5-2023

Computational Aspects of Mixed Characteristic Witt Vectors and Denominators in Canonical Liftings of Elliptic Curves

Jacob Dennerlein

University of Tennessee, Knoxville, jdennerl@vols.utk.edu

To the Graduate Council:

I am submitting herewith a dissertation written by Jacob Dennerlein entitled "Computational Aspects of Mixed Characteristic Witt Vectors and Denominators in Canonical Liftings of Elliptic Curves." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Luís R. A. Finotti, Major Professor

We have read this dissertation and recommend its acceptance:

Marie Jameson, Shashikant Mulay, Michael W. Berry

Accepted for the Council:

Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Computational Aspects of Mixed Characteristic Witt Vectors and Denominators in Canonical Liftings of Elliptic Curves

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Jacob Dennerlein

May 2023

Acknowledgments

I would first like to thank Dr. Luís Finotti for his guidance and suggestions throughout this grueling process and for spending so much of his time listening to my ramblings and reviewing my writing. I would also like to thank Dr. Christopher Davis for reviewing some of my work and pointing me in the direction of relevant results. Finally, I'd like to thank my doctoral committee, Dr. Marie Jameson, Dr. Shashikant Mulay, and Dr. Michael Berry, for their input and questions.

To Mom, Dad, and Lyle, thank you for your unwavering support through this long journey. I'm so thankful to have you all in my life. To my friends Kelly, Jesse, Alec, Carson, and many others: thank you for being there when I needed and keeping me sane. I couldn't have done this without any of you and I am eternally grateful.

Abstract

Given an ordinary elliptic curve E over a field $\Bbbk$ of characteristic p, there is an elliptic curve $\boldsymbol{E}$ over the Witt vectors $\boldsymbol{W}(\Bbbk)$ for which we can lift the Frobenius morphism, called the canonical lifting of E. The Weierstrass coefficients and the elliptic Teichmüller lift of $\boldsymbol{E}$ are given by rational functions over $\mathbb{F}_p$ that depend only on the coefficients and points of E. Finotti studied the properties of these rational functions over fields of characteristic $p \geq 5$. We investigate the same properties for fields of characteristic 2 and 3, make progress on some conjectures of Finotti, and introduce some conjectures of our own. We also investigate the structure of rings of Witt vectors over arbitrary commutative rings and give a computationally useful isomorphism for Witt vectors over $\mathbb{Z}/p^\alpha\mathbb{Z}$ [alpha].

Table of Contents

List of Tables

Chapter 1

Preliminaries

1.1 Introduction

Let $\Bbbk$ be a perfect field of characteristic $p > 0$ and let $E/\Bbbk$ be an elliptic curve. We begin with two definitions.

Definition 1.1. We say that E is *ordinary* if it has non-trivial p-torsion. Otherwise we say E is *supersingular*.

Definition 1.2. Suppose the characteristic of $\Bbbk$ is not 2 and let $E/\Bbbk$ be given by

$$E/\Bbbk : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Then the *Hasse invariant* of E is the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$. We can also define the Hasse invariant if $\mathrm{char}(\Bbbk) = 2$. See Section 2.1.

This leads us to the following proposition, which we will not prove. See Chapter V Section 4 of [Sil86] for more details.

Proposition 1.3. *E is supersingular if and only if the Hasse invariant of E is* 0*.*

Note. This is the only sense in which the Hasse invariant is actually an *invariant*. Isomorphic ordinary curves with different Weierstrass equations can have different Hasse invariants. When necessary, we will fix a Weierstrass form to avoid this ambiguity.

With the above definitions in hand, we can define the main objects of interest for the next two chapters.

Definition 1.4. Associated to an *ordinary* elliptic curve E over $\Bbbk$, there exists a unique (up to isomorphism) elliptic curve $\boldsymbol{E}$ over $\boldsymbol{W}(\Bbbk)$, the ring of Witt vectors over $\Bbbk$, called the *canonical lifting* of E, and a map $\tau : E(\Bbbk) \to \boldsymbol{E}(\boldsymbol{W}(\Bbbk))$, i.e., a *lift of points*, called the *elliptic Teichmüller lift*, characterized by the following properties:

1. The reduction modulo p of $\boldsymbol{E}$ is E.

2. If σ denotes the Frobenius of both $\Bbbk$ and $\boldsymbol{W}(\Bbbk)$, then the canonical lifting of E^σ (the elliptic curve obtained by applying σ to the coefficients of the equation that defines E) is $\boldsymbol{E}^\sigma$.

3. τ is an injective group homomorphism and a section of the reduction modulo p, which we denote by π.

4. If $\phi : E \to E^\sigma$ denotes the p-th power Frobenius, then there exists a map $\boldsymbol{\phi} : \boldsymbol{E} \to \boldsymbol{E}^\sigma$, such that the diagram

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

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

This concept of canonical lifting of elliptic curves was first introduced by Deuring in [Deu41] and then generalized to Abelian varieties by Serre and Tate in [LST64]. Apart from being of independent interest, this theory has been used in many interesting applications, such as counting rational points in ordinary elliptic curves, as in Satoh's [Sat00], coding theory, as in Voloch and Walker's [VW00], and counting torsion points of curves of genus $g \geq 2$, as in Poonen's [Poo01] or Voloch's [Vol97].

An algorithm for computing the canonical lifting of an elliptic curve over a field of characteristic $p \geq 5$ is given in [Fin20]. In this paper, Finotti notes that in all computed examples the algorithm gives formulas which do not involve the discriminant of the curve and conjectures that this is always the case. Some progress on this conjecture was made in [FL20], [FL21], and [FL23]. In Chapter 2 and Chapter 3 of this dissertation, we study the same algorithm for curves over fields of characteristic $p = 2, 3$ and make some progress on the same conjecture. We also extend some of the results in [Fin14], introduce some more conjectures that arose from various computations, and outline a modified algorithm to compute canonical liftings based on these conjectures.

In Chapter 4, we shift our focus to computations involving Witt vectors (introduced in detail below). It is well known that $\boldsymbol{W}(\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}_p$, the p-adic integers, and this isomorphism can be used to drastically speed up this computation. In fact, this works for any finite field. In [Hes15], the structure for $\boldsymbol{W}(\mathbb{Z})$ is given. In this dissertation, we investigate the structure of $\boldsymbol{W}(R)$ and give a computationally useful isomorphism for $\boldsymbol{W}(\mathbb{Z}/p^\alpha\mathbb{Z})$.

1.2 Witt Vectors and the Greenberg Transform

In this section we will review some of the basic facts about Witt vectors and define the Greenberg Transform. More details, including motivation and proofs, can be found in many sources such as Hazewinkel's [Haz09] and Borger's [Bor11]. A more friendly introduction can be found in Rabinoff's notes [Rab14]. We start with the following definition.

Definition 1.5. Fix a prime p. Then for each $n \in \mathbb{Z}_{\geq 0}$, the nth *Witt polynomial* is

$$w_n(X_0, \dots, X_n) \coloneqq X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^n X_n.$$

These Witt polynomials allow us to define two more infinite families of polynomials. Note that despite the denominators in the following formulas, cancellations yield polynomials with coefficients in $\mathbb{Z}$.

Definition 1.6. The *Witt sum polynomials* are $S_i \in \mathbb{Z}[X_0, \ldots, X_i, Y_0, \ldots, Y_i]$, where the S_i are inductively defined by

$$w_n(S_0, \ldots, S_n) = w_n(X_0, \ldots, X_n) + w_n(Y_0, \ldots, Y_n).$$

More explicitly,

$$S_n = X_n + Y_n + \frac{1}{p}\left(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p\right) + \cdots + \frac{1}{p^n}\left(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}\right). \tag{1.1}$$

Definition 1.7. The *Witt product polynomials* are $P_i \in \mathbb{Z}[X_0, \ldots, X_i, Y_0, \ldots, Y_i]$, where the P_i are inductively defined by

$$w_n(P_0, \ldots, P_n) = w_n(X_0, \ldots, X_n) \cdot w_n(Y_0, \ldots, Y_n)$$

More explicitly,

$$P_n = \frac{1}{p^n}\left[(X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - \left(P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p\right)\right]. \tag{1.2}$$

If we introduce a grading on $\mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$ by defining $\operatorname{wgt}(X_i) = \operatorname{wgt}(Y_i) = p^i$, then both S_n and P_n are homogeneous of weights p^n and $2p^n$ respectively in this graded ring. Since these polynomials have integer coefficients, it is well defined to evaluate them with inputs in any commutative ring. This allows us to define the titular ring.

Definition 1.8. Let R be a commutative ring (with 1) and let p be a prime. *The ring of p-Witt vectors over* R is defined to be the set $R^{\mathbb{Z}_{\geq 0}}$ equipped with the following operations. Let $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$. Then

$$\boldsymbol{a} + \boldsymbol{b} \coloneqq (S_0(a_0, b_0), S_1(a_0, a_1, b_0, b_1), \ldots)$$

and

$$\boldsymbol{a} \cdot \boldsymbol{b} \coloneqq (P_0(a_0, b_0), P_1(a_0, a_1, b_0, b_1), \ldots).$$

These operations make $R^{\mathbb{Z}_{\geq 0}}$ into a commutative ring (with 1). When p is clear from context, we denote this ring by $\boldsymbol{W}(R)$ and call it *the ring of Witt vectors over* R. Otherwise, we will use the (non-standard) notation $\boldsymbol{W}_{p,\infty}(R)$. Also, as with $\boldsymbol{a}$ and $\boldsymbol{b}$ above, we will use boldface lettering for any Witt vectors, and normal lettering with subscripts for the components of the vectors.

Since S_i and P_i only depend on the $X_0, \dots, X_i$ and $Y_0, \dots, Y_i$, we can also define the following rings.

Definition 1.9. Let R and p be as above and let $n \in \mathbb{N}$. *The ring of p-Witt vectors over R of length n* is defined to be the set R^n equipped with the operations in Definition 1.8 truncated to length n. This makes R^n into a commutative ring (with 1). When p is clear from context, we denote this ring by $\boldsymbol{W}_n(R)$ and call it *the ring of Witt vectors over R of length n*. Otherwise, we denote it by $\boldsymbol{W}_{p,n}(R)$, which is again non-standard.

Note. Since we are using 0-indexing, the elements of $\boldsymbol{W}_{p,n}(R)$ look like $\boldsymbol{a} = (a_0, \dots, a_{n-1})$ rather than $(a_1, \dots, a_n)$.

We now list some useful facts about Witt vectors. We will not prove any of these, but proofs can be found in in [Rab14].

Proposition 1.10. *Let R be a commutative ring, p a prime, and $n \in \mathbb{N} \cup \{\infty\}$. Then*

1. *The zero of $\boldsymbol{W}_{p,n}(R)$ is $(0, 0, 0, \dots)$ and the one is $(1, 0, 0, \dots)$.*

2. *For any $\boldsymbol{a} \in \boldsymbol{W}_{p,n}(R)$, we have*

$$-\boldsymbol{a} = \begin{cases} (-a_0, -a_1, \dots) & \text{if } p \neq 2 \\ (-1, -1, \dots) \cdot \boldsymbol{a} & \text{if } p = 2 \end{cases}$$

3. *The invertible Witt vectors are $\boldsymbol{W}_{p,n}(R)^\times = \{(a_0, a_1, \dots) \in \boldsymbol{W}_{p,n}(R) : a_0 \in R^\times\}$.*

4. *For $r \in R$ and $\boldsymbol{a} \in \boldsymbol{W}_{p,n}(R)$, $(r, 0, 0, \dots) \cdot \boldsymbol{a} = (ra_0, r^p a_1, r^{p^2} a_2, \dots)$.*

5. *We can define the projection $\pi : \boldsymbol{W}_{p,n}(R) \to R$ by $\pi(\boldsymbol{v}) \coloneqq v_0$. Then π is a ring homomorphism and $R \cong \boldsymbol{W}_{p,n}(R)/\ker(\pi)$.*

6. *If $p \in R^\times$, then $\boldsymbol{v} \mapsto (w_0(\boldsymbol{v}), w_1(\boldsymbol{v}), \ldots)$ is a ring isomorphism from $\boldsymbol{W}_{p,n}(R) \to R^n$.*

7. *For $n \neq \infty$, $\boldsymbol{W}_{p,n}(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$.*

8. *For $q = p^r$, $\boldsymbol{W}_{p,\infty}(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}_q$, the (unique) unramified degree-r extension of the p-adic integers.*

There are two common maps on the Witt vectors that we will make use of: the Verschiebung and Frobenius maps. A more thorough description of them can be found in Chapter 5 of [Rab14], but we will also give the definitions and some properties here.

Definition 1.11. The *Verschiebung map* on $\boldsymbol{W}(\Bbbk)$ is the map $V : \boldsymbol{W}(R) \to \boldsymbol{W}(R)$ defined by

$$(a_0, a_1, \ldots) \mapsto (0, a_0, a_1, \ldots).$$

There is a natural restriction of this map to the map $V : \boldsymbol{W}_n(R) \to \boldsymbol{W}_{n+1}(R)$ given by

$$(a_0, a_1, \ldots, a_n) \mapsto (0, a_0, a_1, \ldots, a_n).$$

Note. *Verschiebung* is the German word for *shift*.

Definition 1.12. The Frobenius map on $\boldsymbol{W}(R)$ is the map $F : \boldsymbol{W}(R) \to \boldsymbol{W}(R)$ defined by

$$\boldsymbol{a} \mapsto (f_0(\boldsymbol{a}), f_1(\boldsymbol{a}), \ldots)$$

where the f_i are uniquely defined by the identity of functions $w_m \circ F = w_{m+1}$ for all $m \in \mathbb{Z}_{\geq 0}$. There is a natural restriction of this map to the map $F : \boldsymbol{W}_{n+1}(R) \to \boldsymbol{W}_n(R)$ given by

$$\boldsymbol{a} \mapsto (f_0(\boldsymbol{a}), f_1(\boldsymbol{a}), \ldots, f_{n-1}(\boldsymbol{a})).$$

Note. This map is called the Frobenius map because it is a lifting of the Frobenius map on $\boldsymbol{W}(R)/p\boldsymbol{W}(R)$. In the case where R already has a Frobenius (e.g. $\mathbb{F}_{p^r}$), the Witt vector Frobenius is a lift of the Frobenius on R.

Normally, the Frobenius is a map from a ring to itself, which *is* the case for $\boldsymbol{W}(R)$, but not for $\boldsymbol{W}_n(R)$. To further illustrate this, we compute the first couple f_i. Firstly, $w_0 \circ F = w_1$

gives $f_0(X_0, X_1) = X_0^p + pX_1$. Then we have $w_1 \circ F = w_2$, which gives

$$\begin{aligned} f_0^p + pf_1 &= X_0^{p^2} + pX_1^p + p^2X_2 \\ \Rightarrow \qquad f_1(X_0, X_1, X_2) &= \frac{1}{p}\left[X_0^{p^2} + pX_1^p + p^2X_2 - (X_0^p + pX_1)^p\right] \end{aligned}$$

Note that despite the $1/p$ at the front, after cancellations f_1 has integer coefficients (just like the sum and product polynomials). Finally, we'll compute f_2,

$$\begin{aligned} w_2 \circ F &= w_3 \\ \Rightarrow \qquad f_0^{p^2} + pf_1^p + p^2f_2 &= X_0^{p^3} + pX_1^{p^2} + p^2X_2^p + p^3X_3 \\ \Rightarrow \qquad f_2(X_0, X_1, X_2, X_3) &= \frac{1}{p^2}\left[X_0^{p^3} + pX_1^{p^2} + p^2X_2^p + p^3X_3 - (f_0^{p^2} + pf_1^p)\right] \end{aligned}$$

Expanding f_0 and f_1 above and cancelling appropriately gives a polynomial that, again, has integer coefficients, despite the denominator. In general, $f_i \in \mathbb{Z}[X_0, \ldots, X_{i+1}]$. However, modulo p, we can make a great simplification: $f_i = X_i^p$ for all i, which is item 2 of the next proposition. This is where we can see the greatest similarity to the usual Frobenius morphism. A deeper investigation into the properties of the Witt vector Frobenius can be found in [DK14].

Proposition 1.13. *Let $\boldsymbol{a} \in \boldsymbol{W}(R)$. Then*

1. $F(V(\boldsymbol{a})) = p \cdot \boldsymbol{a}$.
2. *If R is a ring of characteristic p, then $F(\boldsymbol{a}) = (a_0^p, a_1^p, \ldots)$. In this case, it makes sense to define F as a map on $\boldsymbol{W}_n(R)$ rather than the larger domain given above.*

Proof. Item 1 is proved in Proposition 5.10 of [Rab14] and Item 2 is proved in Lemma 1.4 of [DK14]. □

So far, we have been working with any commutative ring, but most contexts work with Witt vectors over a perfect field $\Bbbk$ of characteristic p. These are called *p-typical Witt vectors* and have additional useful properties, which we enumerate next.

Proposition 1.14. *Let $\Bbbk$ be a perfect field of characteristic p. Then*

1. $\boldsymbol{W}(\Bbbk)$ *is a strict p-ring with residue field $\Bbbk$, that is*

   (a) $\boldsymbol{W}(\Bbbk)$ *is complete and Hausdorff with respect to the p-adic topology,*

   (b) *p is not a zero-divisor in $\boldsymbol{W}(\Bbbk)$, and*

   (c) *the residue ring, $\Bbbk = \boldsymbol{W}(\Bbbk)/p\boldsymbol{W}(\Bbbk)$, is perfect.*

2. *The integer p^r in $\boldsymbol{W}(\Bbbk)$ is given by $V^r(\mathbf{1})$, where V is the Verschiebung map.*

3. *Let $\tau : \Bbbk \to \boldsymbol{W}(\Bbbk)$ be the map $a \mapsto (a, 0, 0, \ldots)$ (called the Teichmüller map). Then for any $\boldsymbol{a} = (a_0, a_1, \ldots) \in \boldsymbol{W}(\Bbbk)$, we can write*

$$\boldsymbol{a} = \sum_{i=0}^{\infty} \tau(a_i^{1/p^i})p^i.$$

Moreover, $\tau|_{\Bbbk^\times} : \Bbbk^\times \to \boldsymbol{W}(\Bbbk)^\times$ is an injective group homomorphism.

Finally, we define the Greenberg transform.

Definition 1.15. Let $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$. Let $\boldsymbol{x_0} = (x_0, x_1, \ldots), \boldsymbol{y_0} = (y_0, y_1, \ldots) \in \boldsymbol{W}(\Bbbk[x_0, y_0, x_1, y_1, \ldots])$. Then we can evaluate $\boldsymbol{f}(\boldsymbol{x_0}, \boldsymbol{y_0}) = (f_0, f_1, \ldots)$, which is an element of $\boldsymbol{W}(\Bbbk[x_0, y_0, x_1, y_1, \ldots])$ (in fact, $f_i \in \Bbbk[x_0, y_0, \ldots, x_i, y_i]$ for all i). This is called the *Greenberg transform* of $\boldsymbol{f}$ and is denoted $\mathscr{G}(\boldsymbol{f})$.

Moreover, if

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

is a variety, we define the *Greenberg transform of $\boldsymbol{C}$*, denoted $\mathscr{G}(\boldsymbol{C})$, to be the (infinite dimensional) variety over $\Bbbk$ defined by the zeroes of the coordinates f_i of $\mathscr{G}(\boldsymbol{f})$.

It is clear from the definition that there is a bijection between $\boldsymbol{C}(\boldsymbol{W}(\Bbbk))$ and $\mathscr{G}(\boldsymbol{C})(\Bbbk)$, so we will often identify them and implicitly switch between the two forms. Also, we have

$$\mathscr{G}(\boldsymbol{x} + \boldsymbol{y}) = (S_0, S_1, \ldots) \quad \text{and} \quad \mathscr{G}(\boldsymbol{x} \cdot \boldsymbol{y}) = (P_0, P_1, \ldots).$$

For more information on the Greenberg transform and its computation, see [Fin14].

Chapter 2

Canonical Liftings in Characteristic 2

In [Fin20], Finotti investigates the Weierstrass coefficients and the elliptic Teichmüller lift of canonical liftings of elliptic curves over a field of characteristic 5 or more. Our goal in this chapter is to prove similar results for characteristic 2. Throughout this chapter, let $\Bbbk$ be a field of characteristic 2, let $E/\Bbbk$ be an ordinary elliptic curve, and let $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$ be its canonical lifting.

2.1 Weierstrass Forms

We start by giving two forms for E, both of which will be useful for us.

Proposition 2.1. *Any ordinary elliptic curve $E/\Bbbk$ is isomorphic to a curve of the form*

$$E'/\Bbbk : y^2 + hxy = x^3 + ax^2 + b \tag{2.1}$$

and to a curve of the form

$$E''/\Bbbk : y^2 + xy = x^3 + a'x^2 + b' \tag{2.2}$$

where $a' = a/h^2$ and $b' = b/h^6$.

Proof. Let $E/\Bbbk$ be given by

$$E/\Bbbk : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The Hasse invariant of this curve is a_1, and since E is ordinary, $a_1 \neq 0$. So we can define $r = a_3/a_1$ and $t = (a_1^2a_4 + a_3^2)/a_1^3$. Then the standard isomorphism given by $x \mapsto x' + r$ and $y \mapsto y' + t$ gives the form E' in Equation (2.1), with $h = a_1$. The expressions for a and b are messier, and so will not be included here, but they can be easily computed. Then, applying the isomorphism given by $x \mapsto h^2x'$ and $y \mapsto h^3y'$ to E' gives the form E'' in Equation (2.2). ☐

Using the form in Equation (2.1), the Hasse invariant of E is $\mathfrak{h} = h$ and the discriminant is $\Delta = h^6b$. We reiterate that since E is ordinary, $h \neq 0$. Since $\Delta \neq 0$, we also have $b \neq 0$. It may seem strange to use this form, as Equation (2.2) appears simpler on inspection (and it is). However, it has one useful property for us: by assigning weights of 1, 2, and 6 respectively to h, a, and b, and weights of 2 and 3 respectively to x and y, each monomial in Equation (2.1) has weight 6. These balanced weights will benefit us later. Next, we show that $\boldsymbol{E}$ has the same form.

