JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Luís R. A. FINOTTI

Computations with Witt vectors of length 3

Tome 23, n^o 2 (2011), p. 417-454.

<http://jtnb.cedram.org/item?id=JTNB_2011__23_2_417_0>

Journal de Théorie des Nombres de Bordeaux **23** (2011), 417-454

Computations with Witt vectors of length 3

par Luís R. A. FINOTTI

Résumé. Dans cet article, nous décrivons comment effectuer des calculs avec les vecteurs de Witt de longueur 3 d'une manière efficace et donnons une formule qui permet de calculer directement la troisième coordonnée de la transformée de Greenberg d'un polynôme. Nous appliquons ces résultats afin d'obtenir des renseignements sur la troisième coordonnée de l'invariant j du relèvement canonique en fonction de l'invariant j de la courbe elliptique ordinaire en caractéristique p.

Abstract. In this paper we describe how to perform computations with Witt vectors of length 3 in an efficient way and give a formula that allows us to compute the third coordinate of the Greenberg transform of a polynomial directly. We apply these results to obtain information on the third coordinate of the j-invariant of the canonical lifting as a function on the j-invariant of the ordinary elliptic curve in characteristic p.

1. Introduction

Let $\Bbbk$ be a perfect field of characteristic $p > 0$, $\boldsymbol{W}(\Bbbk)$ be the ring of Witt vectors over $\Bbbk$, and $\boldsymbol{W}_n(\Bbbk)$ denote the ring of Witt vectors of length n, which in this case can be seen as the quotient of $\boldsymbol{W}(\Bbbk)$ modulo the principal ideal generated by p^n. (See section 2 for a quick review of Witt vectors.) Then, given an ordinary elliptic curve $E/\Bbbk$, there is a unique elliptic curve (up to isomorphism), say $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$, which reduces to E modulo p for which we can lift the Frobenius. $\boldsymbol{E}$ is then called the *canonical lifting* of E. (See, for instance, [4] or [16].) Hence, given an ordinary j-invariant $j_0 \in \Bbbk$, the canonical lifting gives us a unique $\boldsymbol{j} \in \boldsymbol{W}(\Bbbk)$. Therefore, if $\Bbbk^{\mathrm{ord}}$ denotes the set of ordinary values of j-invariants in $\Bbbk$, then we have functions $J_i : \Bbbk^{\mathrm{ord}} \to \Bbbk$, for $i = 1, 2, 3, \ldots$, such that the j-invariant of the canonical lifting of an elliptic curve with j-invariant $j_0 \in \Bbbk^{\mathrm{ord}}$ is $(j_0, J_1(j_0), J_2(j_0), \ldots)$.

B. Mazur asked about the nature of these functions J_i and J. Tate asked about the possibility of extending them to supersingular values. (See [10].)

Tate's question motivates the following definition:

Manuscrit reçu le 4 février 2010, révisé le 26 juillet 2010.

Mots clefs. Witt vectors, elliptic curves, canonical lifting, pseudo-canonical lifting, modular polynomial.

Classification math. 11G20, 11Y16.

Definition 1.1. Suppose that $j_0 \not\in \Bbbk^{\mathrm{ord}}$ and J_i is regular at j_0 for all $i \leq n$. Then, we call an elliptic curve over $\boldsymbol{W}(\Bbbk)$ whose the j-invariant reduces to $(j_0, J_1(j_0), \dots, J_n(j_0))$ modulo p^{n+1} a *pseudo-canonical lifting modulo* p^{n+1} *(or over* $\boldsymbol{W}_{n+1}(\Bbbk)$*)* of the elliptic curve associated to j_0.

If J_i is regular for all i, we call the elliptic curve with j-invariant $(j_0, J_1(j_0), J_2(j_0), \dots)$ the *pseudo-canonical lifting* of the elliptic curve associated to j_0.

Hence, Tate asks about the existence of such pseudo-canonical liftings. One would not expect pseudo-canonical liftings to exist, as they would yield curves which although are not canonical liftings, as those do not exist in the supersingular case, are obtained through the same formulas. On the other hand, we've proved that pseudo-canonical liftings modulo p^2 do exist. More precisely, we've studied J_1 in detail in [10] (using many results from [13]), proving the following:

Theorem 1.2. *With the notation above and* $p \geq 5$*:*

1. $J_i \in \mathbb{F}_p(X)$ *for all* i.
2. $J_1(X)$ *is* always *regular at* $X = 0$ *and* $X = 1728$*, even when those values are supersingular.*
3. *We* always *have that* $(0, J_1(0)) \equiv 0 \pmod{p^2}$ *and* $(1728, J_1(1728)) \equiv 1728 \pmod{p^2}$.
4. *If* $j_0 \not\in \Bbbk^{\mathrm{ord}} \cup \{0, 1728\}$*, then* J_1 *has a simple pole at* j_0.
5. $J_1(X)$ *has a zero of order* $\lfloor (2p+1)/3 \rfloor$ *at* $X = 0$.

In particular, this theorem tells us that only 0 and 1728 yield pseudo-canonical liftings modulo p^2 (and they always do!), and hence we can only possibly have pseudo-canonical liftings for those values.

Before proving the result above, we were able to conjecture it to be true from computational evidence. In the same way, we wanted to have some computational data on J_2 to form a proper conjecture in that case. The problem is that computations with Witt vectors of length 3 demand a lot more computer power than with length 2.

At first, the author computed J_1 and J_2 by computing the canonical lifting of the elliptic curve E given by $y_0^2 = x_0^3 + a_0 x_0 + b_0$ over $\mathbb{F}_p(a_0, b_0)$, where a_0 and b_0 were variables, i.e., algebraically independent transcendental elements over $\mathbb{F}_p$, using the algorithm described in [6]. (Note that the algorithm gives more than just the canonical lifting $\boldsymbol{E}$ of E. It also gives a lifting of points from $E(\bar{\Bbbk})$ to $\boldsymbol{E}(\boldsymbol{W}_3(\bar{\Bbbk}))$ called the *elliptic Teichmüller lift.*) The algorithm gives the coefficients of the Weierstrass equation of the canonical lifting over $\boldsymbol{W}_3(\mathbb{F}_p(a_0, b_0))$, say $\boldsymbol{a} = (a_0, a_1, a_2)$ and $\boldsymbol{b} = (b_0, b_1, b_2)$, where $a_i, b_i \in \mathbb{F}_p(a_0, b_0)$ for $i = 1, 2$. Thus, we can compute its j-invariant using the operations of Witt vectors. The resulting formula can then be easily be put in $\mathbb{F}_p(j_0)$, where $j_0 = 1728(4a_0^3)/(4a_0^3 + 27b_0^2)$, thus giving us $J_1(X)$ and $J_2(X)$.

But, since a_0 and b_0 were taken as variables in a field of rational functions, the computations get quite demanding. While we were able to compute the reduction modulo p^2 of the canonical lifting, i.e., a_1 and b_1, for several values of p, we could only initially compute a_2 and b_2 for $p \leq 13$. With the methods used at the time, the computation of the third coordinate of the canonical lifting (and elliptic Teichmüller lift) for $p = 17$ in this situation used almost 24 gigabytes of memory (16 gigabytes of RAM and 8 gigabytes of swap) before it crashed still unfinished. Formulas for the canonical lifting and elliptic Teichmüller lift modulo p^3 for $p \leq 13$ can be found, at the time of writing, at

`http://www.math.utk.edu/~finotti/can_lifts/`.

On the other hand, as seen in [10], one can compute J_1 much more efficiently by using the (classical) modular polynomial. More precisely, we have:

Theorem 1.3. *Let $\Phi_p(X,Y)$ denote the modular polynomial and $\bar{H}_p(X)$ be the reduction modulo p of $\Phi_p(X,X^p)/p$. Then,*

$$J_1(X) = -\bar{H}_p(X)/(X^{p^2} - X).$$

The goal here is then twofold: on the one hand, we would like to find a more efficient way to perform computation with Witt vectors of length 3 in general. (We have special interest on Witt vectors over polynomial rings. Over finite fields computations can be done quickly by working with the proper extension of $\mathbb{Z}_p$ instead.) On the other hand, we would like to find an efficient way to compute J_2, in the same vein as Theorem 1.3, so that we can obtain more precise information on its nature, in the same vein as Theorem 1.2.

It should be mentioned up front that we will not be able to prove a full analogue of Theorem 1.2 to J_2 here. Theorem 9.6 gets pretty close, while Conjecture 9.3 gives what we believe, from numerical evidence, to be the missing pieces. In particular, Theorem 9.6 tells us that $j = 0$ yields pseudo-canonical liftings modulo p^3, while Conjecture 9.3 states that $j = 1728$ does not.

Also, Theorem 9.1 gives a precise description of how to obtain J_2 from the modular polynomial as done in Theorem 1.3, although the formula is not nearly as simple. More precisely, Eq. (9.1) gives us

$$J_2(X) = \frac{F(X)}{(X^{p^2} - X)^{2p+1}}$$

for some polynomial $F(X)$ that can be explicitly obtained from $\Phi_p(X, X^p)$. Theorem 9.6 and Conjecture 9.3 describe $J_2(X)$ as *reduced* rational function, thus giving information about possible pseudo-canonical liftings.

