=0}^{n} G_i^{2^{n-i}-1} dG_i/dy_0}{(f' + g'\, y_0)^{2^n-1}}\, \frac{dx_0}{g}. \tag{9.3}$$

Observe that the differential dx_0/g does not vanish on U, and since $\boldsymbol{\omega}_n$ is regular on $\boldsymbol{U}^{\sigma^n}$, ω_n must also be regular on U. Thus,

$$\frac{\sum_{i=0}^{n} G_i^{2^{n-i}-1}\, dG_i/dy_0}{(f' + g'\, y_0)^{2^n-1}} \in \mathcal{O}(U),$$

and so it can be written as a polynomial, say $h_n(x_0, y_0)$. Hence

$$\omega_n = h_n(x_0, y_0) \frac{dx_0}{g} \tag{9.4}$$

and

$$\frac{dG_n}{dy_0} = h_n(x_0, y_0)(f' + g'\, y_0)^{2^n-1} + \sum_{i=0}^{n-1} G_i^{2^{n-i}-1}\, \frac{dG_i}{dy_0}. \tag{9.5}$$

Note that $h_n(x_0, y_0)$ is not equal to zero, since $(1/2^n \boldsymbol{\phi}^n)^*$ is the "inverse" of the n-th power of the Cartier operator, which we shall denote by $\mathcal{C}^n$, and therefore, $\mathcal{C}^n(\omega_n) = dx_0/g(x_0) \neq 0$, which implies that ω_n cannot be equal to zero.

Now, for $i = 0, \ldots, (n-1)$,

$$\deg \left(G_i^{2^{n-i}-1}\, \frac{dG_i}{dy_0} \right) = 2^{n+1}(d-1) - 2^{n-i}(d-2) - d < (2^n - 1)(2d-2),$$

and hence,

$$\deg \left(\frac{dG_n}{dy_0} \right) = \deg h_n + (2^n - 1)(2d-2) \geq (2^n - 1)(2d-2).$$

Thus,

$$\deg G_n \geq 2^{n+1}(d-1) - (d-2).$$

Moreover, we can only have equality if $h_n(x_0, y_0)$ is a constant.

Let us assume now that

$$\deg G_i = 2^{i+1}(d-1) - (d-2),$$

for $i = 0, \dots, n$. By equation (9.4) and the conclusion of the previous paragraph, we must have

$$\omega_i = \lambda_i \frac{dx_0}{g} = \lambda_i \frac{dy_0}{f' + g' y_0}, \tag{9.6}$$

where $\lambda_i \in k$.

On the other hand, for $i = 1$, ω_1 is defined as the reduction modulo 2 of

$$\frac{1}{2}\boldsymbol{\phi}^*(\boldsymbol{\omega}_1) = \frac{1}{2}\boldsymbol{\phi}^*\left(\frac{d\boldsymbol{x}}{2\boldsymbol{y} + \boldsymbol{g}^\sigma}\right),$$

and thus, by equation (9.1) with $n = 1$,

$$\omega_1 = \frac{dF_1 + x_0 dx_0}{g(x_0)^2}. \tag{9.7}$$

Comparing equations (9.7) and (9.6), with $i = 1$, we obtain

$$(\lambda_1 g + x_0) = \frac{dF_1}{dx_0}.$$

By taking differentials in the above equation, and since we are in characteristic 2, we obtain

$$(\lambda_1 g' + 1) dx_0 = d\left(\frac{dF_1}{dx_0}\right) = 0.$$

Thus, $\lambda_1 = \lambda^{-1}$, where λ is then the necessarily non-zero coefficient of x_0 in g, and we have established items (1) and (2) of the theorem. Also, note that, by equation (9.5), we also proved item (3) for $n = 1$ in the theorem.

With the case $i = 1$ done, we can now finish the proof of item (3) by induction on i. So, assume that

$$dG_{i-1} = \lambda^{-(2^{i-1}-1)}(f' + g'y_0)^{2^{i-1}-1}\, dy_0 + \sum_{j=0}^{i-2} G_j^{2^{i-1-j}-1}\, dG_j$$

for some $i \leq n$.

The properties of the Cartier divisor, together with our induction hypothesis, give us

$$\mathcal{C}\left(\frac{\sum_{j=0}^{i} G_j^{2^{i-j}-1} dG_j}{(f' + g'\, y_0)^{2^i}}\right) = \frac{\sum_{j=0}^{i-1} G_j^{2^{i-1-j}-1} dG_j}{(f' + g'\, y_0)^{2^{i-1}}} = \lambda^{-(2^{i-1}-1)} \frac{dy_0}{f' + g' y_0}. \tag{9.8}$$

On the other hand, since by assumption $\deg G_i = 2^{i+1}(d-1) - (d-2)$, equation (9.6) holds, and thus we just need to show that $\lambda_i = \lambda^{-(2^i-1)}$. But, since $g' = \lambda$,

$$\mathcal{C}\left(\frac{\sum_{j=0}^{i} G_j^{2^{i-j}-1} dG_j}{(f' + g'\, y_0)^{2^i}}\right) = \mathcal{C}\left(\lambda_i \frac{dy_0}{f' + g' y_0}\right) = \lambda_i^{1/2}\, \lambda^{1/2} \frac{dy_0}{f' + g' y_0}. \tag{9.9}$$

Comparing equations (9.8) and (9.9), we obtain $\lambda_i = \lambda^{-(2^i-1)}$.

$\square$

The next proposition, which follows from an analysis of the proof of Theorem 6.5 above, establishes a relation between the formulas for the dF_n's and formulas for the dG_n's in general and will be used in the proof of Theorem 6.12.

Proposition 9.1. *Let C and $\boldsymbol{C}$ be as in equations* (3.1) *and* (3.3)*, and ν, as in equation* (3.4)*, be a lift of points between the affine parts of C and $\boldsymbol{C}$. Then,*

$$dF_n = h_n g^{2^n-1}\, dx_0 + \sum_{i=0}^{n-1} F_i^{2^{n-i}-1}\, dF_i,$$

and

$$dG_n = h_n (f' + g' y_0)^{2^n-1}\, dy_0 + \sum_{i=0}^{n-1} G_i^{2^{n-i}-1}\, dG_i$$

for some $h_n \in k[x_0, y_0]$.

Proof. In the proof of Theorem 6.5 one sees that, by using the two different forms of $\boldsymbol{\omega}_n$ in equation (9.2), we must have

$$\omega_n = \frac{\sum_{i=0}^{n} F_i^{2^{n-i}-1} dF_i}{g^{2^n}} = \frac{\sum_{i=0}^{n} G_i^{2^{n-i}-1} dG_i}{(f' + g'\, y_0)^{2^n}}.$$

Also, still following the proof of Theorem 6.5, we see that, as in equation (9.4),

$$\omega_n = h_n \frac{dx_0}{g} = h_n \frac{dy_0}{f' + g' y_0}$$

for some *non-zero* $h_n \in k[x_0, y_0]$. Comparing the two formulas for ω_n finishes the proof.

□

As observed in section 6, the same idea used to prove Theorem 6.5 gives the analogous result for the F_n's.