Proposition 2.2. *The curve $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$ is isomorphic to*

$$\boldsymbol{E}'/\boldsymbol{W}(\Bbbk) : \boldsymbol{y}^2 + \boldsymbol{hxy} = \boldsymbol{x}^3 + \boldsymbol{ax}^2 + \boldsymbol{b} \tag{2.3}$$

where

$$\boldsymbol{h} = (h, h_1, \dots), \ \ \boldsymbol{a} = (a, a_1, \dots), \ \ \textit{and } \boldsymbol{b} = (b, b_1, \dots).$$

Proof. Let $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$ be given by

$$\boldsymbol{E}/\boldsymbol{W}(\Bbbk) : \boldsymbol{y}^2 + \boldsymbol{hxy} + \boldsymbol{cy} = \boldsymbol{x}^3 + \boldsymbol{ax}^2 + \boldsymbol{dx} + \boldsymbol{b}.$$

Since $\boldsymbol{E}$ is the canonical lifting of E, it must reduce to E modulo 2, which immediately gives

$$\boldsymbol{c} = (0, c_1, c_2, \dots) \quad \text{and} \quad \boldsymbol{d} = (0, d_1, d_2, \dots).$$

Consider the isomorphism given by

$$\boldsymbol{x} \mapsto \boldsymbol{x}' + \boldsymbol{r} \qquad \boldsymbol{y} \mapsto \boldsymbol{y}' + \boldsymbol{t},$$

which gives a new curve $\boldsymbol{E'}/\boldsymbol{W}(\mathbb{k})$ given by

$$\begin{aligned}&\boldsymbol{y}^2 + \boldsymbol{hxy} + (\boldsymbol{hr} + \boldsymbol{c} + 2\boldsymbol{t})\boldsymbol{y} \\ &= \boldsymbol{x}^3 + (\boldsymbol{a} + 3\boldsymbol{r})\boldsymbol{x}^2 + (2\boldsymbol{ar} + 3\boldsymbol{r}^2 + \boldsymbol{d} - \boldsymbol{ht})\boldsymbol{x} + (\boldsymbol{b} + \boldsymbol{ar}^2 + \boldsymbol{r}^3 - \boldsymbol{hrt} + \boldsymbol{dr} - \boldsymbol{ct} - \boldsymbol{t}^2).\end{aligned}$$

We want $\boldsymbol{hr} + \boldsymbol{c} + 2\boldsymbol{t} = 2\boldsymbol{ar} + 3\boldsymbol{r}^2 + \boldsymbol{d} - \boldsymbol{ht} = 0$, i.e.

$$\boldsymbol{r} = -\boldsymbol{h}^{-1}(\boldsymbol{c} + 2\boldsymbol{t}) \text{ and } \boldsymbol{t} = \boldsymbol{h}^{-1}(2\boldsymbol{ar} + 3\boldsymbol{r}^2 + \boldsymbol{d}).$$

Note that $h_0 \in k^\times$, so $\boldsymbol{h}^{-1}$ exists. These two equations over $\boldsymbol{W}(\mathbb{k})$ give us an infinite system of equations over $\mathbb{k}$. Firstly, we have

$$\begin{aligned}(r_0, r_1, r_2, \ldots) &= -\boldsymbol{h}^{-1}\left((0, c_1, c_2, \ldots) + (0, t_0^2, t_1^2, \ldots)\right) \\ &= -\boldsymbol{h}^{-1}\left(0, S_1(0, c_1, 0, t_0^2), S_2(0, c_1, c_2, 0, t_0^2, t_1^2), \ldots\right)\end{aligned}$$

which gives $r_0 = 0$ and for all $i \geq 1$, we can write

$$r_i = f_i\left(h_0^{-1}, h_0, \ldots, h_i, c_1, \ldots, c_i, t_0, \ldots, t_{i-1}\right)$$

where each f_i is a polynomial over $\mathbb{Z}$. Note that, crucially, r_i does *not* depend on t_i. Now, we also have

$$(t_0, t_1, t_2, \ldots) = \boldsymbol{h}^{-1}\left((0, a_0^2, a_1^2, \ldots) \cdot (0, r_1, r_2, \ldots) + 3(0, r_1, r_2, \ldots)^2 + (0, d_1, d_2, \ldots)\right).$$

which gives $t_0 = 0$ and for $i \geq 1$, we can write

$$t_i = g_i\left(h_0^{-1}, h_0, \ldots, h_i, a_0, \ldots, a_{i-1}, r_1, \ldots, r_i, d_1, \ldots, d_i\right)$$

where each g_i is a polynomial over $\mathbb{Z}$. Since r_i does *not* depend on t_i, we can alternate between computing r_i and t_i to get a solution for this system. That is, there are $\boldsymbol{r}, \boldsymbol{t} \in \boldsymbol{W}(\Bbbk)$ so that $\boldsymbol{hr} + \boldsymbol{c} + 2\boldsymbol{t} = 2\boldsymbol{ar} + 3\boldsymbol{r}^2 + \boldsymbol{d} - \boldsymbol{ht} = 0$. So we can write

$$\boldsymbol{E}'/\boldsymbol{W}(\Bbbk) : \boldsymbol{y}^2 + \boldsymbol{hxy} = \boldsymbol{x}^3 + (\boldsymbol{a} + 3\boldsymbol{r})\boldsymbol{x}^2 + \boldsymbol{b} + \boldsymbol{r}(\boldsymbol{ar} + \boldsymbol{r}^2 - \boldsymbol{ht} + \boldsymbol{d}) - \boldsymbol{t}(\boldsymbol{c} + \boldsymbol{t}).$$

Since $r_0 = t_0 = 0$, we have that $\boldsymbol{r} \equiv \boldsymbol{t} \equiv 0 \pmod 2$, and so $\boldsymbol{E}'$ also reduces to E modulo 2. $\square$

Since $h_0 = h$, $a_0 = a$, and $b_0 = b$, we will typically forgo the subscript for the first components of the Weierstrass coefficients, in order to make the reduction modulo p more clear. We will however use x_0 and y_0 instead of x and y, which makes the notation in the elliptic Teichmüller lift consistent with the usual Witt vector notation.

2.2 The Voloch-Walker Algorithm

In Section 5 of [Fin20], Finotti describes the Voloch-Walker algorithm to compute the Weierstrass coefficients and the coordinates of the elliptic Teichmüller lift for $p \geq 5$. This algorithm also works for $p = 2$ with some modifications, which we will elucidate here, along with a summary of the algorithm.

2.2.1 The Setup

Firstly, from the reasoning just before Theorem 1.1 of [Fin02], we have that the Teichmüller lift takes the form

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

where $x_n = F_n$ and $y_n = G_n + y_0 H_n$ with $F_n, G_n, H_n \in \Bbbk[x_0]$ for all $n \geq 0$. By Theorem 2.1 of [Fin04], we have $dF_n/dx_0 = 0$, so we can skip the integration step. Unlike for $p \geq 5$, we can't assume that $G_i = 0$, but we can still apply Theorem 1.1 of [Fin02] to get $\deg(F_n) \leq 2^{n-2}(n+4)$, $\deg(G_n) \leq 2^{n-2}(n+6)$, and $\deg(H_n) \leq 2^{n-2}(n+6) - \frac{3}{2}$.

This algorithm can be applied to specific elliptic curves, but in order to calculate general formulas, we can take our base field to be $\mathbb{K} = \mathbb{F}_2(a, b, h)$, where a, b, and h are indeterminates. We then apply the algorithm to the curve given by

$$E/\mathbb{K} : y_0^2 + hx_0y_0 = x_0^3 + ax_0^2 + b,$$

to compute the Weierstrass coordinates a_n, b_n, and h_n and the F_n, G_n, and H_n, one coordinate at a time.

2.2.2 The Affine Part

Inductively, suppose we have already computed $a_i, b_i, h_i \in \mathbb{K}$, and $F_i, G_i, H_i \in \mathbb{K}[x_0]$ for $i < n$. To compute the $(n+1)$-st coordinates, we first compute the $(n+1)$-st coordinate of the Greenberg transform, $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$ which gives

$$\begin{aligned}
& h_0^{2^n}(x_0^{2^n}y_n + x_ny_0^{2^n}) + x_0^{2^n}y_0^{2^n}h_n = x_0^{2^{n+1}}x_n + x_0^{2^{n+1}}a_n + b_n + \varepsilon_n && (2.4)\\
\Rightarrow \quad & (h_0x_0)^{2^n}y_n + (x_0y_0)^{2^n}h_n = (x_0^{2^{n+1}} + (h_0y_0)^{2^n})x_n + x_0^{2^{n+1}}a_n + b_n + \varepsilon_n && (2.5)\\
\Rightarrow \quad & (h_0x_0)^{2^n}(G_n + y_0H_n) + (x_0y_0)^{2^n}h_n = (x_0^{2^{n+1}} + (h_0y_0)^{2^n})F_n + x_0^{2^{n+1}}a_n + b_n + \varepsilon_n && (2.6)
\end{aligned}$$

where $\varepsilon_n \in \mathbb{K}[x_0, y_0]$ contains all the other terms that come from the Greenberg transform. We will use this equation to set up a system of equations to solve for a_n, b_n, and h_n and the F_n, G_n, and H_n. Solving for the latter three means solving for their coefficients. Letting

$$M \coloneqq \lfloor 2^{n-3}(n+4) \rfloor, \; N \coloneqq \lfloor 2^{n-2}(n+6) \rfloor, \text{ and } \delta \coloneqq \begin{cases} 1 & \text{if } n = 1 \\ 2 & \text{if } n \geq 2 \end{cases}$$

we have that

$$F_n = \sum_{i=0}^{M} c_i x_0^{2i}, \; G_n = \sum_{i=0}^{N} d_i x_0^i, \text{ and } H_n = \sum_{i=0}^{N-\delta} e_i x_0^i.$$

Note that F_n has no terms with an odd power since its derivative is zero. Also note that in the algorithm for $p \geq 5$, the coefficients of H_n are called d_i rather than e_i. This distinction is not important, we merely point it out to avoid confusion. Replacing F_n, G_n, and H_n in the Greenberg transform by these expressions gives

$$\begin{aligned}(h_0x_0)^{2^n}\left(\sum_{i=0}^{N} d_ix_0^i + y_0\sum_{i=0}^{N-\delta} e_ix_0^i\right) + (x_0y_0)^{2^n}h_n \\ = (x_0^{2^{n+1}} + (h_0y_0)^{2^n})\sum_{i=0}^{M} c_ix_0^{2i} + x_0^{2^{n+1}}a_n + b_n + \varepsilon_n.\end{aligned} \tag{2.7}$$

Then using the equation for the curve E, we can repeatedly replace any powers of y_0 greater than one (including those in ε_n). Lemma 2.3 below can help with this. At this point, by comparing coefficients of monomials of the same degrees, we get a *linear* system of coefficients over $\mathbb{K}$ in the unknowns a_n, b_n, h_n, c_i's, d_i's, and e_i's. We are guaranteed that this system has a solution, namely the one associated to the canonical lifting. However, not every solution to the system gives a canonical lifting. For this, we need the following step.

2.2.3 Regularity at Infinity

The next step in the algorithm is to ensure that $\tau^*(\boldsymbol{x}/\boldsymbol{y})$ has a zero at infinity. (If $n = 1$, this does not give us any information, and so can be skipped.) Let $\mathfrak{m}_O$ be the elements h of the function field of E that have a zero at infinity, i.e. $\mathrm{ord}_O(h) \geq 1$. Then, letting τ_n be the $(n+1)$-st coordinate of $\tau^*(\boldsymbol{x}/\boldsymbol{y})$, we have

$$\tau_n = \frac{x_n}{y_0^{2^n}} + \frac{x_0^{2^n}y_n}{y_0^{2^{n+1}}} + \frac{\delta_1}{y_0^{(n+1)2^n}} \equiv 0 \pmod{\mathfrak{m}_O}$$

for some $\delta_1 \in \mathbb{K}[x_0, y_0]$. Using Equation (2.5) we can replace $x_0^{2^n}y_n$ and get

$$\frac{x_n}{y_0^{2^n}} + \frac{(x_0y_0)^{2^n}h_n + (x_0^{2^{n+1}} + (h_0y_0)^{2^n})x_n + x_0^{2^{n+1}}a_n + b_n}{h_0^{2^n}y_0^{2^{n+1}}} + \frac{\delta_2}{y_0^{(n+1)2^n}} \equiv 0 \pmod{\mathfrak{m}_O},$$

where δ_2 absorbs the terms from ε_n. The terms involving a_n, b_n, and h_n are already in $\mathfrak{m}_O$, and after getting a common denominator, some cancellations occur. So we end up with

$$\frac{1}{h_0^{2^n}y_0^{(n+1)2^n}}\left[x_0^{2^{n+1}}y_0^{(n-1)2^n}x_n + \delta_3\right] \equiv 0 \pmod{\mathfrak{m}_O}, \tag{2.8}$$

that is, we need

$$\begin{aligned}
&\operatorname{ord}_O\left(x_0^{2^{n+1}}y_0^{(n+1)2^n}x_n+\delta_3\right) > -\operatorname{ord}_O\left(h_0^{2^n}y_0^{(n+1)2^n}\right) = -3(n+1)2^n\\
\Rightarrow\ &\deg_{x_0}\left(x_0^{2^{n+1}}y_0^{(n-1)2^n}x_n+\delta_3\right) < 3(n+1)2^{n-1}.
\end{aligned}$$

Since $\deg\left(y_0^{(n-1)2^n}\right) = 3(n-1)2^{n-1}$, this degree restriction determines the c_i for $i \geq 2^{n-1}$. Since the d_i and e_i can never be in the same coefficient, as the e_i have a y_0 attached, this then determines the d_i for $i \geq 2^{n+1}-1$ and the e_i for $i \geq 2^n - 2$. Also, with these values determined, we are guaranteed that any solution to the system that remains will give us a canonical lifting. So, letting $M' = 2^{n-1}-1$, $N' = 2^{n+1}-2$ and $N'' = 2^n - 3$, what remains to be solved is

$$\begin{aligned}
&(h_0x_0)^{2^n}\left(\sum_{i=0}^{N'} d_i x_0^i + y_0\sum_{i=0}^{N''} e_i x_0^i\right) + (x_0y_0)^{2^n}h_n\\
&\quad = (x_0^{2^{n+1}} + (h_0y_0)^{2^n})\sum_{i=0}^{M'} c_i x_0^{2i} + x_0^{2^{n+1}}a_n + b_n + \varepsilon_n
\end{aligned} \tag{2.9}$$

As before, this gives a (now smaller) linear system over $\mathbb{K}$ in the unknowns a_n, b_n, h_n, c_i's, d_i's and e_i's. Note that this system does not have a unique solution, but the canonical lifting is only unique *up to isomorphism*. Also, since the system is over $\mathbb{K}$, the solutions will also be in $\mathbb{K}$, ensures that the induction hypothesis holds at every step.

2.3 Choosing a Solution

In this section, our goal is study solutions to the system given by Equation (2.9). More specifically, we would like to pick a solution that is both "simple" in some sense and gives nice properties to the Weierstrass coefficients and Teichmüller coordinates. First, we need the following lemma.

Lemma 2.3. *Using the form in Equation (2.1) for $E/\Bbbk$, for all $n \geq 1$, we have*

$$y^{2^n} = h^{2^n-1}x^{2^n-1}y + \sum_{k=1}^{n}\left[h^{(2^{k-1}-1)2^{n-k+1}}\left(x^{(2^k+1)2^{n-k}} + a^{2^{n-k}}x^{2^n} + b^{2^{n-k}}x^{(2^{k-1}-1)2^{n-k+1}}\right)\right].$$

Proof. For $n = 1$, the identity gives

$$\begin{aligned} y^2 &= h^{2^1-1}x^{2^1-1}y + h^{(2^{1-1}-1)2^{1-1+1}}\left(x^{(2^1+1)2^{1-1}} + a^{2^{1-1}}x^{2^1} + b^{2^{1-1}}x^{(2^{1-1}-1)2^{1-1+1}}\right) \\ &= hxy + x^3 + ax^2 + b, \end{aligned}$$

which is correct. Recall that we're in characteristic 2, so $-1 = 1$ *and* we can take advantage of the Frobenius for powers of 2. We proceed by induction. We have

$$\begin{aligned} y^{2^n} &= (hxy + x^3 + ax^2 + b)^{2^{n-1}} \\ &= h^{2^{n-1}}x^{2^{n-1}}y^{2^{n-1}} + x^{3\cdot 2^{n-1}} + a^{2^{n-1}}x^{2^n} + b^{2^{n-1}} \\ &= h^{2^n-1}x^{2^n-1}y + x^{3\cdot 2^{n-1}} + a^{2^{n-1}}x^{2^n} + b^{2^{n-1}} \\ &\quad + h^{2^{n-1}}x^{2^{n-1}}\sum_{k=1}^{n-1}\left[h^{(2^{k-1}-1)2^{n-k}}\left(x^{(2^k+1)2^{n-k-1}} + a^{2^{n-k-1}}x^{2^{n-1}} + b^{2^{n-k-1}}x^{(2^{k-1}-1)2^{n-k}}\right)\right] \\ &= h^{2^n-1}x^{2^n-1}y + h^0\left(x^{3\cdot 2^{n-1}} + a^{2^{n-1}}x^{2^n} + b^{2^{n-1}}\right) \\ &\quad + \sum_{k=1}^{n-1}\left[h^{(2^k-1)2^{n-k}}\left(x^{(2^{k+1}+1)2^{n-k-1}} + a^{2^{n-k-1}}x^{2^n} + b^{2^{n-k-1}}x^{(2^k-1)2^{n-k}}\right)\right] \\ &= h^{2^n-1}x^{2^n-1}y + \left[h^{(2^{1-1}-1)2^{n-1+1}}\left(x^{(2^1+1)2^{n-1}} + a^{2^{n-1}}x^{2^n} + b^{2^{n-1}}x^{(2^{1+1}-1)2^{n-1+1}}\right)\right] \\ &\quad + \sum_{j=2}^{n}\left[h^{(2^{j-1}-1)2^{n-j+1}}\left(x^{(2^j+1)2^{n-j}} + a^{2^{n-j}}x^{2^n} + b^{2^{n-j}}x^{(2^{j+1}-1)2^{n-j+1}}\right)\right] \\ &= h^{2^n-1}x^{2^n-1}y + \sum_{j=1}^{n}\left[h^{(2^{j-1}-1)2^{n-j+1}}\left(x^{(2^j+1)2^{n-j}} + a^{2^{n-j}}x^{2^n} + b^{2^{n-j}}x^{(2^{j+1}-1)2^{n-j+1}}\right)\right]. \quad \square \end{aligned}$$

Now we can move on to a description of the solutions.

Proposition 2.4. *The system described in the previous section has two free parameters which can be assigned to the values of a_n and h_n.*

Proof. Suppose we have computed a_i, b_i, h_i, F_i, G_i, and H_i for $i < n$ and that we have two solutions to the system given by

$$(a_n, b_n, h_n, c_0, \ldots, c_{M'}, d_0, \ldots, d_{N'}, e_0, \ldots, e_{N''})$$
$$\text{and } (a'_n, b'_n, h'_n, c'_0, \ldots, c'_{M'}, d'_0, \ldots, d'_{N'}, e'_0, \ldots, e'_{N''}).$$

Consider the curves given by these two solutions, say

$$\begin{aligned}\boldsymbol{E}/W_{n+1}(\mathbb{K}): &\quad \boldsymbol{y}^2 + (h,\dots,h_{n-1},h_n)\boldsymbol{x}\boldsymbol{y} = \boldsymbol{x}^3 + (a,\dots,a_{n-1},a_n)\boldsymbol{x}^2 + (b,\dots,b_{n-1},b_n)\\ \boldsymbol{E'}/W_{n+1}(\mathbb{K}): &\quad \boldsymbol{y'}^2 + (h,\dots,h_{n-1},h'_n)\boldsymbol{x'}\boldsymbol{y'} = \boldsymbol{x'}^3 + (a,\dots,a_{n-1},a'_n)\boldsymbol{x'}^2 + (b,\dots,b_{n-1},b'_n)\end{aligned}$$

Since $\boldsymbol{E}$ and $\boldsymbol{E'}$ are isomorphic, we must have $\boldsymbol{u} \in W_{n+1}(\mathbb{K})^\times$ and $\boldsymbol{r},\boldsymbol{s},\boldsymbol{t} \in W_{n+1}(\mathbb{K})$ such that

$$\boldsymbol{x} = \boldsymbol{u}^2\boldsymbol{x'} + \boldsymbol{r} \text{ and } \boldsymbol{y} = \boldsymbol{u}^3\boldsymbol{y'} + \boldsymbol{u}^2\boldsymbol{s}\boldsymbol{x'} + \boldsymbol{t}.$$

Note that mod 2^n, $\boldsymbol{E}$ and $\boldsymbol{E'}$ are actually *identical*, not just isomorphic, so we must have

$$\begin{aligned}\boldsymbol{u} &\equiv 1 \pmod{2^n}\\ \boldsymbol{r} \equiv \boldsymbol{s} \equiv \boldsymbol{t} &\equiv 0 \pmod{2^n}\end{aligned}$$

that is

$$\boldsymbol{u} = (1,0,\dots,0,u);\quad \boldsymbol{r} = (0,0,\dots,0,r);\quad \boldsymbol{s} = (0,0,\dots,0,s);\quad \boldsymbol{t} = (0,0,\dots,0,t)$$

with $u,r,s,t \in \mathbb{K}$. Substituting these values into the equation for $\boldsymbol{E}$, we get

$$\begin{aligned}\boldsymbol{E'}: \boldsymbol{y'}^2 &+ (h,\dots,h_{n-1},h_n + uh^{2^n})\boldsymbol{x'}\boldsymbol{y'} + (0,\dots,0,rh^{2^n})\boldsymbol{y}\\ &= \boldsymbol{x'}^3 + (a,\dots,a_{n-1},a_n + sh^{2^n} + r)\boldsymbol{x'}^2 + (0,\dots,0,th^{2^n})\boldsymbol{x} + (b,\dots,b_{n-1},b_n).\end{aligned}$$

We immediately see that we must have $r = t = 0$, as $h \neq 0$ and the coefficients of $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\boldsymbol{E}'$ are zero. Simplifying gives

$$\begin{aligned}\boldsymbol{E'}: \boldsymbol{y'}^2 &+ (h,\dots,h_{n-1},h_n + uh^{2^n})\boldsymbol{x'}\boldsymbol{y'}\\ &= \boldsymbol{x'}^3 + (a,\dots,a_{n-1},a_n + sh^{2^n})\boldsymbol{x'}^2 + (b,\dots,b_{n-1},b_n).\end{aligned} \tag{2.10}$$

So we have

$$h'_n = h_n + uh^{2^n},\quad a'_n = a_n + sh^{2^n},\quad \text{and}\quad b'_n = b_n.$$

With these values, subtracting equations for the $(n+1)$-st coordinate of the Greenberg Transforms of $\boldsymbol{E}$ and $\boldsymbol{E'}$ (with unknowns) gives

$$h^{2^n}\sum(d_i-d_i')x_0^{2^n+i}+y_0h^{2^n}\sum(e_i-e_i')x_0^{2^n+i}+u(x_0y_0h)^{2^n}$$

$$=(x_0^{2^{n+1}}+h^{2^n}y_0^{2^n})\sum(c_i-c_i')x_0^{2i}+sh^{2^n}x_0^{2^{n+1}}$$

The term $x_0^{2^{n+1}}\sum(c_i-c_i')x_0^{2i}$ is the only term without h, and so cannot be cancelled by any other terms. Thus, we must have $c_i=c_i'$ for all i. This now gives:

$$\begin{aligned}h^{2^n}\sum(d_i-d_i')x_0^{2^n+i}+y_0h^{2^n}\sum(e_i-e_i')x_0^{2^n+i}+u(x_0y_0h)^{2^n}+sh^{2^n}x_0^{2^{n+1}}&=0\\ \Rightarrow h^{2^n}x_0^{2^n}\left(\sum(d_i-d_i')x_0^i+y_0\sum(e_i-e_i')x_0^i+uy_0^{2^n}+sx_0^{2^n}\right)&=0\end{aligned}$$

Since h and x_0 are non-zero, we can now focus on the term in parentheses.