It should also be mentioned that the method from [6] used to obtain the initial examples of J_2 mentioned above is not the most efficient. There are better methods to compute the canonical lifting if we are not also interested in the elliptic Teichmüller lift. (In fact, Theorem 9.1 below gives us one such method.) One of the difficulties of this method is the computation of the *Greenberg transform* (see section 3) of an elliptic curve over a ring of Witt vectors of length 3, and we study here also an efficient way to compute the Greenberg transform. (See Theorem 6.1.)

We should emphasize that our result on the Greenberg transform is not just of importance to our algorithm to compute the canonical lifting together with the Teichmüller lift, although it is still relevant as one might actually need the elliptic Teichmüller lift (e.g., to construct error-correcting codes as in [19] and [8]). It also has theoretical implications, namely, it is the most important step in obtaining Theorems 9.1 and 9.6 mentioned above.

Moreover, the formula for the third coordinate of the Greenberg transform given here is necessary if one wants to attempt to generalize the method to prove Theorem 1.2 in [10] to try to prove Conjecture 9.3.

We now give a brief description of the content of the next sections. Section 2 and 3 give brief reviews of Witt vectors and Greenberg transform, respectively. Section 4 introduces many auxiliary functions that are necessary to describe the third coordinate of the Greenberg transform of a polynomial. Section 5 gives efficient methods to compute these auxiliary functions, giving also an efficient method to compute the polynomials that give the third coordinates of sums and products of Witt vectors. Section 6 gives the formula for the third coordinate of the Greenberg transform of a polynomial. Section 7 briefly analyzes the complexity of the computations using the new methods introduced, while Section 8 gives explicit examples of how much time and memory is saved when computing the first three coordinates of the Greenberg with these methods in some specific cases. Section 9 gives the results and conjectures on J_2. Finally, section 10 has a brief discussion and speculations on what happens with J_3.

The reader will notice that we need to introduce a lot of notation and that proofs, although mostly straight forward, sometimes are done by long and involved computations. Although this might make it tedious and laborious to follow some proofs, hopefully it will not prevent one from appreciating the results themselves.

2. Witt vectors

In this section we will review some of the basic facts about Witt vectors. More details, including motivation and proofs, can be found in [17] or [12]. Let p be a prime, and and for each non-negative integer n consider

$$W^{(n)}(X_0,\ldots,X_n) \overset{\text{def}}{=} X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^n X_n, \tag{2.1}$$

the corresponding *Witt polynomial.* Then, there exist polynomials $S_i, P_i \in \mathbb{Z}[X_0,\ldots,X_i,Y_0,\ldots,Y_i]$ satisfying:

$$W^{(n)}(S_0,\ldots,S_n) = W^{(n)}(X_0,\ldots,X_n) + W^{(n)}(Y_0,\ldots,Y_n) \tag{2.2}$$

and

$$W^{(n)}(P_0,\ldots,P_n) = W^{(n)}(X_0,\ldots,X_n) \cdot W^{(n)}(Y_0,\ldots,Y_n). \tag{2.3}$$

More explicitly, we have the following recursive formulas:

$$S_n = (X_n+Y_n)+\frac{1}{p}(X_{n-1}^p+Y_{n-1}^p-S_{n-1}^p)+\cdots+\frac{1}{p^n}(X_0^{p^n}+Y_0^{p^n}-S_0^{p^n}), \tag{2.4}$$

and

$$\begin{aligned} P_n &= \frac{1}{p^n}\Big[(X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - \\ &\qquad \Big(P_0^{p^n} + \cdots + p^{n-1}P_{n-1}^p\Big)\Big] \\ &= (X_0^{p^n}Y_n + X_1^{p^{n-1}}Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) \\ &\quad + \frac{1}{p}(X_0^{p^n}Y_{n-1}^p + \cdots + X_{n-1}^p Y_0^{p^n}) \\ &\quad \vdots \\ &\quad + \frac{1}{p^n}(X_0^{p^n}Y_0^{p^n}) - \frac{1}{p^n}P_0^{p^n} - \cdots - \frac{1}{p}P_{n-1}^p \\ &\quad + p\left(X_1^{p^{n-1}}Y_n + X_2^{p^{n-2}}(Y_{n-1}^p + pY_n) + \ldots\right). \end{aligned} \tag{2.5}$$

(Note that despite the denominators in the formulas, cancellations yield polynomials with *integer* coefficients.)

We can then define sums and products of infinite vectors in $A^{\mathbb{Z}_{\geq 0}}$, where A is a commutative ring (with 1), say $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$, by

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

and

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

These operations make $A^{\mathbb{Z}_{\geq 0}}$ into a commutative ring (with 1) called the *ring of Witt vectors over* A and denoted by $\boldsymbol{W}(A)$.

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

Then, we obtain:

$$\bar{S}_1 = X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}, \tag{2.6}$$

$$\bar{P}_1 = X_1 Y_0^p + X_0^p Y_1, \tag{2.7}$$

and

$$\begin{aligned} \bar{S}_2 = X_2 + Y_2 + \frac{1}{p}\left(X_1^p + Y_1^p - \left(X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}\right)^p\right) \\ + \frac{X_0^{p^2} + Y_0^{p^2} - (X_0 + Y_0)^{p^2}}{p^2}, \end{aligned} \tag{2.8}$$

$$\bar{P}_2 = X_2 Y_0^{p^2} + X_1^p Y_1^p + X_0^{p^2} Y_2 + \frac{X_1^p Y_0^{p^2} + X_0^{p^2} Y_1^p - (X_1 Y_0^p + X_0^p Y_1)^p}{p}. \tag{2.9}$$

Observe that we are abusing the notation here, as it seems that we are dividing by p in rings of characteristic p. But the meaning should be clear, as we have all terms divided by p are in fact congruent to zero modulo p over $\mathbb{Z}$. Hence, we should interpret those terms as the reduction modulo p after the division by p. For instance,

$$\frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p} = \sum_{i=1}^{p-1} c_i X_0^i Y_0^{p-i},$$

where c_i is the reduction modulo p of the integer $-\frac{1}{p}\binom{p}{i}$ for $i = 1, \dots, (p-1)$.

Also, observe that although

$$X_0^{p^2} + Y_0^{p^2} - (X_0 + Y_0)^{p^2} \not\equiv 0 \pmod{p^2},$$

we have that

$$\begin{aligned} p\left(X_1^p + Y_1^p - \left(X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}\right)^p\right) \\ + X_0^{p^2} + Y_0^{p^2} - (X_0 + Y_0)^{p^2} \equiv 0 \pmod{p^2}, \end{aligned}$$

and hence we should interpret Eq. (2.8) accordingly. On section 4 we shall describe how we can define (and compute) those terms without having to refer to computations in characteristic zero, thus avoiding this clumsy notation.

One should observe that simply computing S_2 can take a lot of time and memory. For instance, for $p = 31$ the polynomial S_2 has 152994 monomials! In MAGMA creating a ring of Witt vectors of length 3, which computes the S_i and P_i for $i = 1, 2$, can take a long time. The command "`W:=WittRing(GF(31),3);`", which creates a ring of Witt vectors of length 3 over $\mathbb{F}_{31}$, takes about 150.31 seconds on a server with two 64 bit 3.2 gigahertz Inter Xeon processors and 16 gigabytes of RAM. With the methods that we describe below, we can compute the S_1, S_2, P_1, and P_2 for $p = 31$ in 1.39 seconds on the same computer.

Before we proceed, we review a few more results about Witt vectors that shall be used later on. Let $\Bbbk$ be a perfect field of characteristic p, where p is the same prime as used in $W^{(n)}$ above. Since $\Bbbk$ has characteristic p, it can be shown that $\boldsymbol{W}(\Bbbk)$ has characteristic 0 and p is represented by the Witt vector $(0, 1, 0, 0, \ldots)$ of $\boldsymbol{W}(\Bbbk)$, while p^n is represented by the Witt vector that has 1 on its $(n + 1)$-th coordinate and zeros in all others. This allows us to deduce that, since $\Bbbk$ is perfect, saying that $(a_0, a_1, \ldots)$ is congruent to $(b_0, b_1, \ldots)$ modulo p^n (or modulo the principal ideal generated by p^n) is equivalent to saying that $a_i = b_i$ for all $i \in \{0, 1, \ldots, n - 1\}$. Hence, we can represent the elements of the quotient of $\boldsymbol{W}(\Bbbk)$ by the principal ideal generated by p^n by vectors of length n in a unique way, i.e., we can identify this quotient with the *ring Witt vectors of length* n, which we denote by $\boldsymbol{W}_n(\Bbbk)$.

Also, one can show that $\boldsymbol{W}(\Bbbk)$ is a *strict p-ring* (as defined in [17]) with residue field $\Bbbk$. (Hence, any perfect field of characteristic p is a residue field of a strict p-ring.) For example, if $q = p^r$ and if we denote by $\mathbb{Z}_q$ the ring of integers of the unramified extension of $\mathbb{Q}_p$ of degree r, then we have $\mathbb{Z}_q \cong \boldsymbol{W}(\mathbb{F}_q)$.