Proof of Theorem 6.7. We work modulo 4, and hence there is a lift of ϕ, which we denote by $\boldsymbol{\phi}$, given by equation (9.1) (with $n = 1$). With $\boldsymbol{\omega}_1$ as in equation (9.2), $(1/2\,\boldsymbol{\phi})^* \boldsymbol{\omega}_1$ reduces, modulo 2, to

$$\omega_1 \stackrel{\text{def}}{=} \frac{dF_1 + x_0\, dx_0}{g^2} = \frac{x_0\, dx_0}{g^2}.$$

Since dx_0/g does not vanish on U, and since $\boldsymbol{\omega}_1$ is regular on $\boldsymbol{U}^\sigma$, ω_1 must also be regular on U. Thus,

$$\omega_1 = h_1 \frac{dx_0}{g}$$

for some $h_1 \in k[x_0, y_0]$. Hence

$$x_0 = h_1\, g.$$

Therefore, either $g = \lambda$ or $g = \lambda x_0$ for some $\lambda \in k$. Since the curve is non-singular, we must have $\lambda \neq 0$.

□

10. Proofs of Propositions About Achieving the Lower Bound

In this section we prove Propositions 6.6, 6.8 and 6.9.

Proof of Proposition 6.6. By Theorem 6.5, we have that $g' = \lambda$, with $\lambda \in k^{\times}$. This says that the coefficient of x_0 in g is λ, and this, with a change of variables $\tilde{x}_0 = \lambda x_0$ and $\tilde{y}_0 = y_0/\lambda^{d/2}$, we may assume, without loss of generality, that $\lambda = 1$.

Write

$$\boldsymbol{f}(\boldsymbol{x}) = \sum_{i=0}^{d} \boldsymbol{a}_i \boldsymbol{x}^i,$$

and

$$\boldsymbol{g}(\boldsymbol{x}) = \sum_{j=0}^{(d-1)/2} \boldsymbol{b}_j \boldsymbol{x}^j,$$

where

$$\begin{aligned} \boldsymbol{a}_i &= (a_{i,0}, a_{i,1}), \quad \text{for } i = 0, \dots, d, \\ \boldsymbol{b}_j &= (b_{j,0}, b_{j,1}), \quad \text{for } j = 0, \dots, (d-1)/2. \end{aligned}$$

By Lemma 7.6, we have on the second coordinate of equation the Greenberg transform of equation (3.3)

$$y_1 g^2 + x_1 (g' y_0)^2 + \Psi(y_0^2 + g\, y_0) + \left(\sum_{j=0}^{(d-1)/2} b_{j,1} x_0^{2j} \right) y_0^2 = x_1 (f')^2 + \Psi(f) + \sum_{i=0}^{d-1} a_{i,1} x_0^{2i},$$

For ν to be well defined, it is necessary that

$$G_1\, g^2 + F_1 (g' y_0)^2 + \Psi(y_0^2 + g\, y_0) + \left(\sum_{j=0}^{(d-1)/2} b_{j,1} x_0^{2j} \right) y_0^2 = F_1 (f')^2 + \Psi(f) + \sum_{i=0}^{d-1} a_{i,1} x_0^{2i},$$

in $k(C)$, or

$$G_1\, g^2 + F_1 (f' + g' y_0)^2 = \Psi(f) + \sum_{i=0}^{d-1} a_{i,1} x_0^{2i} + \Psi(y_0^2 + g\, y_0) + \left(\sum_{j=0}^{(d-1)/2} b_{j,1} x_0^{2j} \right) y_0^2. \quad (10.1)$$

One can easily check that all the terms in the right-hand-side of the equation above have degrees less than or equal to $(4d-1)$. Therefore, all terms from $G_1\, g^2$ and $F_1(f' + g' y_0)^2$ of degree greater than $(4d-1)$, if any, have to cancel each other out.

Assume now that $\deg g \geq (d+1)/2$, so that we have $\deg(G_1\, g^2) \geq (4d-1)$. Since $\deg G_1 = (3d-2)$, we must then have

$$\deg F_1 = 2 \deg g - d + 2 \leq d. \quad (10.2)$$

Hence, if we write

$$F_1 = h_1 + h_2\, y_0, \;\; h_1, h_2 \in k[x_0],$$

then $h_2 \in k$. Therefore, by Proposition 9.1 and Theorem 6.5,

$$dF_1 = \left(h_1' + \frac{f' h_2}{g} + \frac{h_2}{g} y_0 \right) dx_0 = (g + x_0) dx_0.$$

Thus, $h_2 = 0$ and $F_1' = h_1' = g + x_0$. Then, $\deg F_1 \geq \deg g + 2$, unless $\deg g = 2$, in which case the proposition automatically holds. But if $\deg F_1 \geq \deg g + 2$, then the equality in equation (10.2) would imply that $\deg g \geq d$, a contradiction, since the degree of $\deg g$ is always less than or equal to $(d-1)$. Therefore, if $\deg g \neq 2$, then we must have $\deg g < (d+1)/2$.

But, if $\deg g < (d+1)/2$, then all terms in the right-hand-side of (10.1) have degrees less than or equal to $(4d-2)$ and since $G_1\, g^2$ also has degree less than or equal to this bound, so does $F_1 (f' + g' y_0)^2$. Hence, $\deg F_1 \leq 2$ and therefore F_1 is a polynomial in x_0 of degree (*as a function in $k(C)$*) at most 2.

Now, all terms of *odd* degree in equation (10.1) come from either $G_1 g^2$ or $\Psi(y_0^2 + g\, y_0) = g\, y_0^3 + \Psi(g\, y_0)$. Observe that every term of $\Psi(g y_0)$ has even degree, since every term of $g y_0$ has odd degree. So, the terms of highest odd degree in $G_1 g^2$ and $g y_0^3$ have to cancel out each other. Hence,

$$(3d - 2) + 2 \deg g = 3d + \deg g.$$

Thus, $\deg g = 2$.

$\square$

We now proceed to prove Proposition 6.8.

Proof of Proposition 6.8. We prove the proposition by induction on n. For $n = 1$, in order to have a lift modulo 4, F_1 and G_1 have to satisfy

$$G_1\, \lambda^2 + F_1\, (f')^2 = \dots,$$

where $\lambda \stackrel{\text{def}}{=} g \in k^\times$ and the omitted terms are the terms in the right hand side of equation (10.1), and therefore, have degrees less than or equal to $4d-1$. Since $\deg(f')^2 = 4d-4$, we can take F_1 to be *any* constant and obtain, from the above equation, G_1 with $\deg G_1 \leq 4d-1$. Thus, the bounds hold for $n = 1$.