We will use Lemma 2.3 to expand the term $uy_0^{2^n}$ above. First, we note that after expanding using this identity, the only remaining term with y_0 is $h^{2^n-1}x_0^{2^n-1}y_0$. So we must have $e_i=e_i'$ for all $i\neq 2^n-1$ and we get $e_{2^n-1}=e_{2^n-1}'+uh^{2^n-1}$. We now turn to what remains:

$$\sum(d_i-d_i')x_0^i+u\sum_{k=1}^{n}\left[h^{(2^{k-1}-1)2^{n-k+1}}\left(x_0^{(2^k+1)2^{n-k}}+a^{2^{n-k}}x_0^{2^n}+b^{2^{n-k}}x_0^{(2^{k-1}-1)2^{n-k+1}}\right)\right]+sx_0^{2^n}$$

We can see right away that s will affect d_{2^n} and no others. So we get the first generator for the nullspace of the coefficient matrix:

$$(h^{2^n},0,\dots,0,1,0,\dots,0)$$

where the 1 is in the coordinate corresponding to d_{2^n}.

We can also see that d_i will be affected by u for all i corresponding to the powers of x_0 above. So we must have $d_i=d_i'$ for all i not appearring in a power of x_0. This gives the second (and final) generator for the nullspace:

$$\left(0,0,h^{2^n},0,\ldots,0,b_0^{2^{n-1}},\ldots,\sum_{k=1}^{n} a_0^{2^{n-k}} h^{(2^{k-1}-1)2^{n-k+1}},\ldots,1,0,\ldots,0,h^{2^n-1},0,\ldots,0\right)$$

where $b_0^{2^{n-1}}$ corresponds to d_0, the large sum corresponds to d_{2^n}, the 1 corresponds to $d_{3\cdot 2^{n-1}}$, and h^{2^n-1} corresponds to e_{2^n-1}.

So, these two free parameters allow us to choose two of a_n, h_n, many of the d_i's, or e_{2^n-1}. Notably, since $h \neq 0$ (even if we're not treating it like a variable), this means that we can choose both a_n **and** h_n! □

Throughout, we have been using Equation (2.1). But we noted that we also have Equation (2.2) and in fact, if there is some $\lambda \in \Bbbk$ so that $\lambda^2 + \lambda = a' = a/h^2$, then E is isomorphic to

$$E'''/\Bbbk : y^2 + xy = x^3 + b'$$

where $b' = b/h^6$ (via $x \mapsto x$ and $y \mapsto y + \lambda x$). So, in some sense, E is almost isomorphic to a curve with $h = 1$ and $a = 0$. This gives some intuition for why we can choose $a_n = h_n = 0$ at every step. If $h = 1$ and $a = 0$, then the coefficient of $\boldsymbol{xy}$ in $\boldsymbol{E}$ would be $\mathbf{1} = (1, 0, 0, \ldots)$ and the coefficient of $\boldsymbol{x}^2$ would be $\mathbf{0} = (0, 0, 0, \ldots)$.

2.4 Universality

As we showed in the previous section, at every step of the Voloch-Walker algorithm, we can choose both a_n and h_n. The "simplest" choice would be to choose them both to be 0. However, as explained in Section 2 of [Fin20], this could lead to the formula for b_n to be undefined for some values of a_0, b_0, h_0 that give an ordinary curve. This leads us to the following definitions, which are the characteristic 2 analogues of Definitions 1.2 and 2.1 of [Fin20], respectively.

Definition 2.5. The set of ordinary coefficients over $\Bbbk$ is defined to be

$$\Bbbk^3_{\text{ord}} := \{(a_0, b_0, h_0) \in \Bbbk^3 : \text{the elliptic curve } E/\Bbbk \text{ defined by Equation (2.1) is ordinary.}\}$$

Note that in this definition, we are implicitly assuming that E is non-singular as well. So while the statement of this definition is very general, by the reasoning in Section 2.1, we have that $\Bbbk^3_{\mathrm{ord}} = \{(a_0, b_0, h_0) \in \Bbbk^3 : b_0 \neq 0 \text{ and } h_0 \neq 0\}$.

Definition 2.6. A rational function $f \in \mathbb{F}_2(a, b, h)$ is called *universal* if it is defined for all $(a_0, b_0, h_0) \in \Bbbk^3_{\mathrm{ord}}$.

Our goal in this section is to show that for every $n \geq 1$ there are $a_n, b_n, h_n \in \mathbb{F}_2(a, b, h)$ that are universal, i.e. we only need *one* formula for the Weierstrass coefficients of $\boldsymbol{E}$. First, we show that the condition of universality restricts the form of these rational functions.

Proposition 2.7. *If $f \in \mathbb{F}_2(a, b, h)$ is universal, then $f \in \mathbb{F}_2[a, b, h, 1/(bh)]$.*

Proof. Suppose not and let $g \in \mathbb{F}_2[a, b, h]$ be an irreducible factor of the denominator of f with g not equal to b or h. Let $\Bbbk = \overline{F_2}$. Then $V \coloneqq \{g(a, b, h) = 0\}$ is a variety of positive dimension over $\Bbbk$, and thus $|V| = \infty$. Furthermore, since $(g, b) = 1$ and $(g, h) = 1$, by Bézout's Theorem, we have $|V \cap \{b = 0\} \cap \{h = 0\}| < \infty$. So there is some $(a_0, b_0, h_0) \in \Bbbk^3$ such that $g(a_0, b_0, h_0) = 0$ and $b_0, h_0 \neq 0$. But then

$$E/\Bbbk : y^2 + h_0xy = x^3 + a_0x^2 + b_0$$

is an ordinary elliptic curve, so $(a_0, b_0, h_0) \in \Bbbk^3_{ord}$, contradicting the universality of f. Thus we must have $f \in \mathbb{F}_2[a, b, h, 1/(bh)]$. □

Now we move on to the main result of this section. As stated, the "simplest" choice for a_n and h_n is to take both of them to be 0. We will see that b_n remains universal under this choice and we even get some results about the coefficients of F_n, G_n, and H_n.

Proposition 2.8. *Let $\mathbb{K} = \mathbb{F}_2(a, b, h)$ and let $\mathbb{L} \coloneqq \mathbb{F}_2[a, b, h, 1/(bh)]$. Then there are $a_n, b_n, h_n \in \mathbb{L}$ and $F_n, G_n, H_n \in \mathbb{L}[x_0]$ for all $n \geq 1$ such that the canonical lifting of $E/\mathbb{K}$ is given by*

$$\boldsymbol{E}/\boldsymbol{W}(\mathbb{K}) : y^2 + (h, h_1, \ldots)xy = x^3 + (a, a_1, \ldots)x^2 + (b, b_1, \ldots)$$

and the associated Teichmüller lift is given by

$$\tau(x_0, y_0) = ((x_0, F_1, \ldots), (y_0, G_1 + y_0H_1, \ldots)).$$

Proof. Inductively suppose we have $a_i, b_i, h_i \in \mathbb{L}$ and $F_i, G_i, H_i \in \mathbb{L}[x_0]$ for all $i < n$.

Choosing $a_n = h_n = 0$ immediately gives $a_n, h_n \in \mathbb{L}$. As can be seen in Equation (2.10), the formula for b_n is not affected by any choice we make and so must be universal. Therefore we also have $b_n \in \mathbb{L}$.

Consider Equation (2.7). By induction, we must have that all the terms contained in ε_n are in $\mathbb{L}$. Also, the c_i determined by the condition on $\tau^*(x/y)$ must all be in $\mathbb{L}$, as the leading coefficient of the expression in Equation (2.8) is in $\mathbb{F}_p$.

By the reasoning in the proof of Proposition 2.4, we must have that $c_i' = c_i$ for all i and that $e_i' = e_i$ for all $i \neq 2^n - 1$. Therefore these coefficients must all be universal as well, showing $F_n \in \mathbb{L}$ and nearly showing $H_n \in \mathbb{L}$. At this stage we have a system of the form

$$(hx_0)^{2^n} \left(\sum_{i=0}^{N'} d_i x_0^i + e_{2^n-1} x_0^{2^n-1} y_0 \right) = \cdots$$

where the right-hand side is in $\mathbb{L}$. Equating coefficients and solving can only introduce a denominator of h, which won't kick us out of $\mathbb{L}$, and so the d_i and e_{2^n-1} are also in $\mathbb{L}$, which shows $G_i, H_i \in \mathbb{L}$, finishing the proof. $\square$

There are two things of note in this proof. First, it does not depend strictly on choosing $a_n = h_n = 0$. As long as they are chosen to be in $\mathbb{L}$, the proof still holds. Second, the only denominator that is explicitly introduced is h. Hiding in the details of solving the linear system, there is the potential for a denominator of b to be introduced. However, in all computed examples, this denominator does *not* appear, which we will further investigate in Section 2.6.

2.5 Modularity

In this section, our goal is to show that a_n, b_n, h_n, F_n, G_n, and H_n are modular functions of specific weights. To clarify this statement, we first define $\mathrm{wgt}(a_0) \coloneqq 2$, $\mathrm{wgt}(b_0) \coloneqq 6$, $\mathrm{wgt}(h_0) \coloneqq 1$, $\mathrm{wgt}(x_0) \coloneqq 2$, and $\mathrm{wgt}(y_0) \coloneqq 3$. These weights allow us to make the following definition.

Definition 2.9. The *modular functions of weight n* (over $\mathbb{F}_2(a, b, h, x_0, y_0)$) are

$$\mathcal{S}_n := \left\{ \frac{f}{g} : f, g \in \mathbb{F}_2[a, b, h, x_0, y_0] \text{ homogeneous and } \operatorname{wgt}(f) - \operatorname{wgt}(g) = n \right\} \cup \{0\}.$$

As noted in Section 2.1, both sides of Equation (2.1) are in $\mathcal{S}_6$. We then prove the following proposition.

Proposition 2.10. *If we choose $a_n \in \mathcal{S}_{2^{n+1}}$ and $h_n \in \mathcal{S}_{2^n}$ in each step of the Voloch-Walker algorithm, then $b_n \in \mathcal{S}_{6\cdot 2^n}$, $F_n \in \mathcal{S}_{2^{n+1}}$, $G_n \in \mathcal{S}_{3\cdot 2^n}$, and $H_n \in \mathcal{S}_{3\cdot 2^n - 3}$ for all $n \geq 0$.*

Note. Since we are choosing $a_n = h_n = 0$ at every step, we satisfy the conditions of this statement, but there are many choices that guarantee modularity.

Proof. We (as usual) use induction to prove this proposition. Since both sides of Equation (2.1) are in $\mathcal{S}_6$, we have our base case done. (This means that if we instead start with Equation (2.2) we will *not* necessarily get modular functions!) Now, we assume that for $0 \leq i < n$, we have $b_i \in \mathcal{S}_{6\cdot 2^i}$, $F_i \in \mathcal{S}_{2^{i+1}}$, $G_i \in \mathcal{S}_{3\cdot 2^i}$, and $H_i \in \mathcal{S}_{3\cdot 2^i - 3}$.

By applying Lemma 3.1 of [Fin20] to the Greenberg Transform of $\boldsymbol{E}/\boldsymbol{W}_{n+1}(\mathbb{K})$ with the $(n+1)$-st coordinate of each vector set to 0, we get that ε_n from Equation (2.5) is in $\mathcal{S}_{6\cdot 2^n}$. The same lemma applied in a similar way gives us that $\tau_n \in \mathcal{S}_{-2^n}$ and therefore $\delta_3 = h^{2^n}\delta_2$ from Equation (2.8) is in $\mathcal{S}_{(3n+3)2^n}$. Therefore, we get that $c_i \in \mathcal{S}_{2^{n+1}-4i}$ for $2^n \leq i \leq M$ Then following the Voloch-Walker algorithm, this gives $d_i \in \mathcal{S}_{3\cdot 2^n - 2i}$ for $2^{n+1} - 1 \leq i \leq N$ and $e_i \in \mathcal{S}_{3\cdot 2^n - 2i - 3}$ for $2^n - 2 \leq i \leq N - \delta$.

Now, we're choosing a_n and h_n, which gives a *unique* solution to the system in the last step of the Voloch-Walker algorithm. Also, by Proposition 2.8, we can take the denominators of the c_i's, the d_i's, the e_i's, and b_n to be powers of bh, which is homogeneous of degree 7. So by splitting the numerators, we can write

$$b_n = b_{n,0} + b_{n,1}$$

$$c_i = c_{i,0} + c_{i,1}$$

$$d_i = d_{i,0} + d_{i,1}$$

$$e_i = e_{i,0} + e_{i,1}$$

where

$$b_{n,0} \in \mathcal{S}_{6\cdot 2^n}, \text{ and no term of } b_{n,1} \text{ is in } \mathcal{S}_{6\cdot 2^n}$$
$$c_{i,0} \in \mathcal{S}_{2^{n+1}-4i}, \text{ and no term of } c_{i,1} \text{ is in } \mathcal{S}_{2^{n+1}-4i}$$
$$d_{i,0} \in \mathcal{S}_{3\cdot 2^n-2i}, \text{ and no term of } d_{i,1} \text{ is in } \mathcal{S}_{3\cdot 2^n-2i}$$
$$e_{i,0} \in \mathcal{S}_{3\cdot 2^n-2i-3}, \text{ and no term of } e_{i,1} \text{ is in } \mathcal{S}_{3\cdot 2^n-2i-3}.$$

Since only terms of the same weight can cancel each other out, we get

$$\begin{aligned}(h_0x_0)^{2^n}\left(\sum_{i=0}^{N'} d_{i,0}x_0^i + y_0\sum_{i=0}^{N''} e_{i,0}x_0^i\right) + (x_0y_0)^{2^n} h_n \\ = (x_0^{2^{n+1}} + (h_0y_0)^{2^n})\sum_{i=0}^{M'} c_{i,0}x_0^{2i} + x_0^{2^{n+1}}a_n + b_{n,0} + \varepsilon_n.\end{aligned}$$

But then this is a solution to Equation (2.9), by uniqueness, it must be the only solution. Therefore we must have $b_{n,1} = c_{i,1} = d_{i,1} = e_{i,1} = 0$. This gives $b_n \in \mathcal{S}_{6\cdot 2^n}$, $F_n \in \mathcal{S}_{2^{n+1}}$, $G_n \in \mathcal{S}_{3\cdot 2^n}$, and $H_n \in \mathcal{S}_{3\cdot 2^n-3}$, which is what we needed to show. □

2.6 A Partial Result

In [Fin20], Finotti notes that in all computed examples, the only factor that appears in the denominator of the Weierstrass coefficients and Teichmüller coordinates is the Hasse invariant. In later papers, this becomes the following conjecture (see [FL20] and [FL21] for some partial results).

Conjecture 2.11. *Let $p \geq 5$, $\mathbb{K} = \mathbb{F}_p(a, b)$, and $\mathfrak{h}$ be the Hasse invariant of*

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

Let the canonical lifting of E be given by

$$\boldsymbol{E}/\boldsymbol{W}(\mathbb{K}) : \boldsymbol{y}^2 = \boldsymbol{x}^3 + (a, a_1, a_2, \dots)\boldsymbol{x} + (b, b_1, b_2, \dots)$$

with associated Teichmüller lift

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

Then as computed in the Voloch-Walker algorithm, $a_n, b_n \in \mathbb{F}_p[a, b, 1/\mathfrak{h}]$ *and* $F_n, H_n \in \mathbb{F}_p[a, b, 1/\mathfrak{h}][x_0]$ *for all* $n \geq 1$*.*

As noted at the end of Section 2.4, all computed examples in characteristic 2 have the same property: the only term in the denominator is a power of h. However, the possibility for a power of b to appear in the denominator is not explicitly disallowed by the algorithm. In fact, on inspection, the linear system *does* appear to require dividing by b. This leads us to make the same conjecture for characteristic 2.

Conjecture 2.12. *As computed by the Voloch-Walker algorithm described in Section 2.2, along with the choice* $a_n = h_n = 0$*, the denominators of* b_n*,* F_n*,* G_n*, and* H_n *are exactly powers of* h*. Equivalently, applying the algorithm to the form in Equation (2.2),* $b_n \in \mathbb{F}_2[a, b]$ *and* $F_n, G_n, H_n \in \mathbb{F}_2[a, b][x_0]$ *for all* $n \geq 1$*.*

All computational evidence collected so far (up to $n = 5$ for $p = 2$) supports this conjecture, but the proof has thus far been elusive. We have narrowed it down to the following condition.

Conjecture 2.13. *Let* $n \geq 1$*, let* $\mathbb{K} = \mathbb{F}_2(a, b, h)$*, and let* $E/\mathbb{K}$ *be as in Equation (2.1). Write the* $(n+1)$*-st coordinate of the Greenberg Transform of* $\boldsymbol{E}$ *as*

$$h^{2^n}(x_0^{2^n} y_n + x_n y_0^{2^n}) + x_0^{2^n} y_0^{2^n} h_n = x_0^{2^{n+1}} x_n + x_0^{2^{n+1}} a_n + b_n + \varepsilon_n.$$

Write $\varepsilon_n = \sum_i r_i x_0^i + y_0 \sum_i s_i x_0^i$ *for* $r_i, s_i \in \mathbb{K}$*. Let* $\nu = \nu_b$ *be the valuation at* b*. Then*

$$\begin{aligned} \nu(r_{2i}) &\geq 2^n - i - 1 \quad \text{for } 0 \leq i < 2^n \\ \nu(s_{2^n - 1}) &\geq 2^n - 1. \end{aligned}$$

Heuristically, this seems likely. For the r_i, we want coefficients of small powers of x_0 to be highly divisible by b. During the Greenberg transform, among other steps, we will be expanding powers of $x_0^3 + hx_0y_0 + ax_0^2 + b$, which would appear to introduce large powers of b in the coefficients of small powers of x_0. And as stated above, this condition holds for all computed examples.

Theorem 2.14. *Assume Conjecture 2.13 and let $R = \mathbb{F}_2[a, b, h, 1/h]$. Then, taking $a_n = h_n = 0$, we have that $b_n \in R$ and $F_n, G_n, H_n \in R[x_0]$ for all $n \geq 1$.*

Proof. For $n = 1$, we can explicitly compute

$$\begin{aligned}
b_1 &= b^2 \\
F_1 &= bh^{-2} \\
G_1 &= h^{-4}\left((ah^2 + h^4)x_0^3 + (ah^4 + b)x_0^2 + b\right) \\
H_1 &= h^{-1}\left(x_0^2 + (a + h^2)x_0\right)
\end{aligned}$$

and so the statement is true for $n = 1$ (regardless of the conjecture). Now, inductively assume the theorem is true for $k < n$. Following the Voloch-Walker algorithm, we write the $(n+1)$-st coordinate of the Greenberg Transform as

$$(h_0x_0)^{2^n}\left(\sum_{i=0}^{N} d_ix_0^i + y_0\sum_{i=0}^{N-2} e_ix_0^i\right) = (x_0^{2^{n+1}} + (h_0y_0)^{2^n})\sum_{i=0}^{M} c_ix_0^{2i} + b_n + \varepsilon_n. \tag{2.11}$$

By the induction hypothesis, we have that $\varepsilon_n \in R[x_0, y_0]$, as ε_n is an integer-polynomial function of the previous coordinates, which are all in R. Since $n > 1$, we must have $\tau^*(\boldsymbol{x}/\boldsymbol{y})$ regular, which, after some calculation, results in the requirement

$$\mathrm{ord}_O\left(x_0^{2^{n+1}}y_0^{(n-1)2^n}x_n + \delta_3\right) > -3(n+1)2^n.$$

Write $\delta_3 = \mathcal{F} + y_0\mathcal{G}$ and $y_0^{(n-1)p^n} = \mathcal{H} + y_0\mathcal{K}$ with $\mathcal{F}, \mathcal{G}, \mathcal{H}, \mathcal{K} \in R[x_0]$. Then we need

$$\begin{aligned}
&\mathrm{ord}_O\left((\mathcal{H} + y_0\mathcal{K})x_0^{2^{n+1}}x_n + \mathcal{F} + y_0\mathcal{G}\right) > -3(n+1)2^n \\
\Rightarrow\ &\mathrm{ord}_O\left((\mathcal{H}x_0^{2^{n+1}}x_n + \mathcal{F}) + y_0(\mathcal{K}x_0^{2^{n+1}}x_n + \mathcal{G})\right) > -3(n+1)2^n
\end{aligned}$$

Terms with y_0 cannot cancel with terms without y_0, so we can split this into two statements.

$$\begin{aligned}
&\operatorname{ord}_O\left(\mathcal{H}x_0^{2^{n+1}}x_n+\mathcal{F}\right)>-3(n+1)2^n \text{ and } \operatorname{ord}_O\left(\mathcal{K}x_0^{2^{n+1}}x_n+\mathcal{G}\right)>-3(n+1)2^n+3\\
\Rightarrow\ &\deg_{x_0}\left(\mathcal{H}x_0^{2^{n+1}}x_n+\mathcal{F}\right)<3(n+1)2^{n-1} \text{ and } \deg_{x_0}\left(\mathcal{K}x_0^{2^{n+1}}x_n+\mathcal{G}\right)<\frac{3(n+1)2^n-3}{2}.
\end{aligned}$$

We can write

$$\mathcal{H}x_n=(x_0^{3(n-1)2^{n-1}}+\cdots)\sum_{i=0}^{M}c_ix_0^{2^{n+1}+2i}.$$

Since the leading coefficient of $\mathcal{H}$ is 1, solving for the c_i for $i\geq 2^{n-1}$ using this requirement gives solutions in R. Note that at this point, we still have not used Conjecture 2.13.