Moreover, $\boldsymbol{W}(\Bbbk)$ has a natural lift of the (p-th power) Frobenius σ of $\Bbbk$ defined by $\sigma(a_0, a_1, \ldots) = (\sigma(a_0), \sigma(a_1), \ldots)$, and the group of units of $\boldsymbol{W}(\Bbbk)$ is the set $\boldsymbol{W}(\Bbbk)^\times = \{(a_0, a_1, \ldots) \in \boldsymbol{W}(\Bbbk) \ : \ a_0 \neq 0\}$.

Before we can make the isomorphism between $\mathbb{Z}_q$ and $\boldsymbol{W}(\mathbb{F}_q)$ explicit (with Eqs. (2.10) and (2.11) below), we need the following definitions:

Definition 2.1. (1) We denote by π the *reduction modulo p map*, i.e., $\pi((a_0, a_1, \ldots)) = a_0$.

(2) Let $a \in \Bbbk$. Then, the *Teichüller lift* of a is the Witt vector $\tau(a) \overset{\text{def}}{=} (a, 0, 0, \ldots)$. (Hence, τ is a section of π and when restricted to $\Bbbk^\times$ yields a group homomorphism.)

(3) We also define the *Teichmüller lift* of polynomial over $f \in \Bbbk[x_0, y_0]$ as the polynomial $\tau(f) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$ obtained by applying the Teichmüller lift to the coefficients of f.

(4) Define $\boldsymbol{W}(\Bbbk)^* \overset{\text{def}}{=} \{(a_0, 0, 0, \ldots) \in \boldsymbol{W}(\Bbbk) \; : \; a_0 \in \Bbbk\}$. (This is a multiplicative set. E.g., if $\Bbbk = \mathbb{F}_q$, than $\boldsymbol{W}(\Bbbk)^*$ is made of all $(q-1)$-th roots of unity and zero.)

(5) Let $\boldsymbol{a} \in \boldsymbol{W}(\Bbbk)$. Define $\xi_k(\boldsymbol{a})$, for $k \in \mathbb{Z}_{\geq 0}$, as the *unique* element of $\boldsymbol{W}(\Bbbk)^*$ such that $\boldsymbol{a} = \sum_{k=0}^{\infty} \xi_k(\boldsymbol{a}) p^k$. (This is well defined since $\boldsymbol{W}(\Bbbk)$ is a strict p-ring and $\boldsymbol{W}(\Bbbk)^*$ is a complete set of representatives of $\Bbbk = \boldsymbol{W}(\Bbbk)/(p)$ in $\boldsymbol{W}(\Bbbk)$.)

With the notation above, we have

$$\boldsymbol{a} = \sum_{k=0}^{\infty} \xi_k(\boldsymbol{a}) p^k = (\pi(\xi_0(\boldsymbol{a})), \pi(\xi_1(\boldsymbol{a}))^p, \pi(\xi_2(\boldsymbol{a}))^{p^2}, \ldots) \tag{2.10}$$

and

$$(a_0, a_1, \ldots) = \sum_{k=0}^{\infty} \tau(a_k)^{1/p^k} p^k. \tag{2.11}$$

(Remember we are assuming that $\Bbbk$ is perfect.)

3. The Greenberg transform

In this section we briefly review the definition of the Greenberg transform. (See also [14] and [11].) We will deal only with polynomials in two variables here in order to make the notation and exposition simpler, but one can easily generalize the obtained results for more variables.

Definition 3.1. Let $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$. If we replace $\boldsymbol{x}$ and $\boldsymbol{y}$ by $(x_0, x_1, \ldots)$ and $(y_0, y_1, \ldots)$ seen as Witt vectors of unknowns, and expand the resulting expression using sums and products of Witt vectors, we obtain a Witt vector $(f_0, f_1, \ldots)$, with $f_i \in \Bbbk[x_0, \ldots, x_i, y_0, \ldots, y_i]$. This resulting vector is called the *Greenberg transform* of $\boldsymbol{f}$ and will be denoted by $\mathscr{G}(\boldsymbol{f})$.

Moreover, if

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

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

It is clear from the definition that there is a bijection between $\boldsymbol{C}(\boldsymbol{W}(\Bbbk))$ and $\mathscr{G}(\boldsymbol{C})(\Bbbk)$. Also, we clearly have

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

One can recursively compute the coordinates of the Greenberg transform using the following theorem:

Theorem 3.2. *Let $\boldsymbol{f}(\boldsymbol{x},\boldsymbol{y}) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x},\boldsymbol{y}]$ and suppose that $\mathscr{G}(\boldsymbol{f}) = (f_0, f_1, \ldots)$. If*

$$(3.1)\quad W^{(n)}(\boldsymbol{f}_0,\ldots,\boldsymbol{f}_n) \equiv \boldsymbol{f}^{\sigma^n}(W^{(n)}(\boldsymbol{x}_0,\ldots,\boldsymbol{x}_n), W^{(n)}(\boldsymbol{y}_0,\ldots,\boldsymbol{y}_n)) \pmod{p^{n+1}}$$

(with $W^{(n)}$ as in Eq. (2.1)*) for some $\boldsymbol{f}_i \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}_0,\ldots,\boldsymbol{x}_i,\boldsymbol{y}_0,\ldots,\boldsymbol{y}_i]$, then $\boldsymbol{f}_i$ reduces to f_i modulo p.*

Proof. First, we observe that if $\boldsymbol{g}_i \equiv \boldsymbol{f}_i \pmod{p}$ for $i \in \{0,\ldots,n\}$, then $W^{(n)}(\boldsymbol{f}_0,\ldots,\boldsymbol{f}_n) \equiv W^{(n)}(\boldsymbol{g}_0,\ldots,\boldsymbol{g}_n) \pmod{p^{n+1}}$.

If $\boldsymbol{f} = \boldsymbol{a} = (a_0, a_1, \ldots) \in \boldsymbol{W}(\Bbbk)$, then the theorem is true by Eq. (2.11). Also, the theorem is clearly true for $\boldsymbol{f}$ equal to either $\boldsymbol{x}$ or $\boldsymbol{y}$. So, it suffices to show that if the theorem is true for $\boldsymbol{f}$ and $\boldsymbol{g}$, then it is also true for their sum and product. But these follow from Eqs. (2.2) and (2.3) respectively. □

Theorem 3.2 above allows us to compute the coordinates Greenberg transform recursively, generalizing Eqs. (2.2) and (2.3).

The algorithm described in [6] to compute the second and third coordinates of the canonical lifting of an ordinary elliptic curve starts by computing the Greenberg transform. But this requires a lot of computer power when the coefficients are left as unknowns, and that is exactly the problem we first encountered when trying to compute $J_2(X)$ for $p \geq 17$.

Observe, on the other hand, that Lemma 8.1 from [7], restated below as Proposition 4.5, allows us to compute the second coordinate of $\mathscr{G}(\boldsymbol{f})$ directly, without using sums and products of Witt vectors or the recursive method from Theorem 3.2. In fact, although simple in the case of the second coordinate, this was crucial to the proof of Theorem 1.3. Hence, we need to find an analogue for the the third coordinate. (This analogue is stated as Theorem 6.1 below.)

4. Auxiliary functions

In this section we introduce auxiliary functions that will be used to compute sums and products of Witt vectors. We will again let $\Bbbk$ be a perfect field of characteristic $p > 0$ and use the notation introduced in Definition 2.1.

We shall use also the following terminology:

Definition 4.1. We say that two polynomials f_1 and f_2 are *disjoint* if no monomial has non-zero multiples appearing in both f_1 and f_2. (In other words, if m is a monomial of f_1, there is no $\alpha \neq 0$ such that αm is a monomial of f_2, and vice-versa.)

Definition 4.2. Given $\boldsymbol{f} = \sum_{i,j} \boldsymbol{a}_{i,j} \boldsymbol{x}^i \boldsymbol{y}^j \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$ and a positive integer n, define

$$\boldsymbol{f}^{(p^n)} \stackrel{\text{def}}{=} \sum_{i,j} \boldsymbol{a}_{i,j}^{p^n} \boldsymbol{x}^{ip^n} \boldsymbol{y}^{jp^n}.$$

Note that if $\boldsymbol{f}$ and $\boldsymbol{g}$ are disjoint, then $(\boldsymbol{f} + \boldsymbol{g})^{(p^n)} = \boldsymbol{f}^{(p^n)} + \boldsymbol{g}^{(p^n)}$. For products we need stronger requirements. If $\boldsymbol{f}$, $\boldsymbol{g}$, and $\boldsymbol{f} \cdot \boldsymbol{g}$ have exactly m_1, m_2, and $m_1 m_2$ monomials of distinct degrees, then $(\boldsymbol{f} \cdot \boldsymbol{g})^{(p^n)} = \boldsymbol{f}^{(p^n)} \cdot \boldsymbol{g}^{(p^n)}$.

Definition 4.3. Given $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$, define

$$\psi_1(\boldsymbol{f}) \stackrel{\text{def}}{=} \pi \left(\frac{\boldsymbol{f}^{(p)} - \boldsymbol{f}^p}{p} \right).$$

Also, given $f \in \Bbbk[x_0, y_0]$, let $\boldsymbol{f}$ denote its Teichmüller lift. Then, we define $\psi_1(f) \stackrel{\text{def}}{=} \psi_1(\boldsymbol{f})$. We define ψ_1 in the analogous way for polynomials in more variables.