Now suppose that the bounds for the G_i's in the statement hold for $i = 1, \dots, n$. Then $(y_0, G_1, \dots, G_n) \in U_n(e_n)$, where

$$e_n \stackrel{\text{def}}{=} d \left(\sum_{j=1}^{n} \frac{1}{j} \right) - \frac{1}{2},$$

since, for $i = 1, \dots, n$,

$$\deg G_i \leq 2^i \left(d + i \left(-\frac{1}{2} + d \cdot \sum_{j=1}^{i} \frac{1}{j} \right) \right) \leq 2^n \left(d + n \left(-\frac{1}{2} + d \cdot \sum_{j=1}^{n} \frac{1}{j} \right) \right) = 2^n (d + n\, e_n).$$

Since, clearly $(x_0, F_1, \ldots, F_n) \in U_n(e_n)$, by Lemma 7.5, to obtain a lift modulo 2^{n+2} we need to find F_{n+1} and G_{n+1} such that

$$G_{n+1}\,\lambda^{2^{n+1}} + F_{n+1}\,(f')^{2^{n+1}} = \ldots$$

where the omitted terms have degrees less then or equal to $2^{n+1}(2d + (n+1)\,e_n)$. Hence, we can take F_{n+1} to be any constant and find G_{n+1} with

$$\begin{aligned}\deg G_{n+1} \leq 2^{n+1}(2d + (n+1)\,e_n) &= 2^{n+1}\left(2d + (n+1)\left(-\frac{1}{2} + d\sum_{j=1}^{n}\frac{1}{j}\right)\right)\\ &= 2^{n+1}\left(d + (n+1)\left(-\frac{1}{2} + d\sum_{j=1}^{n+1}\frac{1}{j}\right)\right),\end{aligned}$$

which finishes the proof.

□

Finally, we prove Proposition 6.9.

Proof of Proposition 6.9. We shall use the same notation for $\boldsymbol{f}(\boldsymbol{x})$ and $\boldsymbol{g}(\boldsymbol{x})$ as in the proof of Proposition 6.6. We will also assume that $b_{0,1} = b_{1,1} = 0$, since we can always make a change of variables for $\boldsymbol{C}$ to have it that way.

Write,

$$G_1 = h_1 + h_2\,y_0,\ \ h_1, h_2 \in k[x_0].$$

To have $\deg G_1 \leq (3d-2)$, as in the statement, we need to find h_1 and h_2 such that $\deg h_1 \leq (3d-3)$ and $\deg h_2 = (2d-2)$.

Since $y_0^2 = x_0 y_0 + f(x_0)$ (in $k(C)$), we can rewrite equation (10.1) as

$$\begin{aligned}\left(x_0^2\,h_1 + F_1\,f + x_0^2\,f + f\left(\sum_{j=2}^{(d-1)/2} b_{j,1}x_0^{2j}\right) + F_1\,(f')^2 + \Psi(f) + \sum_{i=0}^{d-1} a_{i,1}x_0^{2i}\right) + \\ \left(x_0^2\,h_2 + x_0\,F_1 + x_0^3 + x_0\,f + x_0\left(\sum_{j=2}^{(d-1)/2} b_{j,1}x_0^{2j}\right)\right) y_0 = 0,\end{aligned}$$

and thus our goal is to find $a_{i,1}$'s, $b_{j,1}$'s (which will define $\boldsymbol{C}$) and F_1, h_1, h_2 (which will define ν) that satisfy this equation (and the requirements on the degrees of h_1, h_2 and F_1). Hence we need:

$$x_0^2\,h_1 + F_1\,f + x_0^2\,f + f\left(\sum_{j=2}^{(d-1)/2} b_{j,1}x_0^{2j}\right) + F_1\,(f')^2 + \Psi(f) + \sum_{i=0}^{d-1} a_{i,1}x_0^{2i} = 0 \qquad (10.3)$$

and

$$x_0^2\,h_2 + x_0\,F_1 + x_0^3 + x_0\,f + x_0\left(\sum_{j=2}^{(d-1)/2} b_{j,1}x_0^{2j}\right) = 0 \tag{10.4}$$

From the term in x_0 in equation (10.4), and since we want $F_1 \in k$, one immediately sees that we need $F_1 = a_{0,0}$, i.e., F_1 has to be the constant term of f. Hence, equation (10.4) has now only terms of power 2 or higher in x_0, and we can define

$$h_2 \stackrel{\text{def}}{=} \frac{f + a_{0,0}}{x_0} + x_0 + \sum_{j=2}^{(d-1)/2} b_{j,1}x_0^{2j-1}$$

for any choice of $b_{j,1}$'s that we might make. (Note that $\deg h_2 = (2d-2)$.)

We now try to find a suitable h_1. The constant term of equation (10.3) is $a_{0,0}^2 + a_{0,0}\,a_{1,0}^2 + a_{0,1}$, and thus we need to have $a_{0,1} \stackrel{\text{def}}{=} a_{0,0}^2 + a_{0,0}\,a_{1,0}^2$. Also, since the coefficient of the term in x_0 of $\Psi(f(x_0))$ is $a_{0,0}\,a_{1,0}$, our choice of F_1 makes the coefficient of the term in x_0 in (10.3) zero. Hence, let

$$\begin{aligned} f_1(x_0) &\stackrel{\text{def}}{=} \sum_{j=2}^{(d-1)/2} b_{j,1}x_0^{2j} \\ f_2(x_0) &\stackrel{\text{def}}{=} \sum_{i=2}^{2d-1} \alpha_i\,x_0^i \stackrel{\text{def}}{=} a_{0,0}f + x_0^2 f + a_{0,0}(f')^2 + \Psi(f). \end{aligned}$$

and one can now always have $h_1 \in k[x_0]$ that will satisfy equation (10.3) by taking

$$h_1 \stackrel{\text{def}}{=} \sum_{l=0}^{2d-3} \beta_l\,x_0^l \stackrel{\text{def}}{=} \frac{1}{x_0^2}\left(\sum_{i=0}^{d-1} a_{i,1}x_0^{2i} + f\,f_1 + f_2\right). \tag{10.5}$$

On the other hand, we need $\deg h_1 \leq (3d-3)$, and thus we must choose the $a_{i,1}$'s, for $i \geq 1$, and $b_{j,1}$'s, for $j \geq 2$, in such a way that $\beta_l = 0$ for all $l \geq (3d-1)/2$.

By choosing the $b_{j,1}$'s such that

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ a_{d-2,0} & 1 & 0 & \dots & 0 \\ a_{d-4,0} & a_{d-2,0} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{5,0} & a_{7,0} & a_{9,0} & \dots & 1 \end{pmatrix} \cdot \begin{pmatrix} b_{(d-1)/2,1} \\ b_{(d-3)/2,1} \\ b_{(d-5)/2,1} \\ \vdots \\ b_{2,1} \end{pmatrix} = \begin{pmatrix} \alpha_{2d-1} \\ \alpha_{2d-3} \\ \alpha_{2d-5} \\ \vdots \\ \alpha_{d+4} \end{pmatrix},$$

we obtain f_1 such that $(f\,f_1 + f_2)$ has no *odd* power of x_0 greater than $(d+2) \leq (3d+1)/2$. Since $\sum_{i=0}^{d-1} a_{i,1}x_0^{2i}$ has only even powers of x_0, this implies that $\beta_l = 0$ for all *odd* $l \geq (d+2)$.

If $d = 3$, then $(d+2) = (3d+1)/2 = 5$, and hence we have we have $\beta_l = 0$ for all odd $l \geq (3d-1)/2 = 4$. If $d > 3$, then $(d+2) \leq (3d-1)/2$, and we also have $\beta_l = 0$ for all odd $l \geq (3d-1)/2$.