The next step in the algorithm is to equate the remaining coefficients and solve the linear system. Notably, d_i and e_i only occur on the left-hand side of Equation (2.11) and all have a coefficient of h_0. Therefore, if we can show that the right-hand side has coefficients in R, so must the left-hand side. Also, all of the terms on the left-hand side have a power of x_0 of 2^n or higher. So any coefficients attached to a power of x_0 strictly less than 2^n must come entirely from the right-hand side. Our goal now is to analyze those coefficients and show that they give a solution to the linear system of the form we want.

Let $\eta=2^n-1$. Multiplying the sum on the right-hand side by $x_0^{2^{n+1}}$ will result in terms with a power of x_0 greater than η. So we will move those terms to the left-hand side. Then expanding $y_0^{2^n}$ using Lemma 2.3 and again moving all powers of x_0 greater than η to the left-hand side gives the right-hand side as

$$\begin{aligned}
&h^{2^n}\left(\sum_{k=1}^{n}h^{(2^{k-1}-1)2^{n-k+1}}b^{2^{n-k}}x_0^{(2^{k-1}-1)2^{n-k+1}}\right)\left(\sum_{i=0}^{2^{n-1}-1}c_ix_0^{2i}\right)+h^{2^{n+1}-1}c_0x_0^{2^n-1}y_0+b_n+\varepsilon_n\\
&=\sum_{k=1}^{n}\sum_{i=0}^{2^{n-1}-1}h^{2^{n+1}-2^{n-k+1}}b^{2^{n-k}}c_ix_0^{2^n-2^{n-k+1}+2i}+h^{2^{n+1}-1}c_0x_0^{2^n-1}y_0+b_n+\varepsilon_n\\
&=\sum_{j=0}^{2^n-2}\left(\sum_{\substack{i\geq 0,k>0\\ 2^{n-1}-2^{n-k}+i=j}}h^{2^{n+1}-2^{n-k+1}}b^{2^{n-k}}c_i\right)x_0^{2j}+h^{2^{n+1}-1}c_0x_0^{2^n-1}y_0+b_n+\varepsilon_n.
\end{aligned}$$

We move all terms with $j > \eta$ to the LHS and are left with

$$\sum_{j=0}^{2^{n-1}-1} \left(\sum_{k=1}^{n-\lceil \log_2(2^{n-1}-j) \rceil} h^{2^{n+1}-2^{n-k+1}} b^{2^{n-k}} c_{j-2^{n-1}+2^{n-k}} \right) x_0^{2j} + h^{2^{n+1}-1} c_0 x_0^{2^n-1} y_0 + b_n + \varepsilon_n.$$

Now we write $\varepsilon_n = \sum_i r_i x_0^i + y_0 \sum_i s_i x_0^i$ and move all its terms with a power of x_0 greater than η to the left-hand side. Then we have

$$\sum_{j=1}^{2^{n-1}-1} \left(r_{2j} + \sum_{k=1}^{n-\lceil \log_2(2^{n-1}-j) \rceil} h^{2^{n+1}-2^{n-k+1}} b^{2^{n-k}} c_{j-2^{n-1}+2^{n-k}} \right) x_0^{2j}$$
$$+ (h^{2^{n+1}-1} c_0 + s_{2^n-1}) x_0^{2^n-1} y_0 + (b_n + h^{2^n} b^{2^{n-1}} c_0 + r_0) = 0.$$

This expression being zero means that all the coefficients are zero. Here is where Conjecture 2.13 finally comes in. First, since $h^{2^{n+1}-1} c_0 + s_{2^n-1} = 0$, we get that $c_0 \in R$ and $\nu_b(c_0) \geq 2^n - 1$. This gives right away that $b_n \in R$. Now, turning our attention to the summation coefficients, for each j, we have

$$b^{2^{n-1}} c_j = \frac{1}{h^{2^n}} \left(r_{2j} + \sum_{k=2}^{n-\lceil \log_2(2^{n-1}-j) \rceil} b_0^{2^{n-k}} c_{j-2^{n-1}+2^{n-k}} \right).$$

For $j = 1$, this gives $b^{2^{n-1}} c_1 = h^{-2^n} r_2$, and so $\nu_b(c_1) = \nu_b(r_2) - 2^{n-1} \geq 2^{n-1} - 2$. Now, inductively suppose that for $i < j$, $\nu_b(c_i) \geq 2^{n-1} - i - 1$. Then we have

$$\nu(c_j) \geq \min \left\{ \nu_b(r_{2j}),\ \min_k \{2^{n-k} + 2^{n-1} - (j - 2^{n-1} + 2^{n-k}) - 1\} \right\} - 2^{n-1}$$
$$= 2^n - j - 1 - 2^{n-1} = 2^{n-1} - j - 1 \geq 0.$$

So we have $c_j \in R$ for all $0 \leq j \leq 2^{n-1} - 1$ which is the rest of the c_j and so by the reasoning above, we have $d_i, e_i \in R$ as well, completing the proof. $\square$

Chapter 3

Canonical Liftings in Odd Characteristic

Our goals in this chapter are two-fold. First, we prove results similar to those in Chapter 2 for characteristic 3. Second, we collect some other results that apply to curves in characteristic 5 and greater.

To start, let $\Bbbk$ be a field of characteristic 3, let $E/\Bbbk$ be an ordinary elliptic curve, and let $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$ be its canonical lifting. Our first goal is to investigate properties of the Weierstrass coefficients and Teichmüller lift of $\boldsymbol{E}$.

3.1 Weierstrass Form in Characteristic 3

We start by giving the form for E that will be useful to us.

Proposition 3.1. *Any ordinary elliptic curve $E/\Bbbk$ is isomorphic to a curve of the form*

$$E'/\Bbbk : y^2 = x^3 + ax^2 + b \tag{3.1}$$

with $a, b \neq 0$.

Proof. Since $\mathrm{char}(\Bbbk) \neq 2$, we know that we can let $E/\Bbbk$ be given by

$$E/\Bbbk : y^2 = x^3 + b_2x^2 + b_4x + b_6.$$

The Hasse invariant of this curve is $\mathfrak{h} = b_2$, which is non-zero since E is ordinary. So we can apply the isomorphism given by $x \mapsto x + \frac{b_4}{b_2}$, which gives

$$E'/\Bbbk : y^2 = x^3 + b_2 x^2 + \frac{-b_2^3 b_6 + b_2^2 b_4^2 - b_4^3}{b_2^3}.$$

Renaming variables gives the form we want. Then the Hasse invariant of E is $\mathfrak{h} = a$ and the discriminant is $\Delta = 2a^3 b$. This means, since $\Delta \neq 0$, we have that both $a \neq 0$ and $b \neq 0$, i.e. *every* curve of this form is ordinary. $\square$

In all sections about characteristic 3, we will only ever use the form in Equation (3.1).

Proposition 3.2. *The curve $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$ is isomorphic to*

$$\boldsymbol{E}'/\boldsymbol{W}(\Bbbk) : \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x}^2 + \boldsymbol{b} \tag{3.2}$$

where

$$\boldsymbol{a} = (a, a_1, \ldots), \text{ and } \boldsymbol{b} = (b, b_1, \ldots).$$

Proof. Let $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$ be given by

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

Since $\boldsymbol{E}$ reduces to E mod 3, we have that

$$\boldsymbol{a} = (a, a_1, a_2, \ldots) \quad \text{and} \quad \boldsymbol{b} = (b, b_1, b_2, \ldots)$$

and

$$\boldsymbol{c} = (0, c_1, c_2, \ldots), \ \ \boldsymbol{d} = (0, d_1, d_2, \ldots), \ \text{ and } \ \boldsymbol{e} = (0, e_1, e_2, \ldots).$$

By Proposition 1.10, $2 \in \boldsymbol{W}(\Bbbk)^\times$, so we can apply the standard "completing the square" isomorphism, i.e. $\boldsymbol{y} \mapsto \frac{1}{2}(\boldsymbol{y} - \boldsymbol{c}\boldsymbol{x} - \boldsymbol{d}\boldsymbol{x})$. Since $c_0 = d_0 = 0$, this isomorphism maintains the values of a_0 and b_0. So we have the form

$$\boldsymbol{E}'/\boldsymbol{W}(\Bbbk) : \boldsymbol{y}^2 = \boldsymbol{x}^3 + (a, a_1', a_2', \ldots)\boldsymbol{x}^2 + (0, e_1', e_2', \ldots)\boldsymbol{x} + (b, b_1', b_2', \ldots).$$

Now, consider $\boldsymbol{r} = (0, r_1, r_2, \ldots) \in \boldsymbol{W}(\Bbbk)$ and apply the isomorphism $\boldsymbol{x} \mapsto \boldsymbol{x} + \boldsymbol{r}$. This gives the new equation

$$\boldsymbol{E}''/\boldsymbol{W}(\Bbbk) : \boldsymbol{y}^2 = \boldsymbol{x}^3 + (\boldsymbol{a} + 3\boldsymbol{r})\boldsymbol{x}^2 + (3\boldsymbol{r}^2 + 2\boldsymbol{a}\boldsymbol{r} + \boldsymbol{e})\boldsymbol{x} + (\boldsymbol{a}\boldsymbol{r}^2 + \boldsymbol{r}^3 + \boldsymbol{e}\boldsymbol{r} + \boldsymbol{b}).$$

Since $r_0 = 0$, this isomorphism will again maintain the values of a_0 and b_0 in the first coordinate. So we just need to show that there is some $\boldsymbol{r} \in \boldsymbol{W}(\Bbbk)$ so that $3\boldsymbol{r}^2 + 2\boldsymbol{a}\boldsymbol{r} = -\boldsymbol{e}$. Consider $3\boldsymbol{r}^2 + 2\boldsymbol{a}\boldsymbol{r} = \boldsymbol{r}(3\boldsymbol{r} - \boldsymbol{a})$. We have that $3\boldsymbol{r} = (0, 0, r_1^3, r_2^3, \ldots)$ and so we can write

$$3\boldsymbol{r} - \boldsymbol{a} = (-a_0,\ f_1(a_0, a_1),\ f_2(a_0, a_1, a_2, r_1), \ldots,\ f_n(a_0, \ldots, a_n, r_1, \ldots, r_{n-1}), \ldots)$$

where each f_i is a polynomial with integer coefficients. Then

$$\begin{aligned}\boldsymbol{r}(3\boldsymbol{r} - \boldsymbol{a}) &= (0,\ P_1(0, r_1, a_0, f_1),\ P_2(0, r_1, r_2, a_0, f_1, f_2),\ P_3(0, r_1, r_2, r_3, a_0, f_1, f_2, f_3), \ldots) \\ &= \Big(0,\ g_1(a_0, a_1) - a_0^3 r_1,\ g_2(r_1, a_0, a_1, a_2) - a_0^{3^2} r_2,\ g_3(r_1, r_2, a_0, \ldots, a_3) - a_0^{3^3} r_3, \ldots\Big)\end{aligned}$$

where now each g_i is a polynomial with integer coefficients. So we end up needing to solve the system of equations

$$\begin{aligned} a_0^3 r_1 &= e_1 + g_1(a_0, a_1) \\ a_0^{3^2} r_2 &= e_2 + g_2(r_1, a_0, a_1, f_2) \\ &\vdots \\ a_0^{3^n} r_n &= e_n + g_2(r_1, \ldots, r_{n-1}, a_0, \ldots, a_n) \\ &\vdots \end{aligned}$$

Since $a_0 = a \neq 0$, this system has a solution. So there is some $\boldsymbol{r} \in \boldsymbol{W}(\Bbbk)$ so that $3\boldsymbol{r}^2 + 2\boldsymbol{a}\boldsymbol{r} + \boldsymbol{e} = 0$ and thus we have

$$\boldsymbol{E}''/\boldsymbol{W}(\Bbbk) : \boldsymbol{y}^2 = \boldsymbol{x}^3 + (\boldsymbol{a} + 3\boldsymbol{r})\boldsymbol{x}^2 + (\boldsymbol{a}\boldsymbol{r}^2 + \boldsymbol{r}^3 + \boldsymbol{e}\boldsymbol{r} + \boldsymbol{b}).$$

Renaming variables gives the form we want. $\square$

3.2 Choosing a Solution in the Voloch-Walker Algorithm in Characteristic 3

The Voloch-Walker algorithm in characteristic 3 is effectively identical to the algorithm described in [Fin20], except that $f(x) = x^3 + ax^2 + b$, which slightly changes the Greenberg Transform. Otherwise the procedure is unchanged. However, we can perform the same analysis as in Section 6 of [Fin20] and Chapter 2 of this dissertation to get a slightly nicer result than for $p \geq 5$.

Proposition 3.3. *The linear system in the last step of the Voloch-Walker algorithm in characteristic* 3 *has one free parameter, which can be assigned to either the value of* a_n *or* $c_{3^{n-1}}$*.*

Proof. Let $\mathbb{K} = \mathbb{F}_2(a, b)$. Suppose we have computed a_i, b_i, F_i, and H_i for $i < n$ and that we have two solutions to the system given by

$$\begin{gathered}(a_n, b_n, c_0, \ldots, c_{M'}, d_0, \ldots, d_{N'}) \\ \text{and } (a'_n, b'_n, c'_0, \ldots, c'_{M'}, d'_0, \ldots, d'_{N'}).\end{gathered}$$

where $N' = (3^n - 1)/2$ and $M' = 2 \cdot 3^{n-1} - 3$. Consider the curves given by these two solutions, say

$$\begin{aligned}\boldsymbol{E}/W_{n+1}(\mathbb{K}) &: \boldsymbol{y}^2 = \boldsymbol{x}^3 + (a, \ldots, a_{n-1}, a_n)\boldsymbol{x}^2 + (b, \ldots, b_{n-1}, b_n) \\ \boldsymbol{E'}/W_{n+1}(\mathbb{K}) &: \boldsymbol{y'}^2 = \boldsymbol{x'}^3 + (a, \ldots, a_{n-1}, a'_n)\boldsymbol{x'}^2 + (b, \ldots, b_{n-1}, b'_n).\end{aligned}$$

Since $\boldsymbol{E}$ and $\boldsymbol{E'}$ are isomorphic, we must have $\boldsymbol{u} \in W_{n+1}(\mathbb{K})^\times$ and $\boldsymbol{r}, \boldsymbol{s}, \boldsymbol{t} \in W_{n+1}(\mathbb{K})$ such that

$$\boldsymbol{x} = \boldsymbol{u}^2\boldsymbol{x'} + \boldsymbol{r} \text{ and } \boldsymbol{y} = \boldsymbol{u}^3\boldsymbol{y'} + \boldsymbol{u}^2\boldsymbol{s}\boldsymbol{x'} + \boldsymbol{t}.$$

Note that modulo 3^n, $\boldsymbol{E}$ and $\boldsymbol{E'}$ are actually *identical*, not just isomorphic, so we must have

$$\boldsymbol{u} \equiv 1 \pmod{3^n} \quad \text{and} \quad \boldsymbol{r} \equiv \boldsymbol{s} \equiv \boldsymbol{t} \equiv 0 \pmod{3^n}$$

that is

$$\boldsymbol{u} = (1, 0, \ldots, 0, u); \quad \boldsymbol{r} = (0, 0, \ldots, 0, r); \quad \boldsymbol{s} = (0, 0, \ldots, 0, s); \quad \boldsymbol{t} = (0, 0, \ldots, 0, t)$$

with $u, r, s, t \in \mathbb{K}$. Substituting these values into the equation for $\boldsymbol{E}$, we get

$$\begin{aligned}\boldsymbol{E'}/W_{n+1}(\mathbb{K}) : \boldsymbol{y'}^2 + (0, \ldots, 0, -s)\boldsymbol{x'}\boldsymbol{y'} + (0, \ldots, 0, -t)\boldsymbol{y} \\ = \boldsymbol{x'}^3 + (a, \ldots, a_{n-1}, a_n + ua^{3^n})\boldsymbol{x'}^2 + (0, \ldots, 0, -ra^{3^n})\boldsymbol{x} + (b, \ldots, b_{n-1}, b_n).\end{aligned}$$

We immediately see that we must have $s = r = t = 0$, as $a \neq 0$ and the coefficients of $\boldsymbol{x'}\boldsymbol{y'}$, $\boldsymbol{y}$, and $\boldsymbol{x}$ in $\boldsymbol{E'}$ are zero. Simplifying gives

$$\boldsymbol{E'}/W_{n+1}(\mathbb{K}) : \boldsymbol{y'}^2 = \boldsymbol{x'}^3 + (a, \ldots, a_{n-1}, a_n + ua^{3^n})\boldsymbol{x'}^2 + (b, \ldots, b_{n-1}, b_n).$$

So we have $a'_n = a_n + ua^{3^n}$ and $b'_n = b_n$. Now, the Greenberg Transform of $\boldsymbol{E}$ is

$$2y_0^{3^n+1}H_n = (2ax_0)^{3^n}F_n + a_n x_0^{2\cdot 3^n} + b_n + \varepsilon_n \tag{3.3}$$

where $\varepsilon_n \in \mathbb{F}_p(a, b)$ contains all the terms not involving a_n, b_n, x_n, or y_n. With these values, subtracting equations for $(n+1)$-st coordinate of the Greenberg Transforms of $\boldsymbol{E}$ and $\boldsymbol{E'}$ and substituting the appropriate expressions (with unknowns) for F_n and H_n gives

$$f^{\frac{3^n+1}{2}}\left(\sum_{i=0}^{N'}(d'_i - d_i)x_0^i\right) = (ax_0)^{3^n}\left(\sum_{i=0}^{M'}(c'_i - c_i)x_0^{3i}\right) - ua^{3^n}x_0^{2\cdot 3^n}. \tag{3.4}$$

Taking $c'_i = c_i$ if $i \neq 3^{n-1}$ and $c'_{3^{n-1}} = c_{3^{n-1}} + u$, Equation (2.5) becomes

$$f^{\frac{3^n+1}{2}}\left(\sum_{i=0}^{N'}(d'_i - d_i)x_0^i\right) = 0.$$

This shows that we must have $d_i = d'_i$ for all i and so we see that the nullspace of the coefficient matrix has dimension 1 and is generated by

$$(a^{3^n}, 0, 0, \ldots, 0, 1, 0, \ldots, 0)$$

where 1 appears in the coordinate corresponding to c_{3^n-1}. $\square$

So, similar to the case where $p \geq 5$, we can choose the value of either a_n or c_{3^n-1} (notably we *cannot* choose b_n). Unlike the $p \geq 5$ case though, we know that $a \neq 0$, so choosing the value of a_n is available regardless of the curve we started with! Thus we can make the "simplest" choice and take $a_n = 0$.

Throughout, we have been using Equation (3.1). But actually, if a is a square in $\Bbbk$, E is isomorphic to

$$E''/\Bbbk : y^2 = x^3 + x^2 + d \tag{3.5}$$

where $d = b/a^3$ (via $x \mapsto ax$ and $y \mapsto a^{3/2}y$). So, in some sense, E is almost isomorphic to a curve with $a = 1$. This gives some intuition for why we can choose $a_n = 0$ at every step. If $a = 1$, then the coefficient of $\boldsymbol{x}^2$ in $\boldsymbol{E}$ would be $\mathbf{1} = (1, 0, 0, \ldots)$.

3.3 Universality and Modularity in Characteristic 3

In this section, our goal is to show that a_n, b_n, F_n, G_n, and H_n are universal modular functions of specific weights. To clarify this statement, we make the following definitions.

Definition 3.4. The set of ordinary coefficients over $\Bbbk$ is defined to be

$$\Bbbk^2_{\text{ord}} \coloneqq \{(a_0, b_0) \in \Bbbk^2 : \text{the elliptic curve } E/\Bbbk \text{ defined by } y^2 = x^3 + a_0x^2 + b_0 \text{ is ordinary.}\}$$

Note that in this definition, we are implicitly assuming that E is non-singular as well. So while the statement of this definition is very general, by the reasoning in Section 3.1, we have that $\Bbbk^2_{\text{ord}} = \{(a_0, b_0) \in \Bbbk^2 : a_0 \neq 0 \text{ and } b_0 \neq 0\}$.

Definition 3.5. A rational function $f \in \mathbb{F}_2(a, b)$ is called *universal* if it is defined for all $(a_0, b_0) \in \Bbbk^2_{\text{ord}}$.

Also, we define $\text{wgt}(a) \coloneqq 2$, $\text{wgt}(b) \coloneqq 6$, $\text{wgt}(x_0) \coloneqq 2$, and $\text{wgt}(y_0) \coloneqq 3$. This allows us to define

Definition 3.6. The *modular functions of weight n* (over $\mathbb{F}_3(a,b,x_0,y_0)$) are

$$\mathcal{S}_n := \left\{ \frac{f}{g} : f, g \in \mathbb{F}_3[a,b,x_0,y_0] \text{ homogeneous and } \mathrm{wgt}(f) - \mathrm{wgt}(g) = n \right\} \cup \{0\}.$$

Lemma 3.7. *If $f \in \mathbb{F}_3(a,b)$ is universal, then $f \in \mathbb{F}_3[a,b,1/(ab)]$.*

Proof. Suppose not and let $g \in \mathbb{F}_3[a,b]$ be an irreducible factor of the denominator of f other than a and b. Let $\Bbbk = \overline{\mathbb{F}_3}$. Then $V := \{g(a,b) = 0\}$ is a variety of positive dimension over $\Bbbk$ and thus $|V| = \infty$. Furthermore, since $(g,a) = 1$ and $(g,b) = 1$, by Bézout's Theorem, $|V \cap \{a = 0\}| < \infty$ and $|V \cap \{a = 0\}| < \infty$, so $|V \cap \{a = 0\} \cap \{b = 0\}| < \infty$. So there is some $(a_0, b_0) \in \Bbbk^2$ such that $g(a_0, b_0) = 0$ and $a_0, b_0 \neq 0$. But then

$$E/\overline{\mathbb{F}_3} : y^2 = x^3 + a_0 x^2 + b_0$$

is an ordinary elliptic curve, so $(a_0, b_0) \in \Bbbk^2_{\mathrm{ord}}$, contradicting the universality of f. Thus we must have $f \in \mathbb{F}_3[a,b,1/(ab)]$. $\square$

Proposition 3.8. *Let $\mathbb{K} = \mathbb{F}_3(a,b)$ and let $\mathbb{L} := \mathbb{F}_3[a,b,1/(ab)]$. Then there are $a_n, b_n, \in \mathbb{L}$ and $F_n, H_n \in \mathbb{L}[x_0]$ for all $n \geq 1$ such that the canonical lifting of $E/\mathbb{K}$ is given by*

$$\boldsymbol{E}/\boldsymbol{W}(\mathbb{K}) : y^2 = x^3 + (a, a_1, a_2, \ldots)x^2 + (b, b_1, b_2, \ldots)$$

and the associated Teichmüller lift is given by

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

Proof. Inductively suppose we have $a_i, b_i \in \mathbb{L}$ and $F_i, H_i \in \mathbb{L}[x_0]$ for all $i < n$.