The function ψ_1 was introduced in Definition 2.6 of [7]. As observed there, one can easily compute $\psi_1(f)$ without having to lift it: if f is a single monomial, then $\psi_1(f) = 0$ and if $f = f_1 + f_2$, where f_1 and f_2 are disjoint, then one can easily check that

$$\psi_1(f) = \psi_1(f_1) + \psi_1(f_2) - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} f_1^i f_2^{p-i}. \tag{4.1}$$

In particular, we have that $\bar{S}_1 = X_1 + Y_1 + \psi_1(X_0 + Y_0)$.

This allows us to compute $\psi_1(f)$ recursively, and in trying to speed up the computation of ψ_1, one could try writing $f = f_1 + f_2$ where f_2 is a single monomial from f, which would give us $\psi_1(f_2) = 0$ in the equation above, and hence we would not need to compute this term. But in fact, the most efficient way is to actually split f as the sum of two polynomial with about half of its monomials each, as the powers that show up in the summation are taken from polynomials with less terms. Moreover, this approach allows the algorithm to use multiple processors in parallel, by sending $\psi_1(f_1)$ and $\psi_1(f_2)$ to different processors.

Note that we have to interpret formula (4.1) with care, as again we are in characteristic p, while it seems that we are dividing by p. But obviously, for $i = 1, \ldots, (p-1)$, we have that $\binom{p}{i}$ is divisible by p. To avoid any further confusion of this sort, we introduce some extra notation:

Definition 4.4. We define,

$$\mathrm{bin}_a(i) \stackrel{\text{def}}{=} \frac{1}{a} \binom{a}{i},$$

and (with p implicit)

$$\mathrm{w}_2(i) \overset{\text{def}}{=} \frac{i - i^p}{p}.$$

Finally, we write $\mathrm{bin}_p^{(2)}(i) \overset{\text{def}}{=} -\mathrm{w}_2(\mathrm{bin}_p(i))$.

Hence, for all $i \in \mathbb{Z}$ we have $\mathrm{w}_2(i) \in \mathbb{Z}$, and if p does not divide i, we also have $\mathrm{bin}_p(i), \mathrm{bin}_{p^2}(i), \mathrm{bin}_p^{(2)}(i) \in \mathbb{Z}$.

Besides allowing us to compute $\bar{S}_1$, the function ψ_1 also can be used to compute the second coordinate of the Greenberg transform without performing sums and products of Witt vectors. More precisely, Lemma 8.1 from [7] gives us:

Proposition 4.5. *Let*

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

and $f(x_0, y_0) \in \Bbbk[x_0, y_0]$ *be its reduction modulo* p. *Then, if* $\boldsymbol{a}_{i,j} = (a_{i,j,0}, a_{i,j,1})$, *we have that the second coordinate of the Greenberg transform of* $\boldsymbol{f}$ *is*

$$(f_{x_0})^p x_1 + (f_{y_0})^p y_1 + \sum_{i,j} a_{i,j,1}\, x_0^{ip} y_0^{jp} + \psi_1(f),$$

where f_{x_0} *and* f_{y_0} *denote the partial derivatives of* f.

As we shall see later, computing the Greenberg transform directly makes the process much more efficient and uses much less memory. So, the initial goal is to obtain a similar result for the third coordinate of the Greenberg transform.

We shall need a function ψ_2 similar to ψ_1, which we break down into a few auxiliary functions to simplify the exposition.

Definition 4.6. Let $f, f_1, f_2, \ldots \in \Bbbk[x_0, y_0]$ and $\boldsymbol{f}, \boldsymbol{f}_1, \boldsymbol{f}_2, \ldots \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$ be their respective Teichmüller lifts. (Also remember that π denotes the reduction modulo p.) Define:

(1)

$$\theta(f_1, f_2, i) \overset{\text{def}}{=} \theta(\boldsymbol{f}_1, \boldsymbol{f}_2, i) \overset{\text{def}}{=} \pi\left(\frac{\left(\boldsymbol{f}_1^{(p)}\right)^i \left(\boldsymbol{f}_2^{(p)}\right)^{p-i} - \boldsymbol{f}_1^{ip} \boldsymbol{f}_2^{p(p-i)}}{p}\right);$$

(2)

$$\mu(f) \overset{\text{def}}{=} \mu(\boldsymbol{f}) \overset{\text{def}}{=} \pi\left(\frac{\left(\boldsymbol{f}^{(p)}\right)^p - \boldsymbol{f}^{p^2}}{p^2}\right);$$

(3)
$$\lambda(f) \overset{\text{def}}{=} \lambda(\boldsymbol{f}) \overset{\text{def}}{=} \pi\left(\frac{1}{p}\left[\frac{\boldsymbol{f}^{(p^2)} - \left(\boldsymbol{f}^{(p)}\right)^p}{p} - \left(\frac{\boldsymbol{f}^{(p)} - \boldsymbol{f}^p}{p}\right)^p\right]\right);$$

(4)
$$\psi_2(f) \overset{\text{def}}{=} \mu(f) + \lambda(f).$$

(5) Define
$$\eta_1(f_1, f_2) \overset{\text{def}}{=} -\sum_{i=1}^{p-1} \operatorname{bin}_p(i) f_1^i f_2^{p-i}.$$
Inductively, define for $n \geq 3$,
$$\eta_1(f_1, \dots, f_n) \overset{\text{def}}{=} \eta_1(f_1, f_2 + \cdots + f_n) + \eta_1(f_2, \dots, f_n).$$
We shall also define $\eta_1(f) \overset{\text{def}}{=} 0$. (Note that
$$\eta_1(f_1, \dots, f_n) = \psi_1(X_1 + \cdots + X_n)|_{X_1=f_1,\dots,X_n=f_n},$$
where we compute $\psi_1(X_1 + \cdots + X_n)$ *before* evaluating X_i at f_i.)

(6) Finally, similarly to η_1, we define
$$\eta_2(f_1, \dots, f_n) \overset{\text{def}}{=} \psi_2(X_1 + \cdots + X_n)|_{X_1=f_1,\dots,X_n=f_n}.$$

One should observe that the p^i's appearing in the denominators above will not cause problems with the reductions modulo p, as one can easily verify that the corresponding numerators are congruent to zero modulo p^i. (This also follows from the recursive formulas in the next section.)

5. Computations in characteristic p

As we shall see in Theorem 6.1, the function ψ_2 appears in the computation of the third coordinate of the Greenberg transform of a polynomial. But, computing $\psi_2(f)$ by lifting f, as in the definition, can be quite demanding. Computations are greatly improved if one stays in characteristic p. We now show how we can compute $\mu(f)$, $\lambda(f)$, and $\psi_2(f)$ without having to lift f. The idea is the same as with ψ_1, i.e., to use a recursion based on the number of monomials.

Proposition 5.1. *Let $f \in \Bbbk[x_0, y_0]$. If f has a single monomial, then $\mu(f) = 0$. If f has two or more monomials, let $f = f_1 + f_2$, where f_1 and f_2 are disjoint. Then,*
$$\mu(f) = \mu(f_1) + \mu(f_2) - \sum_{\substack{i=1 \\ p\nmid i}}^{p^2-1} \operatorname{bin}_{p^2}(i) f_1^i f_2^{p^2-i} + \sum_{i=1}^{p-1} \operatorname{bin}_p(i)\theta(f_1, f_2, i).$$

Proof. Let $\boldsymbol{f}$, $\boldsymbol{f}_1$, and $\boldsymbol{f}_2$ be the Teichmüller lifts of f, f_1 and f_2 respectively. Then, observing that $\binom{p^2}{ip} \equiv \binom{p}{i} \pmod{p^3}$ (see, for instance, Theorem 1 of [2]) and $\boldsymbol{f}_1$ and $\boldsymbol{f}_2$ are disjoint, we have

$$\begin{aligned}
\frac{(\boldsymbol{f}^{(p)})^p - (\boldsymbol{f})^{p^2}}{p^2} &= \frac{(\boldsymbol{f}_1^{(p)} + \boldsymbol{f}_2^{(p)})^p - (\boldsymbol{f}_1 + \boldsymbol{f}_2)^{p^2}}{p^2} \\
&= \frac{(\boldsymbol{f}_1^{(p)})^p - \boldsymbol{f}_1^{p^2}}{p^2} + \frac{(\boldsymbol{f}_2^{(p)})^p - \boldsymbol{f}_2^{p^2}}{p^2} - \sum_{\substack{i=1\\ p\nmid i}}^{p^2-1} \frac{1}{p^2}\binom{p^2}{i} \boldsymbol{f}_1^i \boldsymbol{f}_2^{p^2-i} \\
&\quad + \frac{1}{p^2}\left[\sum_{i=1}^{p-1}\binom{p}{i}(\boldsymbol{f}_1^{(p)})^i(\boldsymbol{f}_2^{(p)})^{p-i} - \sum_{i=1}^{p-1}\binom{p^2}{ip}\boldsymbol{f}_1^{ip}\boldsymbol{f}_2^{p^2-ip}\right] \\
&\equiv \frac{(\boldsymbol{f}_1^{(p)})^p - \boldsymbol{f}_1^{p^2}}{p^2} + \frac{(\boldsymbol{f}_2^{(p)})^p - \boldsymbol{f}_2^{p^2}}{p^2} - \sum_{\substack{i=1\\ p\nmid i}}^{p^2-1} \frac{1}{p^2}\binom{p^2}{i} \boldsymbol{f}_1^i \boldsymbol{f}_2^{p^2-i} \\
&\quad + \sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\frac{(\boldsymbol{f}_1^{(p)})^i(\boldsymbol{f}_2^{(p)})^{p-i} - \boldsymbol{f}_1^{ip}\boldsymbol{f}_2^{p(p-i)}}{p} \pmod{p}.
\end{aligned}$$