Now, if we let

$$a_{i,1} \stackrel{\text{def}}{=} \text{coefficient of } x_0^{2i} \text{ in } (f\, f_1 + f_2),$$

(with f_1 chosen as above) for $i = \lfloor (3d-1)/4 \rfloor, \dots, (d-1)$ (note that $\lfloor (3d-1)/4 \rfloor \geq 2$), since $(2\lfloor (3d-1)/4 \rfloor - 2) \leq (3d-1)/2$, we obtain $\beta_l = 0$, for all *even* l such that $(3d-1)/2 \leq l \leq (2d-4)$.

Hence $\beta_l = 0$ for all $l \geq (3d-1)/2$, and thus $\deg h_1 \leq (3d-3)$.

□

If $d = 3$, i.e., if C is an *elliptic* curve, then the requirement that $g' = \lambda \in k^\times$ is equivalent to saying that $\deg g = 2$, which, by item 1 of Theorem 6.13, is a necessary and sufficient condition for elliptic curve to be ordinary. In this case, by Proposition 4.2 in [VW00], the construction described above actually gives us the elliptic Teichmüller lift and the canonical lifting of the elliptic curve (modulo 4). Hence, by following this procedure, one can easily reproduce the explicit formulas for the canonical lifting and elliptic Teichmüller lift (in characteristic 2) exhibited in [VW00].

11. Proofs About Lifting the Frobenius

In this section we prove Proposition 6.11 and Theorem 6.12. But, before we can prove Proposition 6.11, we shall need two simple lemmas.

Lemma 11.1. *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 will also use the following lemma:

Lemma 11.2. *Let C/k and $\boldsymbol{C}/\boldsymbol{W}(k)$ be curves given by equation* (3.1) *and* (3.3) *respectively and*

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

be a lift of points between their affine parts. Then

$$\begin{aligned} (f' + g'y_0)^2 \left(\left(x_0 + \frac{\partial F_1}{\partial x_0} \right) + \frac{f' + g'y_0}{g} \frac{\partial F_1}{\partial y_0} \right) + &\\ g^2 \left(\frac{\partial G_1}{\partial x_0} + \frac{f' + g'y_0}{g} \left(\frac{\partial G_1}{\partial y_0} + y_0 \right) \right) = 0 \quad &(11.1) \end{aligned}$$

Proof. By Theorem 4.1 in [Fin04],

$$\bar{\boldsymbol{\phi}}(\boldsymbol{x},\boldsymbol{y}) \stackrel{\text{def}}{=} (\boldsymbol{x}^2 + 2\boldsymbol{F}_1, \boldsymbol{y}^2 + 2\boldsymbol{G}_1) \tag{11.2}$$

is a well defined lift of the Frobenius modulo 4. Since

$$\frac{1}{2}\bar{\boldsymbol{\phi}}^*(\boldsymbol{\omega}^\sigma) = \frac{1}{2}\bar{\boldsymbol{\phi}}^*\left(\frac{d\boldsymbol{x}}{2\boldsymbol{y}+\boldsymbol{g}^\sigma}\right) = \frac{1}{2}\bar{\boldsymbol{\phi}}^*\left(\frac{d\boldsymbol{y}}{(\boldsymbol{f}')^\sigma - (\boldsymbol{g}')^\sigma\boldsymbol{y}}\right),$$

using equation (11.2), the reduction the equation above modulo 2 gives us

$$\frac{dF_1 + x_0dx_0}{g^2} = \frac{dG_1 + y_0dy_0}{(f' + g'y_0)^2}.$$

Since $dy_0 = (f' + g'y_0)dx_0/g$, equation (11.1) follows. ☐

We now can prove Proposition 6.11.

Proof of Proposition 6.11. We first prove that the condition is necessary. Assume we have a lift of the Frobenius associated to ν. By Theorem 4.1 in [Fin04], it must have the form

$$\boldsymbol{\phi}(\boldsymbol{x},\boldsymbol{y}) = (\boldsymbol{x}^2 + 2\boldsymbol{F}_1 + 4\boldsymbol{P}, \boldsymbol{y}^2 + 2\boldsymbol{G}_1 + 4\boldsymbol{Q}),$$

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

Let δ be the 2-derivation associated to $\boldsymbol{\phi}$ (as in [Bui96]):

$$\delta\boldsymbol{u} \stackrel{\text{def}}{=} \frac{\boldsymbol{\phi}^*\boldsymbol{u}^\sigma - \boldsymbol{u}^2}{2}.$$

We then have

$$\delta\boldsymbol{x} = \boldsymbol{F}_1 + 2\boldsymbol{P}$$

and, using Lemma 11.1,

$$\begin{aligned}\delta^2\boldsymbol{x} &= \frac{(\boldsymbol{F}_1 + 2\boldsymbol{P})^\sigma \circ \boldsymbol{\phi} - (\boldsymbol{F}_1 + 2\boldsymbol{P})^2}{2} \\ &= \frac{\boldsymbol{F}_1^\sigma(\boldsymbol{x}^2,\boldsymbol{y}^2) - \boldsymbol{F}_1^2}{2} + \frac{\partial {\boldsymbol{F}_1}^\sigma}{\partial \boldsymbol{x}}(\boldsymbol{x}^2,\boldsymbol{y}^2)\cdot\boldsymbol{F}_1 + \frac{\partial {\boldsymbol{F}_1}^\sigma}{\partial \boldsymbol{y}}(\boldsymbol{x}^2,\boldsymbol{y}^2)\cdot\boldsymbol{G}_1 + \\ &\quad \boldsymbol{P}^\sigma(\boldsymbol{x}^2,\boldsymbol{y}^2) + 2\cdot(\dots).\end{aligned} \tag{11.3}$$

But, by Lemma 2.6 of [Bui96], the reduction modulo 2 of $\delta^2\boldsymbol{x}$ must be equal to $F_2 + x_0^2F_1 + F_1^2$. Also, since the reduction modulo 2 of $\boldsymbol{P}^\sigma(\boldsymbol{x}^2,\boldsymbol{y}^2)$ is clearly a square, say P^2, and $\boldsymbol{F}_1$ is the Teichmüller lift of F_1, reducing equation (11.3) modulo 2, we obtain

$$F_2 + x_0^2F_1 + F_1^2 = \Psi(F_1) + \left(\frac{\partial F_1}{\partial x_0}\right)^2 F_1 + \left(\frac{\partial F_1}{\partial y_0}\right)^2 G_1 + P^2. \tag{11.4}$$

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

$$G_2 + y_0^2G_1 + G_1^2 = \Psi(G_1) + \left(\frac{\partial G_1}{\partial x_0}\right)^2 F_1 + \left(\frac{\partial G_1}{\partial y_0}\right)^2 G_1 + Q^2,$$

and hence, the condition is necessary.