Choosing $a_n = 0$ immediately gives $a_n \in \mathbb{L}$. As can be seen in the proof of Proposition 3.3, b_n is not affected by the choice of a_n. Therefore b_n must be universal and so by Lemma 3.7 we have $b_n \in \mathbb{L}$.

Consider Equation (3.3). By induction, we must have that all the terms contained in ε_n are in $\mathbb{L}$. By the same logic as in Proposition 2.8, the c_i determined by the condition on $\tau^*(x/y)$ are in $\mathbb{L}$. By the reasoning in the proof of Proposition 3.3, we must have that

$c'_i = c_i$ for all $i \neq 3^{n-1}$ and $d'_i = d_i$. Therefore all these coefficients must be universal as well, showing $H_n \in \mathbb{L}$ and nearly showing $F_n \in \mathbb{L}$. At this stage, we are left with one unknown remaining, $c_{3^{n-1}}$. We end up with an equation of the form

$$ac_{3^{n-1}}x_0^{2\cdot 3^n} = \cdots$$

where everything on the right-hand side is in $\mathbb{L}$. So solving for $c_{3^{n-1}}$ only involves dividing by a, which keeps us in $\mathbb{L}$. Therefore $F_n \in \mathbb{L}$, which finishes the proof. □

Proposition 3.9. *If we choose $a_n \in \mathcal{S}_{2\cdot 3^n}$ in each step of the Voloch-Walker algorithm, then $b_n \in \mathcal{S}_{6\cdot 3^n}$, $F_n \in \mathcal{S}_{2\cdot 3^n}$, and $H_n \in \mathcal{S}_{3^{n+1}-3}$ for all $n \geq 0$.*

Note. Since we are choosing $a_n = 0$ at every step, we satisfy the conditions of this statement, but there are many choices that guarantee modularity.

Proof. The proof of this is essentially identical to the proof of Proposition 8.1 in [Fin20] and to the proof of Proposition 2.10, with small changes made to account for the different Weierstrass equation. □

Note that just like the characteristic 2 case, if we had instead started with Equation (3.5), we would *not* get modular functions, as this Weierstrass equation is not in $\mathcal{S}_6$.

3.4 Some Results and Conjectures in Odd Characteristic

In [Fin20], [FL20], [FL21], and [FL23] Finotti and Li proved many results about the canonical lifting of elliptic curves over fields of characteristic 5 and greater. In this section, we add to those results and posit two conjectures.

Throughout this section, unless otherwise specified, let $p \geq 5$ be prime, $\mathbb{K} = \mathbb{F}_p(a, b)$, and $\mathfrak{h}$ be the Hasse invariant of

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

Let the canonical lifting of E be given by

$$\boldsymbol{E}/\boldsymbol{W}(\mathbb{K}) : \boldsymbol{y}^2 = \boldsymbol{x}^3 + (a, a_1, a_2, \ldots)\boldsymbol{x} + (b, b_1, b_2, \ldots)$$

with associated Teichmüller lift

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

3.4.1 Results

In Theorem 6.4 [Fin14], Finotti proves a formula for the Greenberg Transform of a function $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$. Our goal is to extend that formula to allow $\boldsymbol{f}$ to have a monomial in the denominator (or equivalently, to have terms with negative exponents on $\boldsymbol{x}$ and $\boldsymbol{y}$). This allows us to more easily compute $\tau^*(\boldsymbol{x}/\boldsymbol{y})$ in the Voloch-Walker algorithm, among other things. The proof of this theorem relies on Theorem 3.2 of [Fin11], which we reproduce here.

Theorem 3.10. *Let $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$ and suppose the Greenberg Transform of f is given by $(f_0, f_1, \ldots)$. Then, if*

$$w_n(\boldsymbol{f}_0, \ldots, \boldsymbol{f}_n) \equiv \boldsymbol{f}^{\sigma^n}(w_n(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n), w_n(\boldsymbol{y}_0, \ldots, \boldsymbol{y}_n)) \pmod{p^{n+1}}$$

(with w_n the nth Witt polynomial and σ the Frobenius on $\boldsymbol{W}(\Bbbk)$) for some $f_i \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n, \boldsymbol{y}_0, \ldots, \boldsymbol{y}_n]$, then $\boldsymbol{f}_i$ reduces to f_i modulo p.

If we can extend this theorem to $\boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}, 1/(\boldsymbol{x}\boldsymbol{y})]$, then we can extend Theorem 6.4 of [Fin14] to the same ring.

Proposition 3.11. *The formula for the Greenberg Transform given in Theorem 6.4 of [Fin14] also holds for $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}, 1/(\boldsymbol{x}\boldsymbol{y})]$, that is, we can have a monomial in the denominator and the formulas will still hold.*

Proof. As stated above, we need to show that Theorem 3.10 holds for $\boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}, 1/(\boldsymbol{x}\boldsymbol{y})]$. Then the proof of Theorem 6.4 given in [Fin14] will also work for this larger class of functions. Since we know Theorem 3.10 holds for $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$, it suffices to show that it holds for $1/\boldsymbol{x}$ or $1/\boldsymbol{y}$. Then sums and products will give us the rest of the functions in $\boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}, 1/(\boldsymbol{xy})]$, as the sum and product polynomials are defined the by the w_n.

Suppose we have $\boldsymbol{f}_0, \ldots, \boldsymbol{f}_n \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}, 1/(\boldsymbol{xy})]$ such that

$$w_n(\boldsymbol{f}_0, \ldots, \boldsymbol{f}_n) \equiv \frac{1}{w_n(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n)} \pmod{p^{n+1}}.$$

Then

$$\begin{aligned} & w_n(\boldsymbol{f}_0, \ldots, \boldsymbol{f}_n) \cdot w_n(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n) \equiv 1 \pmod{p^{n+1}} \\ \Rightarrow \quad & w_n(P_0(\boldsymbol{f}_0, \boldsymbol{x}_{\boldsymbol{0}}), \ldots, P_n(\boldsymbol{f}_0, \ldots, \boldsymbol{f}_n, \boldsymbol{x}_0, \ldots, \boldsymbol{x}_n)) \equiv 1 \pmod{p^{n+1}} \end{aligned}$$

Applying Theorem 3.10 to this gives that $P_0(\boldsymbol{f}_0, \boldsymbol{x}_{\boldsymbol{0}}) \equiv 1 \pmod{p}$ and for all $0 < i \leq n$, $P_i(\boldsymbol{f}_0, \ldots, \boldsymbol{f}_i, \boldsymbol{x}_0, \ldots, \boldsymbol{x}_i)) \equiv 0 \pmod{p}$. This is exactly the calculation that one does to compute $1/\boldsymbol{x}$, and so if the Greenberg Transform of $1/\boldsymbol{x}$ is given by $(f_0, f_1, \ldots)$, we must have that $\boldsymbol{f}_i$ reduces to f_i modulo p for all i. The same argument works for $1/\boldsymbol{y}$, which finishes the proof. □

In Theorem 5.3 of [Fin02], Finotti proves a condition on F_2 that is equivalent to $\tau^*(\boldsymbol{x}/\boldsymbol{y})$ having a zero at infinity. For $n \leq 2$, this condition removes the need to actually compute $\tau^*(\boldsymbol{x}/\boldsymbol{y})$ during the Voloch-Walker algorithm. Finotti asked whether we could get a similar condition for $n = 3$. He had the idea to investigate $\tau^*(1/\boldsymbol{x})$ and $\tau^*(1/\boldsymbol{y})$, as these must both also have a zero at infinity and are easier to calculate than $\tau^*(\boldsymbol{x}/\boldsymbol{y})$. We give a partial answer to that question here.

Proposition 3.12. *The requirement that $\tau^*(1/\boldsymbol{x})$ has a zero at infinity determines the coefficients of x^{ip} in F_n for $i \geq 2p^{n-1}$.*

The requirement that $\tau^*(\boldsymbol{x}/\boldsymbol{y})$ has a zero at infinity determines the same coefficients for $i \geq (3p^{n-1}+1)/2$. This is a *larger* set of coefficients than $i \geq 2p^{n-1}$, so $\tau^*(1/\boldsymbol{x})$ being regular doesn't guarantee that we get a canonical lifting. The author is unsure if there is a stronger requirement we can impose on $\tau^*(1/\boldsymbol{x})$, but it seems likely as $1/\boldsymbol{x}$ has a zero of multiplicity *two* at infinity. So it's possible that there is a stricter order requirement on the components of $\tau^*(1/\boldsymbol{x})$ that is sufficient to give a canonical lifting.

Proof of Proposition 3.12. We start by computing $1/\boldsymbol{x} = (z_0, z_1, \ldots)$. Firstly, we have that $z_0 = 1/x_0$. Then for any $n \geq 1$, we have

$$\begin{aligned}
0 &= P_n(\boldsymbol{x}, 1/\boldsymbol{x}) \\
&= \frac{1}{p^n}\left[(x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n)(z_0^{p^n} + pz_1^{p^{n-1}} + \cdots + p^n z_n) - 1\right] \\
&\equiv \frac{1}{p^n}\left[x_0^{p^n}(pz_1^{p^{n-1}} + \cdots + p^n z_n) + px_1^{p^{n-1}}(z_0^{p^n} + \cdots + p^{n-1}z_{n-1}^p) + \cdots + p^n x_n z_0^{p^n}\right].
\end{aligned}$$

where the equivalence in the last line is modulo p. Note that, as usual with Witt vectors, this expression has integer coefficients, despite the denominators of p. Solving this for z_n, we get $z_n = -x_n/(x_0^{2p^n}) +$ *a rational function not involving* x_n. Also, by Lemma 5.1 of [Fin20], we can write this as

$$z_n = \frac{-x_0^{(n-1)p^n} x_n + \text{ a polynomial in } x_0, \ldots, x_{n-1}}{x_0^{(n+1)p^n}}.$$

Now we impose the requirement that $\tau^*(1/\boldsymbol{x})$ has a zero at infinity. That is

$$\begin{aligned}
&\operatorname{ord}_O\left(\frac{-x_0^{(n-1)p^n} x_n + \text{ a polynomial in } x_0, \ldots, x_{n-1}}{x_0^{(n+1)p^n}}\right) \\
\Rightarrow\ &\operatorname{ord}_O\left(-x_0^{(n-1)p^n} x_n + \cdots\right) > -2(n+1)p^n \\
\Rightarrow\ &\deg_{x_0}\left(-x_0^{(n-1)p^n} x_n + \cdots\right) < (n+1)p^n.
\end{aligned}$$

Now, as in the Voloch-Walker algorithm, we can write $x_n = \hat{F}_n + \sum_{i=0}^{M} c_i x_0^{ip}$. Therefore the degree requirement will determine the c_i where $(n-1)p^n + ip \geq (n+1)p^n$, i.e. $i \geq 2p^{n-1}$. $\square$

3.4.2 Conjectures

In [Fin20], Finotti stated the following.

Conjecture 3.13. *As computed in the Voloch-Walker algorithm, $a_n, b_n \in \mathbb{F}_p[a, b, 1/\mathfrak{h}]$ and $F_n, H_n \in \mathbb{F}_p[a, b, 1/\mathfrak{h}][x_0]$ for all $n \geq 1$.*

Conjecture 2.12 is essentially the same statement for characteristic 2 and we can extend Conjecture 3.13 to characteristic 3 as long as we change the Weierstrass equation accordingly.

These conjectures are supported by all computations done to date, which are summarized in the Table 3.1 (next page). This table lists the prime and the highest value of n for which we have computed the Weierstrass coefficients *and* the Teichmüller lift coordinates. These values of n are relatively small because operations with Witt vectors are computationally expensive, both in processor time and memory. The computations were done at various points in both SageMath versions 9.2 – 9.8 and Magma versions 2.26 and 2.27. The files containing these polynomials are available upon request.

At this time, proofs for these conjectures are elusive. Proving any one of them requires analysis of solutions to large linear systems that are quite opaque. In fact, even computing small examples does not clarify things. For example, for $p = 3$ and $n = 2$, after we ensure the regularity of $\tau^*(\boldsymbol{x}/\boldsymbol{y})$, we have to solve a linear system of the form

$$\left(\begin{array}{c|c}
\begin{matrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & -a^{3^2} & 0 & \cdots & 0 \\ 0 & 0 & 0 & -a^{3^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \cdots & -a^{3^2} \end{matrix} & \begin{matrix} 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & b^{\frac{3^n+1}{2}} \\ * & \cdots & * & * \\ * & \cdots & * & * \\ \vdots & \vdots & \vdots & \vdots \\ * & \cdots & * & * \end{matrix} \\ \hline
\Large 0 & \begin{array}{c|c} \begin{matrix} 1 & 0 & 0 & \cdots & 0 \\ * & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & 1 \end{matrix} & \Large 0 \\ \hline \Large * & \Large D \end{array}
\end{array}\right)
\begin{pmatrix} a_n \\ b_n \\ c_0 \\ c_1 \\ \vdots \\ c_4 \\ \hline d_{15} \\ d_{14} \\ \vdots \\ d_7 \\ \hline d_6 \\ \vdots \\ d_0 \end{pmatrix}
=
\begin{pmatrix} 0 \\ * \\ * \\ * \\ \vdots \\ * \\ \hline * \\ * \\ \vdots \\ * \\ \hline * \\ \vdots \\ * \end{pmatrix}$$

Table 3.1: Computed Canonical Liftings

Prime(s)	Highest computed n
2	5
3	4
5	3
7 - 13	2
17 - 997	1

where

$$D = \begin{pmatrix} -a & 1 & 0 & 0 & 0 & 0 & 0 \\ a^2 & -a & 1 & 0 & 0 & 0 & 0 \\ -a^4 - ab & a^3 - b & a^2 & -a & 1 & 0 & 0 \\ a^5 & -a^4 - ab & a^3 - b & a^2 & -a & 1 & 0 \\ -a^4 b & -a^3 b + b^2 & a^5 & -a^4 - ab & a^3 - b & a^2 & -a \\ b^5 & 0 & -ab^4 & -b^4 & a^2 b^3 & -ab^3 & a^3 b^2 + b^3 \\ 0 & 0 & 0 & b^5 & 0 & -ab^4 & -b^4 \end{pmatrix}$$

and all the $*$s are elements of $\mathbb{F}_p(a,b)$. So the determinant of the coefficient matrix is $(-a^{3^2})^5 \det(D) = a^{49} b^9$. In fact, there are many choices for D, as there are more coefficients than unknowns, and so the system is overdetermined (interestingly this only happens for $p = 3$). The computation above shows one of these choices, but there is *no choice* for $n = 2$ that eliminates b from the determinant of the coefficient matrix. Thus by Cramer's Rule, a denominator of b will show up! But mysteriously, these powers of b cancel.

Computational evidence also led to the following conjecture.

Conjecture 3.14. *Let $p \geq 5$. Let h be an irreducible factor of $\mathfrak{h}$ and ν_h be the valuation at h on $\mathbb{F}_p(a,b)$. Then*

$$\nu_h(a_n), \nu_h(b_n), \nu_h(F_n), \nu_h(H_n) \geq -(np^{n-1} + (n-1)p^{n-2}).$$

Furthermore, $\nu_h(F_1') = -1$ and for $n \geq 2$, we have

$$\nu_h(F_n') \geq -\left[(n-1)p^{n-1} + (n-3)p^{n-2} - 2p\left(\frac{p^{n-3}-1}{p-1}\right)\right].$$

Both of these bounds are sharp.

Note. The statement about F_n' can be proved from the first statement. It follows from the properties of valuations.

This conjecture was proved for a_1 and b_1 in [FL23]. Also, these bounds are the same bounds that are given in [FL21] in Corollaries 2.2 and 6.2. However, the A_i and B_i referred to by Li and Finotti are computed using the so-called "j-invariant method." Despite the different algorithm, this result seems to add support to our conjecture. (See Section 2 of [Fin20] for an explanation of the j-invariant algorithm, or Section 1 of [FL23] for a summary of the both of the algorithms.)

3.5 An Alternative Algorithm in Characteristic 5 and Greater

The algorithm described here was first proposed by Finotti during a meeting in 2022.

As stated above, we have computational evidence for Conjecture 3.13 and Conjecture 3.14. We also have Proposition 8.1 of [Fin20], which gives that a_i and b_i are modular functions in $\mathbb{F}_p[a, b, 1/(\Delta\mathfrak{h})]$ of weight $4p^i$ and $6p^i$, respectively. The proof of that proposition also gives that F_i and H_i are modular functions in $\mathbb{F}_p[a, b, 1/(\Delta\mathfrak{h})][x_0, y_0]$ of weight $2p^i$ and $3p^i - 3$, respectively. Combining all of these facts, we (conjecturally) know exactly what form these functions will take. For example, for $p = 5$, we have $\mathfrak{h} = 2a$, and the bound from Conjecture 3.14 (and from [FL23]) for $n = 1$ is -1. So we can write

$$a_1 = \frac{\alpha_1 a^6 + \alpha_2 a^3 b^2 + \alpha_3 b^4}{\mathfrak{h}}$$
$$b_1 = \frac{\beta_1 a^7 b + \beta_2 a^4 b^3 + \beta_3 a b^5}{\mathfrak{h}}$$

for some $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathbb{F}_p$. Solving a linear system over $\mathbb{F}_p$ is (in general) much faster than solving a linear system over $\mathbb{F}_p(a, b)$. So rather than slowly solving one system over $\mathbb{F}_p(a, b)$, we can compute the canonical lifting of many different curves over $\mathbb{F}_{p^r}$, and use those results to set up a linear system in the α's and β's (and the coefficients of F_i and H_i) that gives a solution in $\mathbb{F}_p$. While this algorithm is based on conjecture, it is possible to verify that the result that we get gives the canonical lifting by checking that $\tau^*(\boldsymbol{x}/\boldsymbol{y})$ has a zero at infinity.

We implemented both the standard algorithm and the interpolation algorithm in both SageMath Version 9.8 and Magma Version 2.27-7 in order to compare. These computations were performed on a server with two ten-core 3.0 GHz Intel Xeon E5-2690 v2 CPUs and 192 GiB of RAM, running GNU/Linux with kernel 5.1.11 (64-bit). The results are contained in Table 3.2 (next page). The memory measurements for Magma are imprecise, as it appears Magma allocates memory in chunks.

In SageMath, the interpolation algorithm uses slightly more memory but appears to be orders of magnitude faster. Furthermore, the speedup factor appears to increase as n increases, so we get larger and larger returns. However, it seems that most of this speedup comes because the algorithm used by SageMath to solve linear systems over $\mathbb{F}_p(a, b)$ is *very* slow. In contrast, in Magma, in all cases that we tested, the results are the opposite: the interpolation algorithm is about an order of magnitude *slower* than the classical one, but appears to be more memory efficient. It's possible this slowness may be solved by parallelizing the code, as most of the computations can run independently. The code for both of these implementations can be found at https://github.com/nielrenned/canonical-lifting-comparison. We welcome any input on potential efficiency gains, as these results seem quite strange.

Table 3.2: Comparison of the Two Canonical Lifting Algorithms

SageMath					
Parameters		**Classical**		**Interpolation**	
p	up to n	time (sec)	memory (MiB)	time (sec)	memory (MiB)
5	2	167	23.11	3.47	29.44
7	1	0.680	11.78	0.099	20.13
7	2	> 3 days		29.6	43.33
11	1	1.16	13.27	0.258	21.76
13	1	2.08	14.32	0.358	22.46
17	1	4.6	15.90	0.704	25.76

Magma					
Parameters		**Classical**		**Interpolation**	
p	up to n	time (sec)	memory (MiB)	time (sec)	memory (MiB)
5	2	0.22	32	0.67	32
7	2	2.02	32	8.72	64
11	2	87.4	364	616	317
13	1	0.03	32	0.08	32
17	1	0.04	32	0.12	32
19	1	0.07	32	0.17	32
23	1	0.11	32	0.31	32
101	1	14.4	157	132.5	131

Chapter 4

Mixed Characteristic Witt Vectors

Our goal in this chapter is to investigate the structure of so-called "mixed characteristic" Witt vectors, that is $\boldsymbol{W}_{p,n}(R)$ with $\mathrm{char}(R) \neq p$. We'll start with some general results about the characteristic of these rings, show how $\boldsymbol{W}_{p,n}(R)$ can be seen as a direct sum, and then prove an isomorphism for $\boldsymbol{W}_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$.

4.1 The Characteristic of the Witt Ring

Since $\boldsymbol{W}_{p,n}(R)$ is a commutative ring, it makes sense to ask what its characteristic is. To do this, we investigate the form that the integers take as Witt vectors.

If $\mathrm{char}(R) = p$, then $\mathbb{F}_p \subseteq R$, and we have an algorithm for mapping the integers to $\boldsymbol{W}_{p,n}(R)$. For any $c \in \mathbb{Z}$, we write its p-adic series, i.e., $c = c_0 + c_1 p + c_2 p^2 + \cdots$. Since each $c_i \in \mathbb{F}_p$, we have $c_i^{1/p} = c_i$, and so $\boldsymbol{c} = (c_0, c_1, c_2 \ldots)$. The following proposition extends this idea to any ring. We believe this result is known, but are including a proof for completeness.

Proposition 4.1. *Given $c \in \mathbb{Z}$, the image of c in $\boldsymbol{W}_{p,\infty}(R)$ is given by $\boldsymbol{c} = (\overline{c_0}, \overline{c_1}, \overline{c_2}, \ldots)$, where $c_0, c_1, c_2, \ldots \in \mathbb{Z}$ are defined as follows:*

$$c_0 = c$$

and

$$c_n = \frac{c - c^{p^n}}{p^n} - \sum_{i=1}^{n-1} \frac{c_{n-i}^{p^i}}{p^i} = \frac{1}{p^n}\left[c - \sum_{i=0}^{n-1} p^i c_i^{p^{n-i}}\right].$$

Note. If $p \notin R^\times$, these computations *must* first be done in $\mathbb{Z}$, and then mapped into R.