Since all coefficients are integers, reducing the equation modulo p gives us the desired formula. □

Now, on to λ:

Proposition 5.2. *Let $f \in \Bbbk[x_0, y_0]$. If f has a single monomial, then $\lambda(f) = 0$. If f has two or more monomials, let $f = f_1 + f_2$, where f_1 and f_2 are disjoint. Also, let*

$$v \stackrel{\text{def}}{=} \left(-\operatorname{bin}_p(1) f_1 f_2^{p-1}, -\operatorname{bin}_p(2) f_1^2 f_2^{p-2}, \ldots, -\operatorname{bin}_p(p-1) f_1^{p-1} f_2\right).$$

Then,

$$\begin{aligned}
\lambda(f) = \lambda(f_1) + \lambda(f_2) + \eta_1(\psi_1(f_1), \psi_1(f_2)) + \eta_1(\psi_1(f_1) + \psi_1(f_2), \eta_1(f_1, f_2)) \\
+ \eta_1(v) + \sum_{i=1}^{p-1} \operatorname{bin}_p^{(2)}(i) f_1^{ip} f_2^{(p-i)p} - \sum_{i=1}^{p-1} \operatorname{bin}_p(i)\theta(f_1, f_2, i).
\end{aligned}$$

Proof. Let $\boldsymbol{f}$, $\boldsymbol{f}_1$, and $\boldsymbol{f}_2$ be the Teichmüller lifts of f, f_1 and f_2 respectively. Then,

$$
\begin{aligned}
&\frac{1}{p}\left[\frac{\boldsymbol{f}_1^{(p^2)}+\boldsymbol{f}_2^{(p^2)}-(\boldsymbol{f}_1^{(p)}+\boldsymbol{f}_2^{(p)})^p}{p}-\left(\frac{(\boldsymbol{f}_1^{(p)}+\boldsymbol{f}_2^{(p)})-(\boldsymbol{f}_1+\boldsymbol{f}_2)^p}{p}\right)^p\right]\\
&=\frac{1}{p}\left[\frac{\boldsymbol{f}_1^{(p^2)}-(\boldsymbol{f}_1^{(p)})^p}{p}+\frac{\boldsymbol{f}_2^{(p^2)}-(\boldsymbol{f}_2^{(p)})^p}{p}-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}(\boldsymbol{f}_1^{(p)})^i(\boldsymbol{f}_2^{(p)})^{p-i}\right.\\
&\qquad\left.-\left(\frac{\boldsymbol{f}_1^{(p)}-\boldsymbol{f}_1^p}{p}+\frac{\boldsymbol{f}_2^{(p)}-\boldsymbol{f}_2^p}{p}-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\boldsymbol{f}_1^i\boldsymbol{f}_2^{p-i}\right)^p\right]\\
&=\frac{1}{p}\left[\frac{\boldsymbol{f}_1^{(p^2)}-(\boldsymbol{f}_1^{(p)})^p}{p}+\frac{\boldsymbol{f}_2^{(p^2)}-(\boldsymbol{f}_2^{(p)})^p}{p}-\left(\frac{\boldsymbol{f}_1^{(p)}-\boldsymbol{f}_1^p}{p}+\frac{\boldsymbol{f}_2^{(p)}-\boldsymbol{f}_2^p}{p}\right)^p\right.\\
&\qquad\left.-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}(\boldsymbol{f}_1^{(p)})^i(\boldsymbol{f}_2^{(p)})^{p-i}-\left(-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\boldsymbol{f}_1^i\boldsymbol{f}_2^{p-i}\right)^p\right]\\
&\qquad-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\left(\frac{\boldsymbol{f}_1^{(p)}-\boldsymbol{f}_1^p}{p}+\frac{\boldsymbol{f}_2^{(p)}-\boldsymbol{f}_2^p}{p}\right)^i\left(-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\boldsymbol{f}_1^i\boldsymbol{f}_2^{p-i}\right)^{p-i}\\
&=\frac{1}{p}\left[\frac{\boldsymbol{f}_1^{(p^2)}-(\boldsymbol{f}_1^{(p)})^p}{p}-\left(\frac{\boldsymbol{f}_1^{(p)}-\boldsymbol{f}_1^p}{p}\right)^p+\frac{\boldsymbol{f}_2^{(p^2)}-(\boldsymbol{f}_2^{(p)})^p}{p}-\left(\frac{\boldsymbol{f}_2^{(p)}-\boldsymbol{f}_2^p}{p}\right)^p\right]\\
&\qquad+\frac{1}{p}\left[-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}(\boldsymbol{f}_1^{(p)})^i(\boldsymbol{f}_2^{(p)})^{p-i}-\left(-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\boldsymbol{f}_1^i\boldsymbol{f}_2^{p-i}\right)^p\right]\\
&\qquad-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\left(\frac{\boldsymbol{f}_1^{(p)}-\boldsymbol{f}_1^p}{p}\right)^i\left(\frac{\boldsymbol{f}_2^{(p)}-\boldsymbol{f}_2^p}{p}\right)^{p-i}\\
&\qquad-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\left(\frac{\boldsymbol{f}_1^{(p)}-\boldsymbol{f}_1^p}{p}+\frac{\boldsymbol{f}_2^{(p)}-\boldsymbol{f}_2^p}{p}\right)^i\left(-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\boldsymbol{f}_1^i\boldsymbol{f}_2^{p-i}\right)^{p-i}.
\end{aligned}
$$

Now, the first bracket clearly reduces to $\lambda(f_1)+\lambda(f_2)$, while the last two sums reduce to $\eta_1(\psi_1(f_1),\psi_1(f_2))$ and $\eta_1(\psi_1(f_1)+\psi_1(f_2),\eta_1(f_1,f_2))$.

Now,

$$\begin{aligned}
&\frac{1}{p}\left[-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}(\boldsymbol{f}_1^{(p)})^i(\boldsymbol{f}_2^{(p)})^{p-i} - \left(-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\boldsymbol{f}_1^i\boldsymbol{f}_2^{p-i}\right)^p\right]\\
&=\sum_{i=1}^{p-1}\frac{1}{p}\left[\left(\frac{1}{p}\binom{p}{i}\right)^p-\frac{1}{p}\binom{p}{i}\right](\boldsymbol{f}_1^{(p)})^i(\boldsymbol{f}_2^{(p)})^{p-i}\\
&\qquad+\frac{1}{p}\left[-\sum_{i=1}^{p-1}\left(\frac{1}{p}\binom{p}{i}\right)^p(\boldsymbol{f}_1^{(p)})^i(\boldsymbol{f}_2^{(p)})^{p-i} - \left(-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\boldsymbol{f}_1^i\boldsymbol{f}_2^{p-i}\right)^p\right].
\end{aligned}$$

The first term then clearly reduces to

$$\sum_{i=1}^{p-1}\mathrm{bin}_p^{(2)}(i)f_1^{ip}f_2^{(p-i)p}.$$

So, to finish the proof we need to show that the second term reduces to

$$\eta_1(v)-\sum_{i=1}^{p-1}\mathrm{bin}_p(i)\theta(f_1,f_2,i).$$

But, if $p\neq 2$,

$$\begin{aligned}
&\frac{1}{p}\left[-\sum_{i=1}^{p-1}\left(\frac{1}{p}\binom{p}{i}\right)^p(\boldsymbol{f}_1^{(p)})^i(\boldsymbol{f}_2^{(p)})^{p-i} - \left(-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\boldsymbol{f}_1^i\boldsymbol{f}_2^{p-i}\right)^p\right]\\
&=-\sum_{i=1}^{p-1}\left(\frac{1}{p}\binom{p}{i}\right)^p\frac{(\boldsymbol{f}_1^{(p)})^i(\boldsymbol{f}_2^{(p)})^{p-i}-\boldsymbol{f}_1^{pi}\boldsymbol{f}_2^{(p-i)p}}{p}\\
&\qquad+\frac{1}{p}\left[-\sum_{i=1}^{p-1}\left(\frac{1}{p}\binom{p}{i}\boldsymbol{f}_1^i\boldsymbol{f}_2^{p-i}\right)^p - \left(-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}\boldsymbol{f}_1^i\boldsymbol{f}_2^{p-i}\right)^p\right].
\end{aligned}$$

Reducing modulo p gives the desired result. For $p=2$, this term is zero, which yields the correct result in this case. □

The previous propositions give the following immediate corollary:

Corollary 5.3. *Let $f\in\Bbbk[x_0,y_0]$. If f has a single monomial, then $\psi_2(f)=0$. If f has two or more monomials, let $f=f_1+f_2$, where f_1 and f_2 are disjoint. Also, let*

$$v\overset{\text{def}}{=}\left(-\mathrm{bin}_p(1)f_1f_2^{p-1},-\mathrm{bin}_p(2)f_1^2f_2^{p-2},\dots,-\mathrm{bin}_p(p-1)f_1^{p-1}f_2\right).$$

Then,

$$\begin{aligned}\psi_2(f) = \psi_2(f_1) &+ \psi_2(f_2)\\ &+ \eta_1(\psi_1(f_1),\psi_1(f_2)) + \eta_1(\psi_1(f_1)+\psi_1(f_2),\eta_1(f_1,f_2)) + \eta_1(v)\\ &- \sum_{\substack{i=1\\ p\nmid i}}^{p^2-1} \mathrm{bin}_{p^2}(i) f_1^i f_2^{p^2-i} + \sum_{i=1}^{p-1} \mathrm{bin}_p^{(2)}(i) f_1^{ip} f_2^{(p-i)p}.\end{aligned}$$

One should observe that the optimal way to split f as f_1+f_2 in this case depends on the number of terms. Our experiments seem to indicate that if f has few elements, then it is faster to take f_1 as one of the monomials of f, as then $\psi_2(f_1)$ and $\eta_1(\psi_1(f_1),\psi_1(f_2))$ are both automatically zero. On the other hand, if f has many terms, it is better again to have f_1 and f_2 have roughly half as many terms as f.