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

$$\begin{array}{ccc} \boldsymbol{U}(\boldsymbol{W}_3(\bar{k})) & \xrightarrow{\boldsymbol{\phi}} & \boldsymbol{U}^{\sigma}(\boldsymbol{W}_3(\bar{k})) \\ {\scriptstyle \nu}\big\uparrow & & \big\uparrow{\scriptstyle \nu^{\sigma}} \\ U(\bar{k}) & \xrightarrow{\phi} & U^{\sigma}(\bar{k}) \end{array} \tag{11.5}$$

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

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

we write

$$\boldsymbol{h}(\boldsymbol{x}, \boldsymbol{y}) = (h_0(x_0, y_0), h_1(x_0, x_1, y_0, y_1), h_2(x_0, x_1, x_2, y_0, y_1, y_2)).$$

Then, to prove that $\boldsymbol{\phi}$ is well defined, it suffices to prove that $\boldsymbol{\phi}^* h_i^{\sigma} \in I$, for $i = 0, 1, 2$, where $I \stackrel{\text{def}}{=} (h_0, h_1, h_2)$.

By Theorem 4.1 of [Fin04], we have that $\boldsymbol{\phi}^* h_0^{\sigma}, \boldsymbol{\phi}^* h_1^{\sigma} \in I$. So we just need to show that $\boldsymbol{\phi}^* h_2^{\sigma} \in I$.

One has

$$\boldsymbol{x}^2 = (x_0, x_1, x_2)^2 = (x_0^2, 0, x_0^4\, x_1^2 + x_1^4).$$

Also, by Lemma 7.6, and noticing that $\boldsymbol{F}_1$ is the *Teichmüller* lift of F_1,

$$2\boldsymbol{F}_1 = \left(0, F_1^2, x_1^2 \left(\frac{\partial F_1}{\partial x_0}\right)^4 + y_1^2 \left(\frac{\partial F_1}{\partial y_0}\right)^4 + \Psi(F_1)^2\right).$$

Hence, if $\boldsymbol{P}$ is as in the statement,

$$\boldsymbol{x}^2 + 2\boldsymbol{F}_1 + 4\boldsymbol{P} = \left(x_0^2, F_1^2, F_2^2 + \mathfrak{X}_2^2\right), \tag{11.6}$$

where,

$$\mathfrak{X}_2 \stackrel{\text{def}}{=} (x_1 + F_1)\left(x_0 + \frac{\partial F_1}{\partial x_0}\right)^2 + (y_1 + G_1)\left(\frac{\partial G_1}{\partial y_0}\right)^2 + (x_1 + F_1)^2,$$

and in a similar manner,

$$\boldsymbol{y}^2 + 2\boldsymbol{G}_1 + 4\boldsymbol{Q} = \left(y_0^2, G_1^2, G_2^2 + \mathfrak{Y}_2^2\right), \tag{11.7}$$

where

$$\mathfrak{Y}_2 \stackrel{\text{def}}{=} (x_1 + F_1)\left(\frac{\partial G_1}{\partial x_0}\right)^2 + (y_1 + G_1)\left(y_0 + \frac{\partial G_1}{\partial y_0}\right)^2 + (y_1 + G_1)^2.$$

Note that, by Lemma 7.4,

$$h_2^{\sigma} = (g^{\sigma})^4\, y_2 + ((f')^{\sigma} + (g')^{\sigma} y_0)^4\, x_2 + \dots,$$

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

$$\boldsymbol{\phi}^* h_2^{\sigma} = g^8\, (G_2 + \mathfrak{Y}_2)^2 + (f' + g' y_0)^8\, (F_2 + \mathfrak{X}_2)^2 + \dots. \tag{11.8}$$

Since

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

is a (well defined) lift,

$$g^8\, G_2^2 + (f' + g' y_0)^8\, F_2^2 + \cdots \equiv 0 \pmod{(h_0)},$$

where the omitted terms are the same as the ones in formula (11.8). Therefore

$$\phi^* h_2^\sigma \equiv g^8\, \mathcal{Y}_2^2 + (f' + g' y_0)^8\, \mathcal{X}_2^2 \pmod{I},$$

and it suffices to prove that

$$g^4\, \mathcal{Y}_2 + (f' + g' y_0)^4\, \mathcal{X}_2 \equiv 0 \pmod{I},$$

or,

$$\begin{aligned}(x_1 + F_1)\left((f' + g' y_0)^2 \left(x_0 + \frac{\partial F_1}{\partial x_0}\right) + g^2\, \frac{\partial G_1}{\partial x_0}\right)^2 + \\ (y_1 + G_1)\left((f' + g' y_0)^2\, \frac{\partial F_1}{\partial y_0} + g^2 \left(y_0 + \frac{\partial G_1}{\partial y_0}\right)\right)^2 + \\ \left((x_1 + F_1)(f + g' y_0)^2 + (y_1 + G_1)\, g^2\right)^2 \equiv 0 \pmod{I}.\end{aligned}$$

Applying Lemma 11.2, this equation becomes

$$\begin{aligned}\left((x_1 + F_1)\frac{(f' + g' y_0)^2}{g^2} + (y_1 + G_1)\right)\left((f' + g' y_0)^2\, \frac{\partial F_1}{\partial y_0} + g^2 \left(y_0 + \frac{\partial G_1}{\partial y_0}\right)\right)^2 + \\ \left((x_1 + F_1)(f + g' y_0)^2 + (y_1 + G_1)\, g^2\right)^2 \equiv 0 \pmod{I}.\end{aligned}$$

Thus, it is enough to prove that

$$(x_1 + F_1)(f' + g' y_0)^2 + (y_1 + G_1)\, g^2 \equiv 0 \pmod{I}.$$

But $h_1, \nu^* h_1 \equiv 0 \pmod{I}$, and then

$$\begin{aligned}h_1(x_0, x_1, y_0, y_1) + h_1(x_0, F_1, y_0, G_1) = \\ (x_1 + F_1)(f' + g' y_0)^2 + (y_1 + G_1)\, g^2 \equiv 0 \pmod{I},\end{aligned}$$

which finishes the proof that ϕ is well defined.

Finally, equations (11.6) and (11.7) show the diagram (11.5) commutes, since $\nu^* \mathcal{X}_2 = \nu^* \mathcal{Y}_2 = 0$.

□

With Proposition 6.11 we can now prove Theorem 6.12.

Proof of Theorem 6.12. By Proposition 9.1, we have

$$dG_1 = \big(h\,(f' + g'y_0) + y_0\big)\,dy_0, \tag{11.9}$$

$$dG_2 = \big(h^3\,(f' + g'y_0)^3 + y_0^3\big)\,dy_0 + G_1\,dG_1. \tag{11.10}$$

Moreover, by equation (3.2), $dF_1 = (h\,g + x_0)\,dx_0$ implies that

$$\frac{\partial F_1}{\partial x_0} + \frac{\partial F_1}{\partial y_0}\frac{f' + g'y_0}{g} = h\,g + x_0, \tag{11.11}$$

and equation (11.9) implies that

$$\frac{\partial G_1}{\partial x_0}\frac{g}{f' + g'y_0} + \frac{\partial G_1}{\partial y_0} = h\,(f' + g'y_0) + y_0. \tag{11.12}$$