Proof. We begin by proving the proposition is true for all $c \geq 0$.

First, we note that this is clear for 0. The zero of $\boldsymbol{W}_{p,\infty}(R)$ is $\mathbf{0} = (0, 0, 0, \ldots)$. Now, consider $c = 1$. The one of $\boldsymbol{W}_{p,\infty}(R)$ is $\mathbf{1} = (1, 0, 0, \ldots)$. Using the formulas above we have $c_0 = 1$, and $c_1 = (1 - 1^p)/p = 0$. Then, proceeding inductively, we get

$$c_n = \frac{1 - 1^{p^n}}{p^n} - \sum_{i=1}^{n-1} \frac{0^{p^i}}{p^i} = 0.$$

So the formulas are correct for c = 1.

Now, let $c > 1$ and suppose the formulas are correct for $c - 1$. For the sake of notation, let $d = c - 1$. Then we have $\boldsymbol{c} = \boldsymbol{d} + \mathbf{1}$. So we apply the Witt sum, i.e., we have $c_n = S_n(d_0, \ldots, d_n, 1, 0, \ldots, 0)$ for all $n \geq 0$.

First, we note that this gives $c_0 = S_0(d_0, 1) = d + 1 = c$ and

$$\begin{aligned} c_1 &= S_1(d_0, d_1, 1, 0) \\ &= d_1 + 0 + \frac{d_0^p + 1^p - c_0^p}{p} \\ &= \frac{d - d^p}{p} + \frac{d^p + 1 - c^p}{p} = \frac{c - c^p}{p}. \end{aligned}$$

Now, inductively assume that the formulas are correct for all $m < n$. Then we have

$$\begin{aligned} c_n &= S_n(d_0, \ldots, d_n, 1, 0, \ldots, 0) \\ &= d_n + 0 + \tfrac{1}{p}(d_{n-1}^p + 0^p - c_{n-1}^p) + \cdots + \tfrac{1}{p^{n-1}}(d_1^{p^{n-1}} + 0^{p^{n-1}} - c_1^{p^{n-1}}) + \tfrac{1}{p^n}(d_0^{p^n} + 1^{p^n} - c_0^{p^n}) \\ &= \left(\frac{d - d^{p^n}}{p^n} - \sum_{i=1}^{n-1} \frac{d_{n-i}^{p^i}}{p^i} \right) + \sum_{i=1}^{n-1} \frac{d_{n-i}^{p^i} - c_{n-i}^{p^i}}{p^i} + \frac{d^{p^n} + 1 - c^{p^n}}{p^n} \\ &= \frac{c - c^{p^n}}{p^n} - \sum_{i=1}^{n-1} \frac{c_{n-i}^{p^i}}{p^i}. \end{aligned}$$

Each S_n is a polynomial over $\mathbb{Z}$, so by the first line, despite the denominators, we get that c_n is in $\mathbb{Z}$. So the proposition is true for all $c \geq 0$.

Now, suppose $c < 0$ and let $b = -c$. Define the c_n as above. We know the formulas work for $\boldsymbol{b}$. For $p \neq 2$, we have $\boldsymbol{c} = (-b_0, -b_1, -b_2, \ldots)$. We need to show that $c_n = -b_n$ for all n. This is clearly true for c_0 and we have

$$c_1 = \frac{c - c^p}{p} = \frac{(-b) - (-b)^p}{p} = -\frac{b - b^p}{p} = -b_1.$$

Then, inductively, we have

$$\begin{aligned} c_n &= \frac{1}{p^n}\left[c - \sum_{i=0}^{n-1} p^i c_i^{p^{n-i}}\right] \\ &= \frac{1}{p^n}\left[(-b) - \sum_{i=0}^{n-1} p^i (-b_i)^{p^{n-i}}\right] \\ &= -\frac{1}{p^n}\left[b - \sum_{i=0}^{n-1} p^i b_i^{p^{n-i}}\right] = -b_n \end{aligned}$$

so we indeed have that $\boldsymbol{c} = (\overline{c_0}, \overline{c_1}, \ldots)$. Now, if $p = 2$, we have

$$\boldsymbol{c} = (-1, -1, -1, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (P_0(\boldsymbol{-1}, \boldsymbol{b}), P_1(\boldsymbol{-1}, \boldsymbol{b}), P_2(\boldsymbol{-1}, \boldsymbol{b}), \ldots).$$

Again, right away we get that $c_0 = -b_0$. Now inductively suppose $c_k = P_k(\boldsymbol{-1}, \boldsymbol{b})$ for $k < n$. Then we have

$$\begin{aligned} &P_n(\boldsymbol{-1}, \boldsymbol{b}) \\ &= \frac{1}{2^n}\left[\left((-1)^{2^n} + 2(-1)^{2^{n-1}} + \cdots + 2^n(-1)\right)\left(b_0^{2^n} + 2b_1^{2^{n-1}} + \cdots + 2^n b_n\right) - \sum_{i=0}^{n-1} 2^i P_i^{2^{n-i}}\right] \\ &= \frac{1}{2^n}\left[\left(1 + 2 + \cdots + 2^{n-1} - 2^n\right)\left(b_0^{2^n} + 2b_1^{2^{n-1}} + \cdots + 2^n b_n\right) - \sum_{i=0}^{n-1} 2^i c_i^{2^{n-i}}\right] \\ &= \frac{1}{2^n}\left[-\left(b_0^{2^n} + 2b_1^{2^{n-1}} + \cdots + 2^n b_n\right) - \sum_{i=0}^{n-1} 2^i c_i^{2^{n-i}}\right] \end{aligned}$$

By construction of the b_n, for any n (and any p), we have

$$b = \sum_{i=0}^{n} p^i b_i^{p^{n-i}} \tag{4.1}$$

so the expression above simplifies to

$$P_n(\mathbf{-1}, \boldsymbol{b}) = \frac{1}{2^n}\left[-b - \sum_{i=0}^{n-1} 2^i c_i^{2^{n-i}}\right] = \frac{1}{2^n}\left[c - \sum_{i=0}^{n-1} 2^i c_i^{2^{n-i}}\right] = c_n.$$

finishing the proof. □

Our goal now is to determine the characteristic of $\boldsymbol{W}_{p,n}(R)$ for any R, which will give us our first insight into its structure. We start by investigating the Witt vector representation of $\mathrm{char}(R)$.

Proposition 4.2. *Let $N = char(R)$ and suppose $p \mid N$. Let $v = v_p(N)$. Let $\boldsymbol{N}$ be the image of N in $\boldsymbol{W}_{p,\infty}(R)$. Then for all $j \geq 0$ we have*

$$p^j \boldsymbol{N} = \left(0, \dots, 0, \frac{N}{p} N_{1,j}, \frac{N}{p^2} N_{2,j}, \dots, \frac{N}{p^v} N_{v,j}, \frac{N}{p^v} N_{v+1,j}, \frac{N}{p^v} N_{v+2,j}, \dots\right)$$

where the first $j+1$ entries are zero and $N_{i,j} \in \mathbb{Z}$ for all i.

Proof. First, note that this is clearly true for $N = 0$. So assume $N > 0$. We start with $j = 0$ and apply the Proposition 4.1. Firstly, we have $N_0 = N \equiv 0 \pmod{N}$ and

$$N_1 = \frac{N - N^p}{p} = \frac{N}{p}(1 - N^{p-1}) =: \frac{N}{p} N_{1,0}.$$

Suppose $n \leq v$. Then inductively, we have

$$\begin{aligned}
N_n &= \frac{N - N^{p^n}}{p^n} - \sum_{i=1}^{n-1} \frac{N_{n-i}^{p^i}}{p^i} \\
&= \frac{N}{p^n}(1 - N^{p^n-1}) - \sum_{i=1}^{n-1} \frac{1}{p^i}\left(\frac{N}{p^{n-i}} N_{n-i,0}\right)^{p^i} \\
&= \frac{N}{p^n}\left[1 - N^{p^n-1} - \sum_{i=1}^{n-1}\left(\frac{N}{p^{n-i}}\right)^{p^i-1} N_{n-i,0}^{p^i}\right] =: \frac{N}{p^n} N_{n,0}
\end{aligned}$$

Since $n - i \leq v$, we have that $\frac{N}{p^{n-i}}$ is an integer and so $N_{n,0}$ is an integer. Now suppose $n > v$ and continue with the induction. In this case, we get

$$
\begin{aligned}
N_n &= \frac{N - N^{p^n}}{p^n} - \sum_{i=1}^{n-1} \frac{N_{n-i}^{p^i}}{p^i} \\
&= \frac{1}{p^n}\left[N - N^{p^n} - \sum_{i=1}^{n-1} p^i N_i^{p^{n-i}}\right] \\
&= \frac{1}{p^n}\left[N - N^{p^n} - \sum_{i=1}^{v} p^i \left(\frac{N}{p^i} N_{i,0}\right)^{p^{n-i}} - \sum_{i=v+1}^{n-1} p^i \left(\frac{N}{p^v} N_{i,0}\right)^{p^{n-i}}\right]
\end{aligned}
$$

Note that the expression in square brackets is an integer, since $\frac{N}{p^i} \in \mathbb{Z}$ for all $i \leq v$. Since N_n is also an integer, we must have that that expression is divisible by p^n. So if we factor out an N from the square brackets, that expression must still be divisible by p^{n-v}. So we can write

$$
\begin{aligned}
&= \frac{N}{p^v}\frac{1}{p^{n-v}}\left[1 - N^{p^n-1} - \sum_{i=1}^{v} p^i \left(\frac{N}{p^i}\right)^{p^{n-i}-1} N_{i,0}^{p^{n-i}} - \sum_{i=v+1}^{n-1} p^{i-v} \left(\frac{N}{p^v}\right)^{p^{n-i}-1} N_{i,0}^{p^{n-i}}\right] \\
&=: \frac{N}{p^v} N_{n,0},
\end{aligned}
$$

and rest assured that $N_{n,0}$ is indeed an integer. So the proposition holds for $j = 0$.

Now, inductively assume the proposition holds for all $k < j$. By Proposition 5.10 of [Rab14], we have that multiplication by p is equivalent to applying $F \circ V$, where F and V are the Frobenius and Verschiebung maps, respectively. So, $p^j \cdot \boldsymbol{N} = F(V(p^{j-1} \cdot \boldsymbol{N}))$. Lemma 4.1 of [DK14] gives us a formulation for F, namely, $F(x_0, x_1, \ldots)$ is given by $(y_0, y_1, \ldots)$ with

$$
y_n = x_n^p + p x_{n+1} + p f_n(x_0, \ldots x_n)
$$

where f_n is a polynomial with integer coefficients that is homogeneous of weight p^{n+1} under the weighting $\mathrm{wgt}(x_i) = p^i$. Using this notation, we let $(x_0, x_1, \ldots) = V(p^{j-1} \cdot \boldsymbol{N})$. Then $x_0 = \ldots = x_j = 0$ and

$$
(x_{j+1}, x_{j+2}, \ldots) = \left(\frac{N}{p} N_{1,j-1}, \frac{N}{p^2} N_{2,j-1}, \ldots, \frac{N}{p^v} N_{v,j-1}, \frac{N}{p^v} N_{v+1,j-1}, \frac{N}{p^v} N_{v+2,j-1}, \ldots\right).
$$

Since each f_n is homogeneous of positive weight, $f_n(0, \dots, 0) = 0$. So it is immediately clear that $y_n = 0$ for all $n < j$. Furthermore,

$$\begin{aligned} y_j &= x_j^p + px_{j+1} + pf_j(x_0, \dots, x_j) \\ &= 0^p + p\frac{N}{p}N_{1,j-1} + pf_j(0, \dots, 0) \\ &= NN_{1,j-1} \equiv 0 \pmod{N} \end{aligned}$$

This proves the first part: $p^j \cdot \boldsymbol{N}$ has zero in its first $j + 1$ entries. Now, for $1 \leq n < v$, we consider

$$\begin{aligned} y_{j+n} &= x_{j+n}^p + px_{j+n+1} + pf_{j+n}(x_0, \dots, x_{j+n}) \\ &= \left(\frac{N}{p^n}N_{n,j-1}\right)^p + p\left(\frac{N}{p^{n+1}}N_{n+1,j-1}\right) + pf_{j+n}\left(0, \dots, 0, \frac{N}{p}N_{1,j-1}, \dots, \frac{N}{p^n}N_{n,j-1}\right) \\ &= \frac{N}{p^n}\left(\left(\frac{N}{p^n}\right)^{p-1} N_{n,j-1}^p + N_{n+1,j-1}\right) + pf_{j+n}\left(0, \dots, 0, \frac{N}{p}N_{1,j-1}, \dots, \frac{N}{p^n}N_{n,j-1}\right) \end{aligned}$$

Since f_{j+n} is homogeneous, it has no constant term. Also, f_{j+n} has integer coefficients. Therefore, since $\frac{N}{p^n}$ divides $\frac{N}{p^m}$ for $m \leq n$, every term of f_{j+n} is an integer and has a factor of $\frac{N}{p^n}$ in it. So we can write $y_{j+n} =: \frac{N}{p^n}N_{n,j}$.

Finally, for $n \geq v$, we have

$$\begin{aligned} y_{j+n} &= x_{j+n}^p + px_{j+n+1} + pf_{j+n}(x_0, \dots, x_{j+n}) \\ &= \left(\frac{N}{p^v}N_{n,j-1}\right)^p + p\left(\frac{N}{p^v}N_{n+1,j-1}\right) + pf_{j+n}\left(0, \dots, 0, \frac{N}{p}N_{1,j-1}, \dots, \frac{N}{p^v}N_{n,j-1}\right) \\ &= \frac{N}{p^v}\left(\left(\frac{N}{p^v}\right)^{p-1} N_{n,j-1}^p + pN_{n+1,j-1}\right) + pf_{j+n}\left(0, \dots, 0, \frac{N}{p}N_{1,j-1}, \dots, \frac{N}{p^v}N_{n,j-1}\right) \end{aligned}$$

By the same logic as before, we can factor out $\frac{N}{p^v}$ from f_{j+n}, so we can write $y_{j+n} =: \frac{N}{p^v}N_{n,j}$. Putting this all together, we have

$$p^j \cdot \boldsymbol{N} = (y_0, y_1, \dots) = \left(0, \dots, 0, \frac{N}{p}N_{1,j}, \frac{N}{p^2}N_{2,j}, \dots, \frac{N}{p^v}N_{v,j}, \frac{N}{p^v}N_{v+1,j}, \frac{N}{p^v}N_{v+2,j}, \dots\right),$$

with the first $j+1$ entries 0, which is what we set out to prove. $\square$

Corollary 4.3. *Let $N = char(R)$ and suppose $p \mid N$. Then $char(\boldsymbol{W}_{p,n}(R)) = p^{n-1}N$ and $char(\boldsymbol{W}_{p,\infty}(R)) = 0$.*

Proof. If $N = 0$, then $\mathbb{Z} \hookrightarrow R$. So for any $c \in \mathbb{Z}$, taking $\boldsymbol{c} = (\overline{c_0}, \overline{c_1}, \ldots)$ as in Proposition 4.1, we have $\overline{c_0} \neq 0$. Thus $\operatorname{char}(\boldsymbol{W}_{p,n}(R)) = 0$ for all $n \in \mathbb{N} \cup \{\infty\}$, which shows the corollary is true for $N = 0$. So let $N > 0$ and let $N_{i,j}$ be as in Proposition 4.2.

We first show that $\dfrac{N}{p} N_{1,j} \not\equiv 0 \pmod{N}$ for all j. Let $M = p^j N$. Let $\boldsymbol{M} = (M_0, M_1, \ldots)$ as in Proposition 4.1. Then we have

$$\frac{N}{p} N_{1,j} = M_{j+1} = \frac{1}{p^{j+1}} \left[M - \sum_{i=0}^{j} p^i M_i^{p^{j+1-i}} \right] = \frac{N}{p} - \sum_{i=0}^{j} \frac{M_i^{p^{j+1-i}}}{p^{j+1-i}}. \tag{4.2}$$

Since $\boldsymbol{M} = p^j \boldsymbol{N}$, by Proposition 4.2, we have that $M_i \equiv 0 \pmod{N}$ for all $0 \leq i \leq j$, so we can write $M_i = c_i N$ for some $c_i \in \mathbb{Z}$. Letting $N' = N/p$, we have $M_i = c_i p N'$. Then for $k \geq 0$,

$$\frac{M_i^{p^k}}{p^k} = p^{p^k - k}(c_i N')^{p^k} = p^{p^k - k} N'(\cdots).$$

Since $p^k - k \geq 1$ for all $k \geq 0$, we have $M_i^{p^k}/p^k \equiv 0 \pmod{N}$. So Equation (4.2) simplifies to

$$\frac{N}{p} N_{1,j} \equiv \frac{N}{p} \pmod{N}.$$

Since $\operatorname{char}(R) = N$, $\frac{N}{p} \not\equiv 0 \pmod{N}$. So, we've shown that the first non-zero entry of $p^j \cdot \boldsymbol{N}$ is $\dfrac{N}{p}$ and occurs at index $j+1$. Now, we note that $\operatorname{char}(\boldsymbol{W}_{p,n}(R))$ must be a multiple of N, otherwise the first component would be non-zero.

Let $n \in \mathbb{N}$. We can write $n = cp^j$ for some j with $p \nmid c$. Then we have

$$\boldsymbol{n}\boldsymbol{N} = \boldsymbol{c}\boldsymbol{p}^{\boldsymbol{j}}\boldsymbol{N} = \boldsymbol{c} \cdot \left(0, \ldots, 0, \frac{N}{p}, \ldots\right) = \left(0, \ldots, 0, c\frac{N}{p}, \ldots\right)$$

Since $p \nmid c$, we can never have $\dfrac{cN}{p} \equiv 0 \pmod{N}$, since we'll always be missing a factor of p. This shows two things. Firstly, every multiple of $\boldsymbol{N}$ has a non-zero component, which proves

$\mathrm{char}(\boldsymbol{W}_{p,\infty}(R)) = 0$. Secondly, the number of zeroes at the beginning of $\boldsymbol{nN}$ is exactly $v_p(n) + 1$. So the smallest integer that maps to 0 in $\boldsymbol{W}_{p,n}(R)$ must be $p^{n-1}N$. $\square$

This proposition, along with Remark 2.5 of [Rab14] gives a complete characterization of the characteristic of Witt Rings. We have

$$\mathrm{char}(\boldsymbol{W}_{p,\infty}(R)) = \begin{cases} 0 & \text{if } p \mid \mathrm{char}(R) \\ \mathrm{char}(R) & \text{otherwise} \end{cases}$$

and

$$\mathrm{char}(\boldsymbol{W}_{p,n}(R)) = \begin{cases} p^{n-1}\mathrm{char}(R) & \text{if } p \mid \mathrm{char}(R) \\ \mathrm{char}(R) & \text{otherwise} \end{cases}$$

4.2 The General Structure of $W_{p,n}(R)$

Our goal in this section is to investigate the structure of $\boldsymbol{W}_{p,n}(R)$ a little bit more. We start by showing the ideals of R lift to ideals of $\boldsymbol{W}_{p,n}(R)$ in a natural way.

Proposition 4.4. *Let I be an ideal of R. Thenfor all $n \in \mathbb{N} \cup \{\infty\}$,*

$$\boldsymbol{W}_{p,n}(I) := \{(a_0, a_1, \cdots) \in \boldsymbol{W}_{p,n}(R) : a_i \in I \textit{ for all } i\}$$

is an ideal of $\boldsymbol{W}_{p,n}(R)$ and

$$\boldsymbol{W}_{p,n}(R)/\boldsymbol{W}_{p,n}(I) \cong \boldsymbol{W}_{p,n}(R/I).$$

Proof. Let $\boldsymbol{r} \in \boldsymbol{W}_{p,n}(R)$ and $\boldsymbol{a} \in \boldsymbol{W}_{p,n}(I)$. The product polynomials P_i have integer coefficients and every monomial is of the form $c \prod X_j^{s_j} \prod Y_k^{t_k}$, where $c \in \mathbb{Z}$ and $s_j, t_k > 0$ for all j, k. So the monomials in $P_i(\boldsymbol{r}, \boldsymbol{a})$ will be an integer times an element of R times an element of I, which, since I is an ideal, is in I. Then we add up all these elements, so $P_i(\boldsymbol{r}, \boldsymbol{a}) \in I$ and therefore $\boldsymbol{ra} \in \boldsymbol{W}_{p,n}(I)$.

Now, let $\boldsymbol{b} \in \boldsymbol{W}_{p,n}(I)$. By the above, $-\boldsymbol{b}$ is also in $\boldsymbol{W}_{p,n}(I)$. Then since the sum polynomials S_i all have integer coefficients, $S_i(\boldsymbol{a}, -\boldsymbol{b}) \in I$ for all i. So $(\boldsymbol{a} - \boldsymbol{b}) \in \boldsymbol{W}_{p,n}(I)$. Thus $\boldsymbol{W}_{p,n}(I)$ is an ideal of $\boldsymbol{W}_{p,n}(R)$.

For the second part, define $\boldsymbol{\varphi} : \boldsymbol{W}_{p,n}(R) \to \boldsymbol{W}_{p,n}(R/I)$ by $\boldsymbol{\varphi}(\boldsymbol{v}) = (v_0 + I, v_1 + I, \ldots)$. Then Theorem 2.6 of [Rab14] gives that $\boldsymbol{\varphi}$ is a ring homomorphism. Also, clearly $\ker(\boldsymbol{\varphi}) = \boldsymbol{W}_{p,n}(I)$, so the First Isomorphism Theorem finishes the proof. $\square$

We can take advantage of this lifting of ideals to gain insight into the structure of $\boldsymbol{W}_{p,n}(R)$. First we need a small computational lemma.