Now, using η_1 and η_2, we can compute $\bar{S}_2$ and $\bar{P}_2$ directly in characteristic p:

Proposition 5.4. *Let $\bar{S}_i$ and $\bar{P}_i$ be the polynomials over $\mathbb{F}_p$ that give sum and product of Witt vectors in characteristic p (as in Eqs.* (2.6) *to* (2.9)*). We have:*

$$\bar{S}_1 = X_1 + Y_1 + \eta_1(X_0,Y_0), \tag{5.1}$$

$$\bar{P}_1 = X_1Y_0^p + X_0^pY_1, \tag{5.2}$$

and

$$\bar{S}_2 = X_2 + Y_2 + \eta_1(X_1,Y_1) + \eta_1(X_1+Y_1,\eta_1(X_0,Y_0)) + \eta_2(X_0,Y_0), \tag{5.3}$$

$$\bar{P}_2 = X_2Y_0^{p^2} + X_1^pY_1^p + X_0^{p^2}Y_2 + \eta_1(X_1Y_0^p, X_0^pY_1). \tag{5.4}$$

Proof. The first two formulas are immediate, observing that $\psi_1(X_0+Y_0) = \eta_1(X_0,Y_0)$. Also, the fourth formula follows from Eq. (2.9) and the definition of η_1.

To prove formula (5.3) we use formula (2.8). We shall consider

$$\frac{1}{p}\left(X_1^p + Y_1^p - \left(X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0+Y_0)^p}{p}\right)^p\right) + \frac{X_0^{p^2} + Y_0^{p^2} - (X_0+Y_0)^{p^2}}{p^2}$$

in characteristic 0 and show that it reduces modulo p to $\eta_1(X_1,Y_1) + \eta_1(X_1+Y_1,\eta_1(X_0,Y_0)) + \eta_2(X_0,Y_0)$. Since

$$\eta_1(X,Y) = -\sum_{i=1}^{p-1} \mathrm{bin}_p(i) X^iY^{p-i}$$

(also in characteristic 0), we have that the above expression can be simplified as:

$$\begin{aligned}
&\frac{1}{p}\left(X_1^p + Y_1^p - (X_1 + Y_1 + \eta_1(X_0, Y_0))^p\right) + \frac{X_0^{p^2} + Y_0^{p^2} - (X_0 + Y_0)^{p^2}}{p^2} \\
&= \frac{1}{p}\left(X_1^p + Y_1^p - (X_1 + Y_1)^p\right) + \eta_1\left(X_1 + Y_1, \eta_1(X_0, Y_0)\right) \\
&\quad + \frac{1}{p}\left(\frac{X_0^{p^2} + Y_0^{p^2} - (X_0 + Y_0)^{p^2}}{p} - \left(\frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}\right)^p\right) \\
&= \eta_1(X_1, Y_1) + \eta_1\left(X_1 + Y_1, \eta_1(X_0, Y_0)\right) \\
&\quad + \frac{1}{p}\left(\frac{X_0^{p^2} + Y_0^{p^2} - (X_0 + Y_0)^{p^2}}{p} - \frac{X_0^{p^2} + Y_0^{p^2} - (X_0^p + Y_0^p)^p}{p}\right) \\
&\quad + \frac{1}{p}\left(\frac{X_0^{p^2} + Y_0^{p^2} - (X_0^p + Y_0^p)^p}{p} - \left(\frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}\right)^p\right) \\
&= \eta_1(X_1, Y_1) + \eta_1\left(X_1 + Y_1, \eta_1(X_0, Y_0)\right) \\
&\quad + \frac{1}{p}\left(\frac{(X_0^p + Y_0^p)^p - (X_0 + Y_0)^{p^2}}{p}\right) \\
&\quad + \frac{1}{p}\left(\frac{X_0^{p^2} + Y_0^{p^2} - (X_0^p + Y_0^p)^p}{p} - \left(\frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}\right)^p\right),
\end{aligned}$$

which reduces to $\eta_1(X_1, Y_1) + \eta_1(X_1 + Y_1, \eta_1(X_0, Y_0)) + \mu(X_0 + Y_0) + \lambda(X_0 + Y_0)$, yielding the desired formula. □

It is worth mentioning that we also have

$$\begin{aligned}
\bar{P}_3 = {} & X_0^{p^3} Y_3 + X_1^{p^2} Y_2^p + X_2^p Y_1^{p^2} + X_3 Y_0^{p^3} \\
& + \eta_1(X_0^{p^2} Y_2, X_2 Y_0^{p^2}) + \eta_1(X_0^{p^2} Y_2 + X_2 Y_0^{p^2}, \eta_1(X_0^p Y_1, X_1 Y_0^p)) \\
& + \eta_1(X_0^{p^2} Y_2 + X_2 Y_0^{p^2} + \eta_1(X_0^p Y_1, X_1 Y_0^p), X_1^p Y_1^p) \\
& + \eta_2(X_0^p Y_1, X_1 Y_0^p).
\end{aligned} \tag{5.5}$$

The proof is not too hard if one realizes that many terms similar to Eq. (2.8) appear with X_0, Y_0, X_1, and Y_1 replaced by $X_0^p Y_1$, $X_1 Y_0^p$, $X_0^{p^2} Y_2$, and $X_2 Y_0^{p^2}$ respectively. Then, the same ideas that led Eq. (2.8) to Eq. (5.3), with only a small manipulation involved, give us Eq. (5.5). (The formula for $\bar{S}_3$ should be much more involved.)

6. The third coordinate of the Greenberg transform

We now give the formula for the third coordinate of the Greenberg transform of a polynomial.

Theorem 6.1. *Let $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$ be given by*

$$\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i,j} \boldsymbol{a}_{i,j} \boldsymbol{x}^i \boldsymbol{y}^j,$$

with partial derivatives with respect to $\boldsymbol{x}$ and $\boldsymbol{y}$

$$\boldsymbol{f}_{\boldsymbol{x}}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i,j} \boldsymbol{b}_{i,j} \boldsymbol{x}^i \boldsymbol{y}^j, \qquad \text{and} \qquad \boldsymbol{f}_{\boldsymbol{y}}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i,j} \boldsymbol{c}_{i,j} \boldsymbol{x}^i \boldsymbol{y}^j,$$

respectively. Also, let f be the reduction modulo p of $\boldsymbol{f}$ (and use subscripts x_0 and y_0 to denote its partial derivatives), and

$$\begin{aligned} \boldsymbol{a}_{i,j} &\equiv (a_{i,j,0}, a_{i,j,1}, a_{i,j,2}) \pmod{p^3}, \\ \boldsymbol{b}_{i,j} &\equiv (b_{i,j,0}, b_{i,j,1}, b_{i,j,2}) \pmod{p^3}, \\ \boldsymbol{c}_{i,j} &\equiv (c_{i,j,0}, c_{i,j,1}, c_{i,j,2}) \pmod{p^3}. \end{aligned}$$

Then, the third coordinate of the Greenberg transform of $\boldsymbol{f}$ is given by

$$\begin{aligned} (6.1) \quad & f_{x_0}^{p^2} x_2 + f_{y_0}^{p^2} y_2 + \left(\sum_{i,j} b_{i,j,1} x_0^{ip} y_0^{jp} \right)^p x_1^p + \left(\sum_{i,j} c_{i,j,1} x_0^{ip} y_0^{jp} \right)^p y_1^p \\ & + (f_{x_0x_0}/2)^{p^2} x_1^{2p} + f_{x_0y_0}^{p^2} x_1^p y_1^p + (f_{y_0y_0}/2)^{p^2} y_1^{2p} + \sum_{i,j} a_{i,j,2} x_0^{ip^2} y_0^{jp^2} \\ & + \psi_1 (f_{x_0}^p x_1 + f_{y_0}^p y_1 + \sum_{i,j} a_{i,j,1} x_0^{ip} y_0^{jp}) \\ & + \eta_1 (f_{x_0}^p x_1 + f_{y_0}^p y_1 + \sum_{i,j} a_{i,j,1} x_0^{ip} y_0^{jp}, \psi_1(f)) + \psi_2(f). \end{aligned}$$

Note that since for all $n \in \mathbb{Z}$ we have that

$$(6.2) \qquad n \equiv (n, \mathrm{w}_2(n)) \pmod{p^2},$$

(with w_2 as in Definition 4.4) we obtain

$$\begin{aligned} (6.3) \qquad b_{i,j,1} &= (i+1)^p a_{i+1,j,1} + \mathrm{w}_2(i+1) a_{i+1,j,0}^p, \\ c_{i,j,1} &= (j+1)^p a_{i,j+1,1} + \mathrm{w}_2(j+1) a_{i,j+1,0}^p. \end{aligned}$$

Also, observe that the formula does work for $p = 2$ if we interpret the division by 2 as an abuse of notation with the natural meaning, i.e, if we consider the terms $i(i-1)/2$ that appear in the second order derivatives as the reduction modulo 2 of this integer.