Now, to prove the theorem, by Proposition 6.11, it suffices to prove that

$$d\left(F_2 + x_0^2\,F_1 + \Psi(F_1) + \left(\frac{\partial F_1}{\partial x_0}\right)^2 F_1 + \left(\frac{\partial F_1}{\partial y_0}\right)^2 G_1\right) =$$

$$dF_2 + x_0^2\,dF_1 + d(\Psi(F_1)) + \left(\frac{\partial F_1}{\partial x_0}\right)^2 dF_1 + \left(\frac{\partial F_1}{\partial y_0}\right)^2 dG_1 = 0 \tag{11.13}$$

and

$$d\left(G_2 + y_0^2\,G_1 + \Psi(G_1) + \left(\frac{\partial G_1}{\partial x_0}\right)^2 F_1 + \left(\frac{\partial G_1}{\partial y_0}\right)^2 G_1\right) =$$

$$dG_2 + y_0^2\,dG_1 + d(\Psi(G_1)) + \left(\frac{\partial G_1}{\partial x_0}\right)^2 dF_1 + \left(\frac{\partial G_1}{\partial y_0}\right)^2 dG_1 = 0 \tag{11.14}$$

Since

$$d(\Psi(F_1)) = x_0\left(\frac{\partial F_1}{\partial x_0}\right)^2 dx_0 + y_0\left(\frac{\partial F_1}{\partial y_0}\right)^2 dy_0 + F_1 dF_1, \tag{11.15}$$

using the formulas for dF_1 and dF_2 (in the statement), together with equations (11.9) and (3.2), equation (11.13) reduces to

$$h\,g\left(h\,g + x_0 + \frac{\partial F_1}{\partial x_0} + \frac{\partial F_1}{\partial y_0}\frac{f' + g'y_0}{g}\right)^2 dx_0 = 0, \tag{11.16}$$

which immediately follows from equation (11.11).

We prove that equation (11.14) holds in a similar fashion. Using the formula for dF_1, equations (11.9), (11.10) and (3.2), and the analogue to equation (11.15) for $\Psi(G_1)$, a tedious computation shows that equation (11.14) reduces to

$$h\,(f' + g'y_0)\left(h\,(f' + g'y_0) + y_0 + \frac{\partial G_1}{\partial x_0}\frac{g}{f' + g'y_0} + \frac{\partial G_1}{\partial y_0}\right)^2 dy_0 = 0,$$

which immediately follows from equation (11.12). Hence (11.14) also holds.

To finish the proof, it suffices to show now that if either $\deg F_n = 0$ or if $\deg G_n = 2^{n+1}(d-1)-(d-2)$, for $n=1,2$, then there exists $h \in k(C)$ such that

$$dF_1 = (h\,g + x_0)\,dx_0,$$
$$dF_2 = (h^3\,g^3 + x_0^3)\,dx_0 + F_1\,dF_1.$$

If $\deg F_1 = \deg F_2 = 0$, then $dF_1 = dF_2 = 0$. Moreover, by Theorem 6.7, either $g = \lambda$ or $g = \lambda\,x_0$, for some $\lambda \in k^{\times}$. Thus, take $h = \lambda^{-1} x_0$ if $g = \lambda$, or $h = \lambda^{-1}$ if $g = \lambda\,x_0$.

Finally, if $\deg G_n = 2^{n+1}(d-1)-(d-2)$, for $n = 1,2$, then, by Theorem 6.5,

$$dG_1 = \lambda^{-1}(f' + g'y_0)\,dy_0 + y_0 dy_0,$$
$$dG_2 = (\lambda^{-3}(f' + g'y_0)^3 + y_0^3) dy_0 + G_1\,dG_1,$$

where λ is the (non-zero) coefficient of x_0 in g. By Proposition 9.1,

$$dF_1 = (\lambda^{-1}\,g + x_0)\,dx_0,$$
$$dF_2 = (\lambda^{-3}\,g^3 + x_0^3)\,dx_0 + F_1\,dF_1.$$

Hence, we just take $h = \lambda^{-1}$.

□

12. The Genus 2 Case

In this section we will do some explicit calculations with curves of genus two (i.e., $d = 5$). Besides illustrating the theory with a concrete example, another goal here is to show how the condition that $g = x_0$ seems to be sufficient to obtain a lift of points with the degrees of the G_n's equal to the lower bounds. Note that, by Proposition 6.6, it is necessary only to have $\deg g = 2$, but we further choose to have $g = x_0$ so that we can also obtain minimal degree for F_1, as in Proposition 6.9. (Observe that the condition $g = x_0$ makes the Jacobian of C non-ordinary.)

Let

$$C/k \;:\; y_0^2 + x_0 y_0 = x_0^5 + d_0 x_0^4 + e_0 x_0^3 + f_0 x_0^2 + g_0 x_0 + h_0. \tag{12.1}$$

Since computations in such generality would be too long, we first simplify, via isomorphisms, equation (12.1). Note that, as observed earlier, the degrees are not necessarily invariant under isomorphisms!

An isomorphism of curves of genus 2 that preserve the point at infinity is given by a change of variables of the form

$$\tilde{x}_0 \mapsto \alpha^2 x_0 + \beta, \tag{12.2}$$
$$\tilde{y}_0 \mapsto \alpha^5 y_0 + \gamma x_0^2 + \delta x_0 + \epsilon, \tag{12.3}$$

where $\alpha, \beta, \gamma, \delta, \epsilon \in k$ and $\alpha \neq 0$. Therefore, clearly if

$$\tilde{C}/k \;:\; \tilde{y}_0^2 + (\tilde{a}_0 x_0^2 + \tilde{b}_0 x_0 + \tilde{c}_0)\tilde{y}_0 = \tilde{x}_0^5 + \tilde{d}_0 \tilde{x}_0^4 + \tilde{e}_0 \tilde{x}_0^3 + \tilde{f}_0 \tilde{x}_0^2 + \tilde{g}_0 \tilde{x}_0 + \tilde{h}_0 \tag{12.4}$$

is isomorphic to C, then $\tilde{a}_0 = 0$, and again we can make $\tilde{b}_0 = 1$ and $\tilde{c}_0 = 0$. Hence, in order for two isomorphic curves have this same form (i.e., $g = x_0$), we must have $\beta = 0$ and α must be a cubic root of unity. A tedious computation gives us:

$$\begin{aligned}
\tilde{d}_0 &= \alpha\gamma^2 + \alpha^2 d_0;\\
\tilde{e}_0 &= \alpha^2\gamma + \alpha e_0;\\
\tilde{f}_0 &= \alpha\delta + \alpha^2\delta^2 + f_0;\\
\tilde{g}_0 &= \epsilon + \alpha^2 g_0;\\
\tilde{h}_0 &= \epsilon^2 + \alpha h_0.
\end{aligned}$$

Comparing the equations for $\tilde{d}_0$ and $\tilde{e}_0$, we obtain

$$\gamma = (\alpha d_0 + \alpha^2 \tilde{d}_0)^{1/2} = \alpha^2 e_0 + \alpha \tilde{e}_0, \tag{12.5}$$

and comparing the equations for $\tilde{g}_0$ and $\tilde{h}_0$, we obtain

$$\epsilon = (\alpha h_0 + \tilde{h}_0)^{1/2} = \alpha^2 g_0 + \tilde{g}_0. \tag{12.6}$$

Observe that the curves are non-singular if, and only if, $\Delta \stackrel{\text{def}}{=} g_0^2 + h_0$ and $\tilde{\Delta} \stackrel{\text{def}}{=} \tilde{g}_0^2 + \tilde{h}_0$ are non-zero. But equations (12.5) and (12.6) imply

$$\begin{gathered}
\tilde{d}_0 + \tilde{e}_0^2 = \alpha^2(d_0 + e_0^2),\\
\tilde{\Delta} = \alpha\Delta
\end{gathered}$$

Therefore, clearly

$$j_1 \stackrel{\text{def}}{=} \frac{d_0 + e_0^2}{\Delta^2} = \frac{\tilde{d}_0 + \tilde{e}_0^2}{\tilde{\Delta}^2}$$

and

$$j_2 \stackrel{\text{def}}{=} \Delta^3 = \tilde{\Delta}^3$$

(remember that α is cubic root of unity) are invariants for curves of this particular form.