Lemma 4.5. *Let $p, \alpha, M \in \mathbb{Z}_{>0}$ with p prime and $p \nmid M$. Let $a, b \in \mathbb{Z}$ such that $ap^\alpha + bM = 1$. Then for all $i \geq 0$,*

$$(ap^\alpha)^{p^i} + (bM)^{p^i} \equiv 1 \pmod{p^{\alpha+i}M}.$$

Proof. We have

$$\begin{aligned} 1 = 1^{p^i} &= (ap^\alpha + bM)^{p^i} \\ &= (ap^\alpha)^{p^i} + (bM)^{p^i} + \sum_{n=1}^{p^i-1} \binom{p^i}{n} (ap^\alpha)^n (bM)^{p^i-n} \end{aligned}$$

Clearly, every term in the sum is divisible by M. From [Fin14] Lemma 8.1, we have that $\nu_p(\binom{p^i}{n}) = i - \nu_p(n)$. So each term in the sum is also divisible by $p^{\alpha n + i - \nu_p(n)}$. Since $n < p^n$, we have $\nu_p(n) < n$. This gives

$$\alpha n + i - \nu_p(n) > n(\alpha - 1) + i \geq \alpha + i - 1.$$

Therefore, $\alpha n + i - \nu_p(n) \geq \alpha + i$ and so $p^{\alpha+i}$ divides every term in the sum. So, mod $p^{\alpha+i}M$, the summation is congruent to 0, finishing the proof. $\square$

Theorem 4.6. *Let R be a commutative ring of characteristic $N > 0$. Write $N = p^\alpha M$ with $p \nmid M$. Then, for all $n \in \mathbb{N} \cup \{\infty\}$,*

$$\boldsymbol{W}_{p,n}(R) \cong \boldsymbol{W}_{p,n}(R/p^\alpha R) \oplus \boldsymbol{W}_{p,n}(R/MR).$$

Proof. Let $I = p^\alpha R$ and $J = MR$. Since $p \nmid M$, 1 is a linear combination of p^α and M, so I and J are coprime. Thus by the Chinese Remainder Theorem, $I \cap J = IJ = (p^\alpha M) = (0)$ and $R \cong (R/I) \oplus (R/J)$.

Now we apply a similar argument to $\boldsymbol{W}_{p,n}(R)$. Since $I \cap J = (0)$, we get by construction that $\boldsymbol{W}_{p,n}(I) \cap \boldsymbol{W}_{p,n}(J) = (0)$. If we show that $\boldsymbol{W}_{p,n}(I)$ and $\boldsymbol{W}_{p,n}(J)$ are coprime, we'll have, by the Chinese Remainder Theorem and Proposition 4.4,

$$\boldsymbol{W}_{p,n}(R) \cong \boldsymbol{W}_{p,n}(R)/\boldsymbol{W}_{p,n}(I) \oplus \boldsymbol{W}_{p,n}(R)/\boldsymbol{W}_{p,n}(J) \cong \boldsymbol{W}_{p,n}(R/I) \oplus \boldsymbol{W}_{p,n}(R/J)$$

Let $a, b \in \mathbb{Z}$ such that $ap^\alpha + bM = 1$. By construction of the ideals, we have $(ap^\alpha, 0, 0, \ldots) \in \boldsymbol{W}_{p,n}(I)$ and $(bM, 0, 0, \ldots) \in \boldsymbol{W}_{p,n}(J)$. We claim that $(ap^\alpha, 0, 0, \ldots) + (bM, 0, 0, \ldots) = (1, 0, 0, \ldots)$, which will show that $\boldsymbol{W}_{p,n}(I)$ and $\boldsymbol{W}_{p,n}(J)$ are coprime.

The first component being 1 is clear, so we need to show that the rest of the components are 0. We start with

$$S_1((ap^\alpha, 0, \ldots), (bM, 0, \ldots)) = \frac{1}{p}[(ap^\alpha)^p + (bM)^p - 1].$$

By Lemma 4.5, $(ap^\alpha)^p + (bM)^p \equiv 1 \pmod{p^{\alpha+1}M}$, which gives $S_1 \equiv 0 \pmod{p^\alpha M}$. Now inductively assume $S_j \equiv 0 \pmod{p^\alpha M}$ for all $j < i$. We have

$$S_i((ap^\alpha, 0, \ldots), (bM, 0, \ldots)) = -\sum_{j=1}^{i-2} \frac{S_{i-j}^{p^j}}{p^j} - \frac{1}{p^i}[(ap^\alpha)^{p^i} + (bM)^{p^i} - 1].$$

Again by Lemma 4.5, we have that $p^{-i}[(ap^\alpha)^{p^i} + (bM)^{p^i} - 1] \equiv 0 \pmod{p^\alpha M}$. Also, since $S_{i-j} \equiv 0 \pmod{p^\alpha M}$ and $j < p^j$, we have that $p^{-j}S_{i-j}^{p^j} \equiv 0 \pmod{p^\alpha M}$. So $S_i \equiv 0 \pmod{p^\alpha M}$ as well, proving the claim and finishing the proof of the theorem. □

The isomorphism here is hiding in the details of the proof. Combining the isomorphisms from the Chinese Remainder Theorem and Proposition 4.4, we get the explicit form

$$\begin{aligned}
&\phi : \boldsymbol{W}_{p,n}(R) \to \boldsymbol{W}_{p,n}(R/MR) \oplus \boldsymbol{W}_{p,n}(R/p^\alpha R) \\
&\quad (v_0, v_1, \ldots) \mapsto (v_0 + (p^\alpha), v_1 + (p^\alpha), \ldots) \oplus (v_0 + (MR), v_1 + (MR), \ldots).
\end{aligned}$$

For computational purposes, we would also like to know how to invert this, which leads us to the next theorem.

Theorem 4.7. *Take R as in Theorem 4.6 and let $a, b \in \mathbb{Z}$ such that $ap^\alpha + bM = 1$. Take ϕ as above and define*

$$\begin{aligned}\psi : \boldsymbol{W}_{p,n}(R/MR) \oplus \boldsymbol{W}_{p,n}(R/p^\alpha R) &\to \boldsymbol{W}_{p,n}(R)\\ (\overline{a_0}, \overline{a_1}, \ldots) \oplus (\overline{b_0}, \overline{b_1}, \ldots) &\mapsto ((ap^\alpha)a_0 + (bM)b_0, (ap^\alpha)a_1 + (bM)b_1, \ldots).\end{aligned}$$

Then ϕ and ψ are inverses.

Proof. First we show that ψ is well-defined. Let

$$(a_0, a_1, \ldots) \oplus (b_0, b_1, \ldots) = (a_0', a_1', \ldots) \oplus (b_0', b_1', \ldots).$$

Then we have that $a_i = a_i' + k_i M$ and $b_i = b_i' + \ell_i p^\alpha$ for all i. We compute

$$\begin{aligned}&\psi((a_0, a_1, \ldots) \oplus (b_0, b_1, \ldots))\\ &= ((ap^\alpha)a_0 + (bM)b_0, (ap^\alpha)a_1 + (bM)b_1, \ldots)\\ &= ((ap^\alpha)(a_0' + k_0 M) + (bM)(b_0' + \ell_0 p^\alpha), (ap^\alpha)(a_1' + k_1 M) + (bM)(b_1' + \ell_1 p^\alpha), \ldots)\\ &= ((ap^\alpha)a_0' + (bM)b_0' + (ak_0 + b\ell_0)p^\alpha M, (ap^\alpha)a_1' + (bM)b_1' + (ak_1 + b\ell_1)p^\alpha M, \ldots)\\ &= ((ap^\alpha)a_0' + (bM)b_0', (ap^\alpha)a_1' + (bM)b_1', \ldots) \text{ since } \operatorname{char}(R) = p^\alpha M\\ &= \psi((a_0', a_1', \ldots) \oplus (b_0', b_1', \ldots)).\end{aligned}$$

Therefore ψ is well-defined. Now we compute

$$\begin{aligned}\psi(\phi(\boldsymbol{v})) &= \psi((\overline{v_0}, \overline{v_1}, \ldots) \oplus (\overline{v_0}, \overline{v_1}, \ldots))\\ &= ((ap^\alpha + bM)v_0, (ap^\alpha + bM)v_1, \ldots) = \boldsymbol{v}\end{aligned}$$

and

$$
\begin{aligned}
&\phi(\psi(\boldsymbol{a} \oplus \boldsymbol{b})) \\
&= \phi(((ap^\alpha)a_0 + (bM)b_0, (ap^\alpha)a_1 + (bM)b_1, \ldots)) \\
&= ((\overline{(ap^\alpha)a_0 + (bM)b_0}, \overline{(ap^\alpha)a_1 + (bM)b_1}, \ldots) \oplus ((\overline{(ap^\alpha)a_0 + (bM)b_0}, \overline{(ap^\alpha)a_1 + (bM)b_1}, \ldots) \\
&= (\overline{a_0}, \overline{a_1}, \ldots) \oplus (\overline{b_0}, \overline{b_1}, \ldots) = \boldsymbol{a} \oplus \boldsymbol{b}.
\end{aligned}
$$

So indeed, $\psi = \phi^{-1}$ (and therefore is an isomorphism as well) finishing the proof. □

And finally, we can remove the Witt vector aspect entirely in one component, which is computationally useful.

Corollary 4.8. *Take R as in Theorem 4.6. Then*

$$\boldsymbol{W}_{p,n}(R) \cong (R/MR)^n \oplus \boldsymbol{W}_{p,n}(R/p^\alpha R).$$

Proof. Since $\mathrm{char}(R/MR) = M$, and $p \nmid M$, $p \in (R/MR)^\times$. So by [Rab14] Remark 2.5, which is restated in Proposition 1.10, $\boldsymbol{W}_{p,n}(R/MR) \cong (R/MR)^n$ via $(w_0, w_1, \ldots)$. □

4.3 The Additive Structure of $W_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$

So now we'd like to know the structure of $\boldsymbol{W}_{p,n}(R/p^\alpha R)$. For general R, it seems intractable, so we'll shift our focus to $R = \mathbb{Z}$. In Proposition 1.6 of [Hes15], the structure of $\boldsymbol{W}_{p,n}(\mathbb{Z})$ is given by

$$\boldsymbol{W}_{p,n}(\mathbb{Z})^+ = \prod_{i=0}^{n} \mathbb{Z} \cdot V^i(\mathbf{1}) \cong \mathbb{Z}^n$$

with multiplication given by

$$V^i(\mathbf{1}) \cdot V^j(\mathbf{1}) = p^i \cdot V^j(\mathbf{1})$$

for $i \leq j$. Despite the strange multiplication listed above, we actually get an isomorphism of *rings* given by the ghost map, $w_* : \boldsymbol{W}_{p,n}(\mathbb{Z}) \to \mathbb{Z}^n$ defined by $\boldsymbol{a} \mapsto (w_0(\boldsymbol{a}), w_1(\boldsymbol{a}), \ldots)$.

The results below build on this idea to extend the result that $\boldsymbol{W}_{p,n}(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$ to a slightly larger class of rings. Our goal in this section is to prove the following theorem.

Theorem 4.9. *For all $n \in \mathbb{N}$, the additive group of $\boldsymbol{W}_{p,n}(\mathbb{Z}/p^{\alpha}\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/p^{n+\alpha-1}\mathbb{Z}) \oplus (\mathbb{Z}/p^{\alpha-1}\mathbb{Z})^{n-1}$.*

By Corollary 4.3, we know the first piece is the image of $\mathbb{Z}$, and so is generated by one. So we will start by constructing elements of order $\alpha-1$, then prove that these elements do in fact generate subgroups with trivial intersection. After that, we will show that these elements have "nice" multiplicative properties and use these properties to construct an isomorphism that is computationally useful.

We start by defining the following values. Let $g_0 = p$ and then for $i \in \{1, \dots, n-1\}$, let g_i be defined recursively by

$$g_i = -\frac{1}{p^i}\sum_{j=0}^{i-1} p^j g_j^{p^{i-j}}.$$

This definition gives the following useful property for $i \geq 1$:

$$\sum_{j=0}^{i} p^j g_j^{p^{i-j}} = 0. \tag{4.3}$$

From the construction, these g_i are rational numbers, but we would like to use them as components of the Witt vectors, so we need the following lemma.

Lemma 4.10. *The g_i defined above are integers and $\nu_p(g_i) = p^i - p^{i-1} - \cdots - p - 1$.*

Proof. By definition, g_0 is an integer and $\nu_p(g_0) = 1$.

Now, inductively assume the statement is true for $j < i$. Then we have

$$\begin{aligned}
\nu_p\left(\sum_{j=0}^{i-1} p^j g_j^{p^{i-j}}\right) &\geq \min_{1\leq j\leq i-1}\{j + p^{i-j}\nu_p(g_j)\} \\
&= \min_{1\leq j\leq i-1}\{j + p^{i-j}(p^j - p^{j-1} - \cdots - p - 1)\} \\
&= \min_{1\leq j\leq i-1}\{j + p^i - p^{i-1} - \cdots - p^{i-j}\}
\end{aligned}$$

Now, for $1 \leq k < j \leq i-1$, we have

$$j + p^i - p^{i-1} - \cdots - p^{i-j} = j + p^i - \cdots - p^{i-k} - (p^{i-k-1} + \cdots + p^{i-j})$$

$$< j + p^i - \cdots - p^{i-k} - (\underbrace{1 + \cdots + 1}_{\text{j-k ones}})$$
$$= k + p^i - \cdots - p^{i-k}.$$

Therefore the minimum above is achieved by $j = i - 1$ *and* we are taking a minimum over distinct numbers, so the the inequality becomes an equality. This gives

$$\nu_p\left(\sum_{j=0}^{i-1} p^j g_j^{p^{i-j}}\right) = i + p^i - p^{i-1} - \cdots - p - 1$$

and so

$$\nu_p(g_i) = p^i - p^{i-1} - \cdots - p - 1$$

which is positive, proving both statements in the lemma. $\square$

Now, we can use these g's to define the generators. For all $i \in \{1, \ldots, n-1\}$ define

$$\gamma_i := (\underbrace{0, \ldots, 0}_{i-1 \text{ zeroes}}, g_0, g_1, \ldots, g_{n-i}).$$

Note that g_0 occurs at index $i - 1$ (since Witt vectors are 0-indexed). Our goal now is to prove that these γ's are the correct generators.

Lemma 4.11. *For any $c \in \mathbb{Z}$, $\boldsymbol{c}\gamma_i = (\underbrace{0, \ldots, 0}_{i-1 \text{ zeroes}}, cg_0, c^p g_1, c^{p^2} g_2, \ldots)$.*

Proof. First note that this is clearly true for $c = 0, 1$. Since the first $i - 1$ components of γ_i are 0, we have

$$\boldsymbol{c}\gamma_i = (\underbrace{0, \ldots, 0}_{i-1 \text{ zeroes}}, P_{i-1}(\boldsymbol{c}, \gamma_i), P_i(\boldsymbol{c}, \gamma_i), \ldots).$$

So we consider

$$P_{i-1}(\boldsymbol{c}, \gamma_i) = \frac{1}{p^{i-1}}\left[(c_0^{p^{i-1}} + \cdots + p^{i-1}c_{i-1})(p^{i-1}g_0)\right]$$
$$= g_0(c_0^{p^{i-1}} + \cdots + p^{i-1}c_{i-1})$$
$$= g_0 \sum_{j=0}^{i-1} p^j c_j^{p^{(i-1)-j}} = cg_0.$$

This last equality comes from Equation (4.1). Now, for $j \geq i$, we have

$$\begin{aligned} P_j(\boldsymbol{c}, \gamma_i) &= \frac{1}{p^j}\left[(c_0^{p^j} + \cdots + p^j c_j)\underbrace{(p^{i-1}g_0^{j-(i-1)} + \cdots + p^j g_{j-(i-1)})}_{=0 \text{ by Equation (4.3)}} - \sum_{k=i-1}^{j-1} p^k P_k^{p^{j-k}}\right] \\ &= -\frac{1}{p^j}\sum_{k=i-1}^{j-1} p^k P_k^{p^{j-k}} \end{aligned}$$

Then inductively we have

$$\begin{aligned} P_j(\boldsymbol{c}, \gamma_i) &= -\frac{1}{p^j}\sum_{k=i-1}^{j-1} p^k \left(c^{p^{k-(i-1)}} g_{k-(i-1)}\right)^{p^{j-k}} \\ &= c^{p^{j-(i-1)}}\left(-\frac{1}{p^j}\sum_{k=i-1}^{j-1} p^k g_{k-(i-1)}^{p^{j-k}}\right) \\ &= c^{p^{j-(i-1)}}\left(-\frac{1}{p^j}\sum_{k=0}^{j-i} p^{k+(i-1)} g_k^{p^{(j-i)-(k-1)}}\right) \\ &= c^{p^{j-(i-1)}}\left(-\frac{1}{p^{j-(i-1)}}\sum_{k=0}^{j-i} p^k g_k^{p^{j-(i-1)-k}}\right) = c^{p^{j-(i-1)}} g_{j-(i-1)}. \end{aligned}$$

Since the first $i-1$ components are zero, these indices are correct, proving the statement. □

Proposition 4.12. *For each i, the additive order of γ_i is $p^{\alpha-1}$.*

Proof. By the above Lemma 4.11, for any $c \in \mathbb{Z}$, the component at index $i-1$ is $cg_0 = cp$. For any $c < p^{\alpha-1}$, $cp \not\equiv 0 \pmod{p^\alpha}$. So $|\gamma_i| \geq p^{\alpha-1}$. Now, letting $c = p^{\alpha-1}$, we have $cp \equiv 0 \pmod{p^\alpha}$. Also, since $p^i(\alpha-1) \geq \alpha$ for all $i \geq 1$, we have that $c^{p^i} \equiv 0 \pmod{p^\alpha}$. So each component of $\boldsymbol{c}\gamma_i$ is 0, and thus $|\gamma_i| = p^{\alpha-1}$. □

We've shown that the γ's have the correct order, so now we need to show that $\langle\gamma_i\rangle$ has trivial intersection with the integers and the groups generated by the other γ_j. We can see right away that for $i \neq j$, $\langle\gamma_i\rangle \cap \langle\gamma_j\rangle = \{0\}$: Lemma 4.11 shows that the first non-zero component of respective elements occur at different indices. So we only need to show that the intersection with the integers is trivial. For this, we again need another lemma.

Lemma 4.13. *Let $c \in \mathbb{Z}$ with $c \neq 0$. Let $\beta = \nu_p(c)$ and define the c_i as in Proposition 4.1. Then for $i \in \{0, \ldots, \beta\}$, $\nu_p(c_i) = \beta - i$.*

Proof. Since $c_0 = c$, we have that $\nu_p(c_0) = \beta$. So we proceed by induction.

$$\begin{aligned}\nu_p(c_i) &= -i + \nu_p\left(c - c^{p^i} - \sum_{j=1}^{i-1} p^j c_j^{p^{i-j}}\right) \\ &\geq -i + \min\left\{\beta, p^i\beta, \min_{1\leq j\leq i-1}\left\{j + p^{i-j}(\beta - j)\right\}\right\}\end{aligned}$$

Since $\beta \geq i > j$, we have

$$\begin{aligned}&(p^{i-j} - 1)(\beta - j) > 0 \\ \Rightarrow\ & p^{i-j}\beta - \beta - p^{i-j}j + j > 0 \\ \Rightarrow\ & j + p^{i-j}(\beta - j) > \beta.\end{aligned}$$

Clearly $p^i\beta > \beta$, so the minimum above is β, and furthermore, there is only one expression in the min equal to β, and so the inequality becomes an equality. So we get $\nu_p(c_i) = \beta - i$. $\square$

Note that this argument breaks for $i = \beta + 1$, because the inner min becomes β as well, and so we cannot declare the equality at the end. For $i > \beta$, the only thing we know is that $\nu_p(c_i) \geq 0$, since it is an integer. In fact, in testing, it is possible for the valuation to become positive again.

Also, this lemma shows that the valuations of the c_i *must* first decrease to 0 before they can begin jumping around uncontrollably. We take advantage of this fact in the the proof of the next proposition.

Proposition 4.14. *For all i, $\langle\gamma_i\rangle \cap \langle 1\rangle = \{0\}$.*

Proof. Suppose $m = c\gamma_i$ for some non-zero $m, c \in \mathbb{Z}$. Then by Lemma 4.11, we have $m = (0, \ldots, 0, cg_0, c^p g_1, \ldots)$ where $m_{i-1} = cg_0$, $m_i = c^p g_1$ and so on. Since $m_0, \ldots, m_{i-2}$ are all equivalent to 0 (mod p^α), we get that $\nu_p(m_0), \ldots, \nu_p(m_{i-2}) \geq \alpha$. Also, since $c^p g_0 \neq 0$, we have that $\nu_p(m_{i-1}) < \alpha$. Applying Lemma 4.13, we must have that $\nu_p(m_{i-2}) = \alpha$, which gives that $\nu_p(m) = \alpha + i - 2$ and $\nu_p(m_{i-1}) = \alpha - 1$.

Now, let $\beta = \nu_p(c)$. Since $m \neq 0$ and $|\gamma_i| = p^{\alpha-1}$, we get that $\beta < \alpha - 1$. We also get that $\alpha - 1 = \nu_p(m_{i-1}) = \beta + 1$. Using Lemma 4.10, we get

$$\alpha - 1 = \nu_p(m_i) + 1 = \nu_p(c^p g_1) + 1 = p\beta + (p-1) + 1 = p(\beta + 1) = p(\alpha - 1).$$

This series of equalities implies that $p = 1$, a contradiction. So we must have that $m = 0$. $\square$

With these propositions, we finally have all the tools we need to prove the theorem at the beginning of the section.

Proof of Theorem 4.9. From Corollary 4.3, we have that $|1| = p^{\alpha+n-1}$. From Proposition 4.12, we have that $|\gamma_1| = \cdots = |\gamma_{n-1}| = p^{\alpha-1}$. Furthermore, these elements generate subgroups whose pairwise intersections are always zero. So we have

$$(\mathbb{Z}/p^{n+\alpha-1}\mathbb{Z}) \oplus (\mathbb{Z}/p^{\alpha-1}\mathbb{Z})^{n-1} \leq \boldsymbol{W}_{p,n}(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{+}.$$

But also

$$p^{\alpha+n-1} \cdot (p^{\alpha-1})^{n-1} = p^{\alpha n} = |\boldsymbol{W}_{p,n}(\mathbb{Z}/p^{\alpha}\mathbb{Z})|$$

which completes the proof. $\square$

4.4 The Multiplicative Structure of $W_{p,n}(\mathbb{Z}/p^{\alpha}\mathbb{Z})$

Now we know the additive structure *and* we have an explicit formula for the generators of each component. This construction of the generators, while not extremely complicated, could actually be simpler. From computer testing and proof sketches, the author believes that generators of the form $\gamma_i = V^{i-1}(p, 0, 0, \ldots)$ would also work. However, the particular generators in the previous section were chosen for their *multiplicative* properties. This is a ring after all, and we'd like to have a (relatively) simple expression for multiplication. Unfortunately, the multiplication cannot be done componentwise, as the author initially hoped. However, it can still be simplified quite a bit compared to the standard product polynomials. We start with the following proposition.