Proof of Theorem 6.1. Let $\boldsymbol{f}_0$ be the Teichmüller lift of f, $\boldsymbol{a}_{i,j,k}$, $\boldsymbol{b}_{i,j,k}$, and $\boldsymbol{c}_{i,j,k}$ be the Teichmüller lifts of $a_{i,j,k}$, $b_{i,j,k}$ and $c_{i,j,k}$ respectively, and

$$\begin{aligned}\boldsymbol{f}_1 \overset{\text{def}}{=} \left(\sum_{i,j} \boldsymbol{b}_{i,j,0}^p \boldsymbol{x}_0^{ip} \boldsymbol{y}_0^{jp}\right) \boldsymbol{x}_1 + \left(\sum_{i,j} \boldsymbol{c}_{i,j,0}^p \boldsymbol{x}_0^{ip} \boldsymbol{y}_0^{jp}\right) \boldsymbol{y}_1 \\ + \sum_{i,j} \boldsymbol{a}_{i,j,1} \boldsymbol{x}_0^{ip} \boldsymbol{y}_0^{jp} + \left(\frac{\boldsymbol{f}_0^{(p)} - \boldsymbol{f}_0^p}{p}\right).\end{aligned}$$

Hence, by Proposition 4.5, $\boldsymbol{f}_0$ and $\boldsymbol{f}_1$ reduce the first two coordinates of the Greenberg transform of $\boldsymbol{f}$.

Thus, by Theorem 3.2, it suffices to show that

$$\boldsymbol{f}_2 \overset{\text{def}}{=} \frac{1}{p^2} \left[\boldsymbol{f}^{\sigma^2}(\boldsymbol{x}_0^{p^2} + p\boldsymbol{x}_1^p + p^2\boldsymbol{x}_2, \boldsymbol{y}_0^{p^2} + p\boldsymbol{y}_1^p + p^2\boldsymbol{y}_2) - \boldsymbol{f}_0^{p^2} - p\boldsymbol{f}_1^p\right]$$

is in $\boldsymbol{W}(\mathbb{k})[\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_0, \boldsymbol{y}_1, \boldsymbol{y}_2]$ and reduces to Eq. (6.1) modulo p.

To simplify the notation, let $\boldsymbol{g} \overset{\text{def}}{=} \boldsymbol{f}^{\sigma^2}$. Then, using Taylor expansion, we obtain

$$\begin{aligned}\boldsymbol{g}(\boldsymbol{x}_0^{p^2} + p\boldsymbol{x}_1^p + p^2\boldsymbol{x}_2, \boldsymbol{y}_0^{p^2} + p\boldsymbol{y}_1^p + p^2\boldsymbol{y}_2) &\equiv \boldsymbol{g}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2}) \\ &+ \boldsymbol{g}_{\boldsymbol{x}_0}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2})(p\boldsymbol{x}_1^p + p^2\boldsymbol{x}_2) + \boldsymbol{g}_{\boldsymbol{y}_0}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2})(p\boldsymbol{y}_1^p + p^2\boldsymbol{y}_2) \\ &+ \frac{1}{2}\boldsymbol{g}_{\boldsymbol{x}_0\boldsymbol{x}_0}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2})(p\boldsymbol{x}_1^p)^2 + \boldsymbol{g}_{\boldsymbol{x}_0\boldsymbol{y}_0}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2})(p\boldsymbol{x}_1^p)(p\boldsymbol{y}_1^p) \\ &+ \frac{1}{2}\boldsymbol{g}_{\boldsymbol{y}_0\boldsymbol{y}_0}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2})(p\boldsymbol{y}_1^p)^2 \pmod{p^3}.\end{aligned}$$

By Eq. (2.11), $\boldsymbol{a}_{i,j} \equiv \boldsymbol{a}_{i,j,0} + p\boldsymbol{a}_{i,j,1}^{1/p} + p^2\boldsymbol{a}_{i,j,2}^{1/p^2} \pmod{p^3}$, and hence, $\sigma^2(\boldsymbol{a}_{i,j}) \equiv \boldsymbol{a}_{i,j,0}^{p^2} + p\boldsymbol{a}_{i,j,1}^p + p^2\boldsymbol{a}_{i,j,2} \pmod{p^3}$. Then, we have that

$$\begin{aligned}\boldsymbol{g}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2}) \equiv \boldsymbol{f}_0^{\sigma^2}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2}) + p\sum_{i,j} \boldsymbol{a}_{i,j,1}^p \boldsymbol{x}_0^{ip^2} \boldsymbol{y}_0^{jp^2} \\ + p^2\sum_{i,j} \boldsymbol{a}_{i,j,2} \boldsymbol{x}_0^{ip^2} \boldsymbol{y}_0^{jp^2} \pmod{p^3}.\end{aligned}$$

Now, since σ is a homomorphism which fixes $\mathbb{Z}$, we have that $(\boldsymbol{f}^{\sigma^2})_{\boldsymbol{x}_0} = (\boldsymbol{f}_{\boldsymbol{x}_0})^{\sigma^2}$ and $(\boldsymbol{f}^{\sigma^2})_{\boldsymbol{y}_0} = (\boldsymbol{f}_{\boldsymbol{y}_0})^{\sigma^2}$. Thus,

$$\boldsymbol{g}_{\boldsymbol{x}_0}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2}) \equiv \sum_{i,j} \boldsymbol{b}_{i,j,0}^{p^2} \boldsymbol{x}_0^{ip^2} \boldsymbol{y}_0^{jp^2} + p\sum_{i,j} \boldsymbol{b}_{i,j,1}^p \boldsymbol{x}_0^{ip^2} \boldsymbol{y}_0^{jp^2} \pmod{p^2}$$

and

$$\boldsymbol{g}_{\boldsymbol{y}_0}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2}) \equiv \sum_{i,j} \boldsymbol{c}_{i,j,0}^{p^2} \boldsymbol{x}_0^{ip^2} \boldsymbol{y}_0^{jp^2} + p\sum_{i,j} \boldsymbol{c}_{i,j,1}^p \boldsymbol{x}_0^{ip^2} \boldsymbol{y}_0^{jp^2} \pmod{p^2}.$$

Therefore,

$$
\begin{aligned}
(6.4)\qquad \boldsymbol{f}_2 \equiv{}& \frac{1}{p^2}\left[\boldsymbol{f}_0^{\sigma^2}(\boldsymbol{x}_0^{p^2},\boldsymbol{y}_0^{p^2}) - \boldsymbol{f}_0^{p^2}\right] \\
&+ \frac{1}{p}\left[\sum_{i,j}\boldsymbol{a}_{i,j,1}^{p}\boldsymbol{x}_0^{ip^2}\boldsymbol{y}_0^{jp^2} + \left(\sum_{i,j}\boldsymbol{b}_{i,j,0}^{p^2}\boldsymbol{x}_0^{ip^2}\boldsymbol{y}_0^{jp^2}\right)\boldsymbol{x}_1^{p}\right. \\
&\qquad\left. + \left(\sum_{i,j}\boldsymbol{c}_{i,j,0}^{p^2}\boldsymbol{x}_0^{ip^2}\boldsymbol{y}_0^{jp^2}\right)\boldsymbol{y}_1^{p} - \boldsymbol{f}_1^{p}\right] \\
&+ \sum_{i,j}\boldsymbol{a}_{i,j,2}\boldsymbol{x}_0^{ip^2}\boldsymbol{y}_0^{jp^2} + \left(\sum_{i,j}\boldsymbol{b}_{i,j,0}^{p^2}\boldsymbol{x}_0^{ip^2}\boldsymbol{y}_0^{jp^2}\right)\boldsymbol{x}_2 \\
&+ \left(\sum_{i,j}\boldsymbol{b}_{i,j,1}^{p}\boldsymbol{x}_0^{ip^2}\boldsymbol{y}_0^{jp^2}\right)\boldsymbol{x}_1^{p} + \left(\sum_{i,j}\boldsymbol{c}_{i,j,0}^{p^2}\boldsymbol{x}_0^{ip^2}\boldsymbol{y}_0^{jp^2}\right)\boldsymbol{y}_2 \\
&+ \left(\sum_{i,j}\boldsymbol{c}_{i,j,1}^{p}\boldsymbol{x}_0^{ip^2}\boldsymbol{y}_0^{jp^2}\right)\boldsymbol{y}_1^{p} + \frac{1}{2}\boldsymbol{g}_{\boldsymbol{x}_0\boldsymbol{x}_0}(\boldsymbol{x}_0^{p^2},\boldsymbol{y}_0^{p^2})\boldsymbol{x}_1^{2p} \\
&+ \boldsymbol{g}_{\boldsymbol{x}_0\boldsymbol{y}_0}(\boldsymbol{x}_0^{p^2},\boldsymbol{y}_0^{p^2})\boldsymbol{x}_1^{p}\boldsymbol{y}_1^{p} + \frac{1}{2}\boldsymbol{g}_{\boldsymbol{y}_0\boldsymbol{y}_0}(\boldsymbol{x}_0^{p^2},\boldsymbol{y}_0^{p^2})\boldsymbol{y}_1^{2p} \pmod{p},
\end{aligned}
$$

where the congruence sign means that the difference between the left hand and right hand sides is in $p\boldsymbol{W}(\Bbbk)[\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{y}_0,\boldsymbol{y}_1,\boldsymbol{y}_2]$. Now, clearly, the last three lines of Eq. (6.4) reduce modulo p to the first two lines of Eq. (6.1).