Conversely, if we have curves C and $\tilde{C}$ given by equations (12.1) and (12.4), with $\tilde{a}_0 = 0$, $\tilde{b}_0 = 1$ and $\tilde{c}_0 = 0$, such that

$$\frac{d_0 + e_0^2}{\Delta^2} = \frac{\tilde{d}_0 + \tilde{e}_0^2}{\tilde{\Delta}^2}$$

and

$$\Delta^3 = \tilde{\Delta}^3,$$

then the curves are isomorphic, either over k itself or over a degree two extension of k: just let (as in equations (12.2) and (12.3)):

$$\begin{aligned}
\alpha &\stackrel{\text{def}}{=} \tilde{\Delta}/\Delta \\
\beta &\stackrel{\text{def}}{=} 0 \\
\gamma &\stackrel{\text{def}}{=} \alpha^2 e_0 + \alpha \tilde{e}_0 \\
\delta &\stackrel{\text{def}}{=} \text{a solution of } \alpha^2 X^2 + \alpha X + (f_0 + \tilde{f}_0) = 0 \\
\epsilon &\stackrel{\text{def}}{=} \alpha^2 g_0 + \tilde{g}_0.
\end{aligned}$$

Hence, the invariants $j_1, j_2 \in k$, with $j_2 \neq 0$, determine a curve of genus 2 with $g = x_0$ up to isomorphism, and given such any $j_1, j_2 \in k$, with $j_2 \neq 0$, the curve

$$y_0^2 + x_0 y_0 = x_0^5 + ((j_1 j_2^{2/3})^{1/2}) x_0^3 + j_2^{1/3}$$

is isomorphic (over $\bar{k}$) to a curve with invariants j_1 and j_2. So, we will consider here only curves given by equations of the form

$$y_0^2 + x_0 y_0 = x_0^5 + e_0 x_0^3 + h_0$$

(with $h_0 \neq 0$). The computation, up to the fourth coordinate of the Witt vectors, of the absolute minimal degree lifting with respect to $\boldsymbol{y}$ for a curve given by the above equation yields a lifting (over $\boldsymbol{W}_4(k)$) given by

$$\boldsymbol{C}/\boldsymbol{W}_4(k) \ : \ \boldsymbol{y}^2 + (\boldsymbol{a}\boldsymbol{x}^2 + \boldsymbol{x})\boldsymbol{y} = \boldsymbol{x}^5 + \boldsymbol{d}\boldsymbol{x}^4 + \boldsymbol{e}\boldsymbol{x}^3 + \boldsymbol{f}\boldsymbol{x}^2 + \boldsymbol{g}\boldsymbol{x} + \boldsymbol{h},$$

where $\boldsymbol{a} = (a_0, a_1, a_2, a_3), \dots, \boldsymbol{h} = (h_0, h_1, h_2, h_3)$, are given by

$$\begin{aligned}
\boldsymbol{a} &= (0, 0, e_0 + e_1^2 + h_0, a_3), \\
\boldsymbol{d} &= (0, e_0 + h_0, d_2, d_3), \\
\boldsymbol{e} &= (e_0, e_1, e_2, e_3), \\
\boldsymbol{f} &= (0, f_1, f_2, f_3), \\
\boldsymbol{g} &= (0, g_1, g_2, g_3), \\
\boldsymbol{h} &= (h_0, h_0^2, g_1 + h_0^4, g_1^4 h_0^4 + h_0^8 + f_1^4 h_0^8),
\end{aligned}$$

with $a_3, d_2, d_3, e_1, e_2, e_3, f_1, f_2, f_3, g_1, g_2, g_3 \in k$ arbitrary, and a lift of points is given by

$$\nu(x_0, y_0) = ((x_0, F_1, F_2, F_3), (y_0, G_1, G_2, G_3)),$$

where $F_1 \in k$ (in fact, $F_1 = h_0$, as in section 10), $\deg G_1 = 13$, $\deg F_2 = 20$, $\deg G_2 = 29$, $\deg F_3 = 28$ and $\deg G_3 = 61$, and hence, for $i = 0, \dots, 3$, $\deg G_i = (2^{i+3} - 3)$, i.e., the G_i's have the minimal possible degrees.

It seems worth mentioning that if we just want the lift with minimal degrees modulo 4, then you do not need $d_1 = e_0 + h_0$ as in the formulas above. In this case d_1 could be arbitrary. The condition on d_1 is imposed so that we are able to obtain G_2 with order 29. In the same way, if you only want the minimal degrees modulo 8, you can have any $a_2 \in k$, but if you want $\deg G_3 = 61$, then you have to impose the condition that $a_2 = a_0 + e_1^2 + h_0$ as above. So, to obtain $\deg G_4 = 125$, if at all possible, one might have to impose conditions on the constants left as arbitrary here.

Also, observe that, without extra conditions, the lifting of the curve is not unique up to isomorphisms!

As stated in Theorem 6.13, similar computations with ordinary elliptic curves (genus 1) show we can also obtain lifts of points with the degrees of G_i's equal to the lower bound. It seems then that the condition $g = x_0$ might also to be sufficient to have a lift with G_i's having degrees equal to the lower bounds.

13. Examples of Codes

In this section we exhibit some codes constructed with liftings of hyperelliptic curves. We will deal only with the case when the characteristic of the field and the length of the Witt vectors are both 2, i.e., when, with the notation of section 2, $p^l = 4$. (Also, as observed before, we consider only divisors of the form $n\boldsymbol{P}_\infty$.) It is worth noticing that a few examples for genus 1 were computed by Voloch and Walker in [VW00].

Let $q = 8$ and $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, where $\alpha^3 + \alpha + 1 = 0$. Consider the curve

$$C \,:\, y_0^2 + y_0 = x_0^5 + x_0^3 + x_0,$$

with lifting

$$\boldsymbol{C} \,:\, \boldsymbol{y}^2 + ((0,1)\boldsymbol{x}^2 + (0,1)\boldsymbol{x} + (1,1))\boldsymbol{y} = \boldsymbol{x}^5 + (1,1)\boldsymbol{x}^3 + (1,0)\boldsymbol{x},$$

and the minimal degree lift of points from C to $\boldsymbol{C}$ with respect to $\boldsymbol{y}$

$$\begin{aligned} F_1 &= x_0 + 1, \\ G_1 &= x_0^5\, y_0 + x_0^4\, y_0 + x_0^3\, y_0 + x_0^2\, y_0 + x_0\, y_0 + x_0^5 + x_0^3 + x_0 + 1. \end{aligned}$$

(Observe that, in this case, $\boldsymbol{C}$ is not an absolute minimal degree curve over C, so ν is not an *absolute* minimal degree lift of points.)