Proposition 4.15. *For $i \neq j$, $\gamma_i\gamma_j = 0$.*

Proof. Without loss of generality, suppose $i < j$. Then the first $j-1$ components of $\gamma_i\gamma_j$ are zero and for $k \geq j$, we have the following:

$$\begin{aligned}
&P_k(\gamma_i, \gamma_j) \\
&= \frac{1}{p^k}\Big[(p^{i-1}g_0^{p^{k-i+1}} + \cdots + p^k g_{k-i+1})(p^{j-1}g_0^{p^{k-j+1}} + \cdots + p^k g_{k-j+1}) \\
&\qquad - (p^j P_j^{p^{k-j}} + \cdots + p^{k-1}P_{k-1}^p)\Big]
\end{aligned}$$

Since $k > i$, the first factor inside the brackets is $p^{i-1}\sum_{\ell=0}^{k-i+1} p^\ell g_\ell^{p^{k-i+1-\ell}}$, which is 0 by Equation (4.3). This holds for all $k \geq j$, so each $P_k = 0$. Thus $\gamma_i\gamma_j = 0$. □

This proposition already vastly simplifies multiplication! We know we can write any element of $\boldsymbol{v} \in \boldsymbol{W}_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$ as $v = v_0 + \sum_{i=1}^{n-1} v_i\gamma_i$, where $v_0 \in \mathbb{Z}/p^{\alpha+n-1}\mathbb{Z}$ and $v_i \in \mathbb{Z}/p^{\alpha-1}\mathbb{Z}$. Multiplying two elements of this form would give many terms of the form $\gamma_i\gamma_j$ with $i \neq j$, which all disappear! Multiplying any of the γ's by an integer doesn't introduce any more complications, but there will still be terms of the form $c\gamma_i^2$. To take care of these terms, we can use the next proposition.

Proposition 4.16. *For all i, $\gamma_i^2 = p^i\gamma_i$.*

Proof. Since, the first $i-1$ components of γ_i are zero, the first $i-1$ components of both γ_i^2 and $p^i\gamma_i$ will also be zero. So we consider

$$P_{i-1}(\gamma_i, \gamma_i) = \frac{1}{p^{i-1}}[(p^{i-1}g_0)(p^{i-1}g_0)] = p^{i-1}g_0^2 = p^i g_0.$$

Then, for $k \geq i$, we have

$$\begin{aligned}
P_k(\gamma_i, \gamma_i) &= \frac{1}{p^k}\left[\underbrace{(p^{i-1}g_0^{p^{k-i+1}} + \cdots + p^k g_{k-i+1})}_{=0 \text{ by Equation (4.3)}}{}^2 - (p^i P_i^{p^{k-i}} + \cdots + p^{k-1}P_{k-1}^p)\right] \\
&= -\frac{1}{p^k}\sum_{j=i-1}^{k} p^j P_j^{k-j}
\end{aligned}$$

Now we turn our attention to $p^i\gamma_i$. From Lemma 4.11, we have that the first non-zero component is also $p^i g_0$. Then we can perform the same computation as above and the first term inside the brackets will *again* be zero by Equation (4.3). So the resulting expression has exactly the same form. That is, inductively, for $k \geq i$, we have

$$P_k(\gamma_i, \gamma_i) = -\frac{1}{p^k}\sum_{j=i-1}^{k} p^j P_j^{k-j}(\gamma_i, \gamma_i) = -\frac{1}{p^k}\sum_{j=i-1}^{k} p^j P_j^{k-j}(p^i, \gamma_i) = P_k(p^i, \gamma_i).$$

Therefore $\gamma_i^2 = p^i\gamma_i$. $\square$

Note that it is perfectly valid here to have $i \geq \alpha$, and so we may end up with $\gamma_i^2 = 0$. Using these two propositions, we can see right away how to multiply two elements in this new form. Let $\boldsymbol{a} = a_0 + \sum_{i=1}^{n-1} a_i\gamma_i$ and $\boldsymbol{b} = b_0 + \sum_{i=1}^{n-1} b_i\gamma_i$. Then we have

$$\begin{aligned}
\boldsymbol{ab} &= \left(a_0 + \sum_{i=1}^{n-1} a_i\gamma_i\right)\left(b_0 + \sum_{i=1}^{n-1} b_i\gamma_i\right) \\
&= a_0\left(b_0 + \sum_{i=1}^{n-1} b_i\gamma_i\right) + a_1\gamma_1\left(b_0 + \sum_{i=1}^{n-1} b_i\gamma_i\right) + \cdots + a_{n-1}\gamma_{n-1}\left(b_0 + \sum_{i=1}^{n-1} b_i\gamma_i\right) \\
&= a_0b_0 + \sum_{i=1}^{n-1} a_0b_i\gamma_i + (a_1b_0\gamma_1 + a_1b_1\gamma_1^2) + \cdots + (a_{n-1}b_0\gamma_1 + a_{n-1}b_{n-1}\gamma_{n-1}^2) \\
&= a_0b_0 + \sum_{i=1}^{n-1}(a_0b_i + a_ib_0 + p^ia_ib_i)\gamma_i
\end{aligned}$$

This *greatly* simplifies the multiplication compared to using the product polynomials. We can also see from the formula that it's not quite component-wise multiplication, but it's close: the only coefficient that is affecting the other components is the integer part at the start. As far as the authors can tell (through computer testing), this seems unavoidable. That is, there seems to be no alternative choice for γ_i where the multiplication can be done component-wise.

4.5 The Coefficients of γ_i

We now turn our attention to *how* we can compute the coefficients of 1 and the γ_i for any vector $\boldsymbol{v} \in \boldsymbol{W}_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$. Our goal in this section is to prove this theorem.

Theorem 4.17. *Let $\boldsymbol{v} \in \boldsymbol{W}_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$. Define $c_0 = w_{n-1}(\boldsymbol{v})$ and for $i \in \{1, \ldots, n-1\}$, $c_i = p^{-i}(w_{i-1}(\boldsymbol{v}) - c_0)$, where w_j is the jth Witt polynomial. Then, with the γ_i defined as above,*

$$\boldsymbol{v} = \boldsymbol{c_0} + \sum_{i=1}^{n-1} c_i \gamma_i.$$

Note. These computations must be done in the integers because of the denominators in the formula for the c_i and because c_0 is in $\mathbb{Z}/p^{n+\alpha-1}\mathbb{Z}$.

As with the g_i in Section 4.3, by construction, these c_i are rational numbers with denominators divisible by p. However, we want $c_i \in \mathbb{Z}/p^{\alpha-1}\mathbb{Z}$, and so we need denominators *not* divisible by p. For this, we have the following lemma.

Lemma 4.18. *The c_i defined in Theorem 4.17 are integers for all $\boldsymbol{v} \in \boldsymbol{W}_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$.*

Proof. We consider the numerator of c_i,

$$\begin{aligned} w_{i-1}(\boldsymbol{v}) - w_{n-1}(\boldsymbol{v}) &= \sum_{j=0}^{i-1} p^j v_j^{p^{(i-1)-j}} - \sum_{j=0}^{n-1} p^j v_j^{p^{(n-1)-j}} \\ &= \sum_{j=0}^{i-1} p^j \left(v_j^{p^{(i-1)-j}} - v_j^{p^{(n-1)-j}} \right) - \sum_{j=i}^{n-1} p^j v_j^{p^{(n-1)-j}} \end{aligned}$$

Every term in the second sum is divisible by p^i, so we need only focus on the terms in the first sum. Let $0 \le j \le i-1$. If $v_j = 0$, the entire term is 0 and so is divisible by p^i. So assume $v_j \neq 0$. Then we have

$$\begin{aligned} p^j \left(v_j^{p^{(i-1)-j}} - v_j^{p^{(n-1)-j}} \right) &= p^j v_j^{p^{(i-1)-j}} \left(1 - v_j^{p^{(n-1)-j} - p^{(i-1)-j}} \right) \\ &= p^j v_j^{p^{(i-1)-j}} \left(1 - v_j^{p^{(i-1)-j}(p^{n-i}-1)} \right) \end{aligned}$$

Since $i < n$, we have, by Fermat's Little Theorem, $v_j^{p^{n-i}-1} \equiv 1 \mod p$, since $(p-1) \mid (p^{n-i}-1)$. Then, by Lemma 1.4 of [Rab14], this gives $v_j^{p^{(i-1)-j}(p^{n-i}-1)} \equiv 1 \mod p^{i-j}$. So

$p^{i-j} \mid \left(1 - v_j^{p^{(i-1)-j}(p^{n-i}-1)}\right)$, and thus p^i divides the entire term because we're multiplying by p^j at the front. Therefore p^i divides every term in the numerator, and so c_i is an integer. $\square$

So we know it makes sense to use these c_i as the coefficients. Before we prove Theorem 4.17, we need the following lemma about what happens when we add an element of $\langle \gamma_i \rangle$ to an arbitrary Witt vector.

Lemma 4.19. *Let $\boldsymbol{v} = (v_0, \ldots, v_{n-1}) \in \boldsymbol{W}_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$ and let $c \in \mathbb{Z}$. Define $\boldsymbol{w} = (w_0, \ldots, w_{n-1}) = \boldsymbol{v} + c\gamma_i$. Then $w_j = v_j$ for $0 \le j < i-1$, $w_{i-1} = v_{i-1} + cp$, and for $j \ge i$,*

$$w_j = v_j + \sum_{k=i-1}^{j-1} \frac{1}{p^{j-k}} \left(v_k^{p^{j-k}} - w_k^{p^{j-k}} \right).$$

Proof. We have $c\gamma_i = (\underbrace{0, \ldots, 0}_{i-1 \text{ zeroes}}, cg_0, c^p g_1, \ldots)$. So we get

$$\boldsymbol{v} + c\gamma_i = (v_0, \ldots, v_{i-2}, v_{i-1} + cg_0, S_i(\boldsymbol{v}, c\gamma_i), S_{i+1}(\boldsymbol{v}, c\gamma_i), \ldots).$$

Since $g_0 = p$, this shows the first two of the three statements in the lemma. So now we let $j \ge i$ and consider

$$\begin{aligned}
w_j &= S_j(\boldsymbol{v}, c\gamma_i) \\
&= v_j + c^{p^{j-(i-1)}} g_{j-(i-1)} + \sum_{k=1}^{j-(i-1)} \frac{1}{p^k} \left(v_{j-k}^{p^k} + (c^{p^{j-(i-1)-k}} g_{j-(i-1)-k})^{p^k} - w_{j-k}^{p^k} \right) \\
&= v_j + \sum_{k=1}^{j-(i-1)} \frac{1}{p^k} \left(v_{j-k}^{p^k} - w_{j-k}^{p^k} \right) + \sum_{k=0}^{j-(i-1)} \frac{1}{p^k} (c^{p^{j-(i-1)-k}} g_{j-(i-1)-k})^{p^k} \\
&= v_j + \sum_{k=1}^{j-(i-1)} \frac{1}{p^k} \left(v_{j-k}^{p^k} - w_{j-k}^{p^k} \right) + \frac{c^{p^{j-(i-1)}}}{p^{j-(i-1)}} \underbrace{\sum_{k=0}^{j-(i-1)} p^{j-(i-1)-k} g_{j-(i-1)-k}^{p^k}}_{0 \text{ by Equation (4.3)}} \\
&= v_j + \sum_{k=i-1}^{j-1} \frac{1}{p^{j-k}} \left(v_k^{p^{j-k}} - w_k^{p^{j-k}} \right).
\end{aligned}$$

$\square$

This is the final tool we need to prove Theorem 4.17.

Proof of Theorem 4.17. For the sake of notation, let $\boldsymbol{a_0} = (a_{0,0}, \ldots, a_{0,n-1}) := \boldsymbol{c_0}$. Then, for $i \in 1, \cdots, n-1$, recursively define

$$\boldsymbol{a_i} = (a_{i,0}, \ldots, a_{i,n-1}) := \boldsymbol{a_{i-1}} + c_i \gamma_i.$$

Under this notation, we have, for $0 < i, j \leq n-1$,

$$a_{i,j} = S_j(\boldsymbol{a_{i-1}}, c_i \gamma_i).$$

Our goal is to show that $\boldsymbol{a_{n-1}} = \boldsymbol{v}$. By Lemma 4.19, we have

$$\begin{aligned} a_{1,0} &= a_{0,0} + c_1 g_0 \\ &= a_{0,0} + w_0(\boldsymbol{v}) - w_{n-1}(\boldsymbol{v}) \\ &= v_0 + a_{0,0} - c_0 = v_0. \end{aligned}$$

So $\boldsymbol{a_1} = (v_0, a_{1,1}, \ldots, a_{1,n-1})$. Now, inductively assume $\boldsymbol{a_j} = (v_0, \ldots, v_{j-1}, a_{j,j}, \ldots, a_{j,n-1})$ for all $j < i$ and consider $\boldsymbol{a_i}$. For all $k < i-1$, we have

$$a_{i,k} = S_k(\boldsymbol{a_{i-1}}, c_i \gamma_i) = a_{i-1,k} = v_k,$$

since the first $i-1$ components of $c_i \gamma_i$ are 0. Then, repeatedly using Lemma 4.19, we have

$$\begin{aligned} a_{i,i-1} &= S_{i-1}(\boldsymbol{a_{i-1}}, c_i \gamma_i) \\ &= a_{i-1,i-1} + pc_i \\ &= S_{i-1}(\boldsymbol{a_{i-2}}, c_{i-1} \gamma_{i-1}) + pc_i \\ &= a_{i-2,i-1} + \sum_{k=i-2}^{i-2} \frac{1}{p^{(i-1)-k}} \left(a_{i-2,k}^{p^{(i-1)-k}} - a_{i-1,k}^{p^{(i-1)-k}} \right) + pc_i \\ &= a_{i-3,i-1} + \sum_{m=i-3}^{i-2} \sum_{k=m}^{i-2} \frac{1}{p^{(i-1)-k}} \left(a_{m,k}^{p^{(i-1)-k}} - a_{m+1,k}^{p^{(i-1)-k}} \right) + pc_i \\ &= \vdots \end{aligned}$$

$$
\begin{aligned}
&= a_{0,i-1} + \sum_{m=0}^{i-2} \sum_{k=m}^{i-2} \frac{1}{p^{(i-1)-k}} \left(a_{m,k}^{p^{(i-1)-k}} - a_{m+1,k}^{p^{(i-1)-k}} \right) + pc_i \\
&= a_{0,i-1} + \sum_{k=0}^{i-2} \frac{1}{p^{(i-1)-k}} \underbrace{\sum_{m=0}^{k} \left(a_{m,k}^{p^{(i-1)-k}} - a_{m+1,k}^{p^{(i-1)-k}} \right)}_{\text{telescoping}} + pc_i \\
&= a_{0,i-1} + \sum_{k=0}^{i-2} \frac{1}{p^{(i-1)-k}} \left(a_{0,k}^{p^{(i-1)-k}} - a_{k+1,k}^{p^{(i-1)-k}} \right) + pc_i \\
&= \sum_{k=0}^{i-1} \frac{1}{p^{(i-1)-k}} a_{0,k}^{p^{(i-1)-k}} + pc_i - \sum_{k=0}^{i-2} \frac{1}{p^{(i-1)-k}} a_{k+1,k}^{p^{(i-1)-k}} \\
&= \frac{1}{p^{i-1}} \left[\sum_{k=0}^{i-1} p^k a_{0,k}^{p^{(i-1)-k}} - c_0 + w_{i-1}(\boldsymbol{v}) - \sum_{k=0}^{i-2} p^k a_{k+1,k}^{p^{(i-1)-k}} \right] \\
&= \frac{1}{p^{i-1}} \left[a_{0,0} - c_0 + p^{i-1} v_{i-1} \right] = v_{i-1}.
\end{aligned}
$$

This induction gives us that $\boldsymbol{a_{n-1}} = (v_0, \ldots, v_{n-2}, a_{n-1,n-1})$. So finally we need to compute

$$
\begin{aligned}
a_{n-1,n-1} &= S_{n-1}(\boldsymbol{a_{n-2}}, c_{n-1}\gamma_{n-1}) \\
&= a_{n-2,n-1} + \sum_{k=n-2}^{n-2} \frac{1}{p^{(n-1)-k}} \left(a_{n-2,k}^{p^{(n-1)-k}} - a_{n-1,k}^{p^{(n-1)-k}} \right) \\
&= \vdots \\
&= a_{0,n-1} + \sum_{m=0}^{n-2} \sum_{k=m}^{n-2} \frac{1}{p^{(n-1)-k}} \left(a_{m,k}^{p^{(n-1)-k}} - a_{m+1,k}^{p^{(n-1)-k}} \right) \\
&= a_{0,n-1} + \sum_{k=0}^{n-2} \frac{1}{p^{(n-1)-k}} \sum_{m=0}^{k} \left(a_{m,k}^{p^{(n-1)-k}} - a_{m+1,k}^{p^{(n-1)-k}} \right) \\
&= a_{0,n-1} + \sum_{k=0}^{n-2} \frac{1}{p^{(n-1)-k}} \left(a_{0,k}^{p^{(n-1)-k}} - a_{k+1,k}^{p^{(n-1)-k}} \right) \\
&= \frac{1}{p^{n-1}} \left[\sum_{k=0}^{n-1} p^k a_{0,k}^{p^{(n-1)-k}} - \sum_{k=0}^{n-2} p^k a_{k+1,k}^{p^{(n-1)-k}} \right] \\
&= \frac{1}{p^{n-1}} \left[a_{0,0} - \sum_{k=0}^{n-2} p^k v_k^{p^{(n-1)-k}} \right] \\
&= \frac{1}{p^{n-1}} \left[w_{n-1}(\boldsymbol{v}) - \sum_{k=0}^{n-2} p^k v_k^{p^{(n-1)-k}} \right] = v_{n-1}.
\end{aligned}
$$

Therefore $\boldsymbol{a_{n-1}} = \boldsymbol{v}$ and the formulas for the c_i are correct. $\square$

Finally, we note that these formulas also give us an algorithm for computing the components of a Witt vectors from the c_i without using the sum polynomials. Given $c_0, \ldots, c_{n-1}$, the v_i can be computed recursively as follows. For $i \in \{0, \ldots, n-2\}$, we have

$$v_i = \frac{c_0 + p^{i+1}c_i - \sum_{j=0}^{i-1} p^j v_j^{p^{i-j}}}{p^i}$$

and the final component is given by

$$v_{n-1} = \frac{c_0 - \sum_{j=0}^{n-2} p^j v_j^{p^{n-1-j}}}{p^{n-1}}.$$

Bibliography

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 42

[Bor11] James Borger. The basic geometry of Witt vectors, I: The affine case. Algebra Number Theory, 5(2):231–285, 2011. 3

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hansischen Univ., 14:197–272, 1941. 2

[DK14] Christopher Davis and Kiran S. Kedlaya. On the Witt vector Frobenius. Proc. Amer. Math. Soc., 142(7):2211–2226, 2014. 7, 49

[Fin02] Luís R. A. Finotti. Degrees of the elliptic Teichmüller lift. J. Number Theory, 95(2):123–141, 2002. 12, 37

[Fin04] Luís R. A. Finotti. Minimal degree liftings of hyperelliptic curves. J. Math. Sci. Univ. Tokyo, 11(1):1–47, 2004. 12

[Fin11] Luís R. A. Finotti. Computations with Witt vectors of length 3. J. Théor. Nombres Bordeaux, 23(2):417–454, 2011. 36

[Fin14] Luís R. A. Finotti. Computations with Witt vectors and the Greenberg transform. Int. J. Number Theory, 10(6):1431–1458, 2014. 3, 8, 36, 53

[Fin20] Luís R. A. Finotti. Weierstrass coefficients of the canonical lifting. Int. J. Number Theory, 16(2):397–422, 2020. 3, 9, 12, 19, 22, 23, 31, 35, 38, 42

[FL20] Luís R. A. Finotti and Delong Li. Denominators of the Weierstrass coefficients of the canonical lifting. Available at http://www.math.utk.edu/~finotti, 2020. 3, 23, 35

[FL21] Luís R. A. Finotti and Delong Li. The discriminant in universal formulas for the canonical lifting. Bull. Sci. Math., 169:Paper No. 102981, 20, 2021. 3, 23, 35, 41

[FL23] Luís R. A. Finotti and Delong Li. Improved bounds for the denominators in the formulas of the canonical lifting. Available at http://www.math.utk.edu/~finotti, 2023. 3, 35, 41, 42

[Haz09] Michiel Hazewinkel. Witt vectors. I. In Handbook of algebra. Vol. 6, volume 6 of Handb. Algebr., pages 319–472. Elsevier/North-Holland, Amsterdam, 2009. 3

[Hes15] Lars Hesselholt. The big de rham–witt complex. Acta mathematica, 214(1):135–207, 2015. 3, 56

[LST64] Jonathan Lubin, Jean-Pierre Serre, and John Tate. Elliptic curves and formal groups. *Proc. of Woods Hole summer institute in algebraic geometry*. Available at https://web.ma.utexas.edu/users/voloch/lst.html, 1964. 2

[Poo01] Bjorn Poonen. Computing torsion points on curves. Experiment. Math., 10(3):449–465, 2001. 2

[Rab14] Joseph Rabinoff. The Theory of Witt Vectors, 2014. 3, 5, 6, 7, 49, 52, 53, 56, 64

[Sat00] Takakazu 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. 2

[Sil86] Joseph H. Silverman. The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, 106. Springer New York, New York, NY, 1986. 1

[The23] The Sage Developers. SageMath, the Sage Mathematics Software System (Version 9.8), 2023. `https://www.sagemath.org`. 42

[Vol97] José Felipe Voloch. Torsion points of $y^2 = x^6 + 1$. Available at https://www.ma.utexas.edu/users/voloch/oldpreprint.html, 1997. 2

[VW00] José Felipe Voloch and Judy L. Walker. Euclidean weights of codes from elliptic curves over rings. Trans. Amer. Math. Soc., 352(11):5063–5076, 2000. 2

Vita

Jacob Dennerlein was born in 1995 to Paula Johnson and Jesse Dennerlein and grew up in both Washington State and Kentucky. He attended Bethlehem High School and after graduating in 2013, moved to Murray, KY to attend Murray State University. In 2017, he graduated with his B.S. in Mathematics and Computer Science. After experiencing the joys of higher-level mathematics, he decided to pursue his Ph.D. in Mathematics at the University of Tennessee, Knoxville to continue his exploration of the subject. Jacob finished his Ph.D. in 2023.