Then, considering functions in $\mathcal{L}(5\boldsymbol{P}_\infty)$ and following the procedure described in section 2, one obtains a code with the following generating matrix (over $\mathbb{Z}/4$):

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 3 & 0 & 3 \\ 0 & 1 & 0 & 0 & 3 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 3 & 0 & 3 & 1 \\ 0 & 0 & 0 & 1 & 0 & 3 & 3 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix},$$

The corresponding binary code has length 16, 2^{11} codewords and minimum weight 4. According to N. Sloane's site,

`http://www.research.att.com/~njas/codes/And/`,

this is the size of the largest possible *non-linear* binary code with this length and minimum distance. Note also that, in this particular case, there is a *linear* code with the same parameters.

One can also use only a few functions in $\mathcal{L}(n\boldsymbol{P}_\infty)$ (for some fixed n) to generate the code instead of all functions. We were then able to find a few codes matching the best known *linear* code for a fixed length and size. For example, again over $\mathbb{F}_8$, consider the curve

$$C \;:\; y_0^2 + \alpha^6\, x_0\, y_0 = x_0^5 + \alpha^2\, x_0^4 + \alpha^4\, x_0^2 + \alpha^5$$

with lifting

$$\boldsymbol{C} \;:\; \boldsymbol{y}^2 + (\alpha^6, 0)\boldsymbol{x}\,\boldsymbol{y} = \boldsymbol{x}^5 + (\alpha^2, \alpha)\boldsymbol{x}^4 + (\alpha^4, 0)\boldsymbol{x}^2 + (\alpha^5, \alpha^5),$$

and the minimal degree lift of points from C to $\boldsymbol{C}$ with respect to $\boldsymbol{y}$ (which turns out to be also a minimal degree lift with respect to $\boldsymbol{x}$ in this case) given by

$$\begin{aligned} F_1 &= x_0\, y_0 + \alpha^3\, x_0^3 + x_0^2 + \alpha^2, \\ G_1 &= (\alpha^2\, x_0^7 + \alpha^3\, x_0^4 + \alpha^5\, x_0^3 + \alpha^2\, x_0^2 + \alpha^4\, x_0)\, y_0 + \\ &\qquad \alpha^5\, x_0^9 + \alpha^2\, x_0^8 + \alpha^4\, x_0^7 + \alpha^4\, x_0^6 + \alpha^5\, x_0^5 + \alpha^2\, x_0^3 + x_0^2 + \alpha\, x_0 + \alpha^6. \end{aligned}$$

If we now use only the functions of the form

$$\boldsymbol{h} = \boldsymbol{c}_0 + \boldsymbol{c}_1\, \boldsymbol{x} + \boldsymbol{c}_2\, \boldsymbol{y}, \quad \boldsymbol{c}_0, \boldsymbol{c}_1, \boldsymbol{c}_2 \in \boldsymbol{W}_2(\mathbb{F}_8)$$

in the construction of the code (so we discard functions in $\mathcal{L}(5\boldsymbol{P}_\infty)$ involving $\boldsymbol{x}^2$), then we obtain the generating matrix

$$\begin{pmatrix} 1&0&0&0&0&0&0&1&3&1&2&1&2\\ 0&1&0&0&0&0&0&3&0&2&0&1&3\\ 0&0&1&0&0&0&0&3&1&0&3&1&1\\ 0&0&0&1&0&0&0&1&1&2&2&0&0\\ 0&0&0&0&1&0&0&2&1&0&3&0&3\\ 0&0&0&0&0&1&0&2&2&3&2&1&1\\ 0&0&0&0&0&0&1&1&1&1&1&1&3 \end{pmatrix},$$

and the resulting binary code has length 26, 2^{14} codewords and minimum weight 6, which according to A. Browuer's web site

`http://www.win.tue.nl/~aeb/voorlincod.html`,

is the minimum weight of the best known *linear* code with that size and length. (The size of the best non-linear code with this length and minimum weight is 2^{15}.)

Finally, one can also use the results from the previous section, where we computed *absolute* minimal degree liftings, to construct codes. If we have, again over $\mathbb{F}_8$,

$$C \;:\; y_0^2 + x_0\,y_0 = x_0^5 + \alpha^2\,x_0^3 + \alpha^6,$$

then an absolute minimal degree curve modulo 4 over C, with respect to both $\boldsymbol{x}$ and $\boldsymbol{y}$, is given by (as in the previous section)

$$\boldsymbol{C} \;:\; \boldsymbol{y}^2 + \boldsymbol{x}\,\boldsymbol{y} = \boldsymbol{x}^5 + (0,\alpha^5)\boldsymbol{x}^4 + (\alpha^2,1)\boldsymbol{x}^3 + (0,1)\boldsymbol{x}^2 + (0,1)\boldsymbol{x} + (\alpha^6,\alpha^5),$$

and we have an absolute minimal degree lift of points

$$\begin{aligned} F_1 &= \alpha^6,\\ G_1 &= (x_0^4 + \alpha^2\,x_0^2 + x_0)\,y_0 + \alpha^4\,x_0^6 + x_0^5 + x_0^4 + \alpha^2\,x_0^3 + \alpha\,x_0^2 + \alpha^2. \end{aligned}$$

(Observe that the proof of Proposition 6.9 gives us a method to explicitly find $\boldsymbol{C}$, F_1 and G_1.) Using again only functions generated by $\{1, \boldsymbol{x}, \boldsymbol{y}\}$, one obtains the code given by the generating matrix

$$\begin{pmatrix} 1&0&0&0&0&0&0&2&2&3&1\\ 0&1&0&0&0&0&0&1&1&0&3\\ 0&0&1&0&0&0&0&1&2&0&1\\ 0&0&0&1&0&0&0&1&0&1&3\\ 0&0&0&0&1&0&0&1&1&3&1\\ 0&0&0&0&0&1&0&1&0&0&2\\ 0&0&0&0&0&0&1&2&3&2&2 \end{pmatrix}.$$

This code has then length 22, 2^{14} codewords and minimum weight 4, which is the minimum weight for the best linear code with this length and size. (The largest non-linear code with the same length and minimum weight is $9 \cdot 2^{13}$.)

Acknowledgement. The computations mentioned in this paper were made with either Magma or Mathematica, and the author would like to thank J. Cannon for his invaluable help with the use of Magma in the computations of the parameters of the obtained codes and J. Walker for her helpful comments on the results.

References

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

[Car98] Claude Carlet. $\mathbb{Z}_{2^k}$-linear codes. *IEEE Trans. Inform. Theory*, 44(4):1543–1547, 1998.

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

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

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

[Har77] R. Hartshorne. *Algebriac Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[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.

[Sil85] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1985.

[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.

[Wal99] J. L. Walker. Algebraic geometric codes over rings. *J. Pure Appl. Algebra*, 144(1):91–110, 1999.

Department of Mathematics, Ohio State University, Columbus, OH – 43210
E-mail address: finotti@math.ohio-state.edu