If, again to simplify notation, we let

$$
\boldsymbol{h} \overset{\text{def}}{=} \left(\sum_{i,j}\boldsymbol{b}_{i,j,0}^{p}\boldsymbol{x}_0^{ip}\boldsymbol{y}_0^{jp}\right)\boldsymbol{x}_1 + \left(\sum_{i,j}\boldsymbol{c}_{i,j,0}^{p}\boldsymbol{x}_0^{ip}\boldsymbol{y}_0^{jp}\right)\boldsymbol{y}_1 + \sum_{i,j}\boldsymbol{a}_{i,j,1}\boldsymbol{x}_0^{ip}\boldsymbol{y}_0^{jp},
$$

then we can rewrite the first two lines of the right hand side of Eq. (6.4) as

$$
\frac{\boldsymbol{f}_0^{(p^2)} - \boldsymbol{f}_0^{p^2}}{p^2} + \frac{1}{p}\left[\boldsymbol{h}^{(p)} - \left(\boldsymbol{h} + \left(\frac{\boldsymbol{f}_0^{(p)} - \boldsymbol{f}_0^{p}}{p}\right)\right)^{p}\right] =
$$

$$
\frac{\boldsymbol{f}_0^{(p^2)} - \boldsymbol{f}_0^{p^2}}{p^2} - \frac{1}{p}\left(\frac{\boldsymbol{f}_0^{(p)} - \boldsymbol{f}_0^{p}}{p}\right)^{p} + \frac{\boldsymbol{h}^{(p)} - \boldsymbol{h}^{p}}{p} - \sum_{i=1}^{p-1}\frac{1}{p}\binom{i}{p}\boldsymbol{h}^{i}\left(\frac{\boldsymbol{f}_0^{(p)} - \boldsymbol{f}_0^{p}}{p}\right)^{p-i}.
$$

Now, using Definition 4.6, it is clear that the expression above is in $\boldsymbol{W}(\Bbbk)[\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_0, \boldsymbol{y}_1, \boldsymbol{y}_2]$ and reduces to

$$\psi_2(f) + \psi_1(f_{x_0}^p x_1 + f_{y_0}^p y_1 + \sum_{i,j} a_{i,j,1} x_0^{ip} y_0^{jp}) \\ + \eta_1(f_{x_0}^p x_1 + f_{y_0}^p y_1 + \sum_{i,j} a_{i,j,1} x_0^{ip} y_0^{jp}, \psi_1(f))$$

modulo p, concluding the proof. □

7. Complexity analysis

We now give a brief analysis of the complexity of the new method to compute the Greenberg transform of a polynomial. Some explicit comparisons are made in Section 8.

The main difficulty here is that the complexity is based on the number of (non-zero) terms of the polynomial, and it is difficult to give precise bounds for this number after a few operations.

We will consider that the polynomials are stored as *sparse*, i.e., the zero terms are not stored and do not affect the number of operations. Furthermore, we will disregard the additions of the degrees of the variables when counting operations, i.e., the multiplication of two monomials will be counted as a single operation.

Then, if f_1 and f_2 are polynomials of n_1 and n_2 terms respectively, then the product $f_1 \cdot f_2$ requires $n_1 n_2$ products and $(n_1 n_2 - 1)$ sums, and so $\mathrm{O}(n_1 n_2)$ operations on the base ring. The largest possible number of terms for $f_1 \cdot f_2$ is $n_1 n_2$. In particular, for $k \in \mathbb{Z}_{>0}$, we have that f_1^k requires $\mathrm{O}(n_1^k)$ operations and has at most n_1^k terms. In fact, it is easy to prove that it will have necessarily less terms than that, but in the worst case scenario it would still have $\mathrm{O}(n_1^k)$ terms. On the other hand, if f_1 is a polynomial of degree $(n_1 - 1)$ *in one variable*, it would have at most $(kn_1 - k + 1)$ terms, which in general is considerably less than n_1^k.

We now look at the complexity of computing $\sum_{i=1}^{p-1} \mathrm{bin}_p(i) f_1^i f_2^{p-i}$. We need, in the worst case, $\mathrm{O}(n_i^{p-1})$ operations to compute the $f_i^2, \ldots, f_i^{p-1}$. Let's assume that $n_1 \leq n_2$. Then, we need at most $\mathrm{O}(n_1 n_2^{p-1})$ operations to compute the products $f_1^i f_2^{p-i}$, and p operations to sum, yielding $\mathrm{O}(n_1 n_2^{p-1})$ operations total.

Now, let $N_1(f)$ be the number of operations performed in computing $\psi_1(f)$, where f has n terms. Then, by Eq. (4.1), we have that $N_1(f) = N_1(f_1) + N_1(f_2) + \mathrm{O}(n_1 n_2^{p-1})$, where $f = f_1 + f_2$ and $n = n_1 + n_2$. (We shall keep this notation through out this section.) Although in practice it seems that it is best to take n_1 and n_2 as approximately $n/2$, the number of operations is always $\mathrm{O}(n^p)$. Of course, in this case the operations are in characteristic p, i.e., in $\Bbbk$. Observe that to compute $\psi_1(f)$ by lifting it (as in Definition 4.3) requires $\mathrm{O}(n^p)$ operations in (a ring of) characteristic p^2, i.e., in $\boldsymbol{W}_2(\Bbbk)$.

We now look at terms that appear in Corollary 5.3, so that we can then analyze $\psi_2(f)$. We start with $\eta_1(v)$. Let $v = (g_1, \dots, g_k)$ and assume that g_i has m_i monomials with $m_1 \leq m_2 \leq \cdots \leq m_k$, and let $m = m_1 + \cdots + m_k$. Now, partition the indices $\{1, \dots, k\}$ into two (disjoint) subsets and let h_1 and h_2 be the sums of the g_i's with respect to these two subsets. (Hence, $h_1 + h_2 = g_1 + \cdots + g_k$.) After possible reordering, we can assume $h_1 = g_1 + \cdots + g_r$ and $h_2 = g_{r+1} + \cdots + g_k$. Let l_i be the number of terms of h_i, and assume $l_1 \leq l_2$. In the worst case, we have that $l_1 + l_2 = m$. So, if $N_2(v)$ is the number of operations necessary to compute $\eta_1(v)$, then, since

$$\eta_1(v) = \eta_1(g_1, \dots, g_r) + \eta_1(g_{r+1}, \dots, g_k) + \eta_1(g_1 + \cdots + g_r, g_{r+1} + \cdots + g_k),$$

we have that $N_2(v) = N_2(g_1, \dots, g_r) + N_2(g_{r+1}, \dots, g_k) + \mathrm{O}(l_1 l_2^{p-1})$. As before, this gives us $\mathrm{O}(m^p)$ operations. Hence, if $k = (p-1)$ and $g_i = f_1^i f_2^{(p-i)}$, with f, n, f_i, and n_i as above, and if n_1 and n_2 are approximately $n/2$ again, then we have that $\eta_1(v)$ requires $\mathrm{O}(n^{p^2})$ operations.

Now, let $g_i \overset{\text{def}}{=} \psi_1(f_i)$, for $i = 1, 2$. As observed, we have that the number of terms of g_i, say m_i with $m_1 \leq m_2$, is $\mathrm{O}(n_i^p)$. So, $\eta_1(g_1, g_2)$ requires $\mathrm{O}(m_1 m_2^{p-1})$ operations. If n_1 and n_2 are again approximately $n/2$, we need at most $\mathrm{O}(n^{p^2})$ operations to compute $\eta_1(g_1, g_2)$.

To compute $\eta_1(g_1 + g_2, \eta_1(f_1, f_2))$, with the g_i's as above, we have that $g_1 + g_2$ and $\eta_1(f_1, f_2)$ will have $\mathrm{O}(n^p)$ terms, requiring then $\mathrm{O}(n^{p^2})$ operations.

Finally, computing

$$\sum_{\substack{i=1 \\ p \nmid i}}^{p^2-1} \mathrm{bin}_{p^2}(i) f_1^i f_2^{p^2-i} \qquad \text{and} \qquad \sum_{i=1}^{p-1} \mathrm{bin}_p^{(2)}(i) f_1^{ip} f_2^{(p-i)p}$$

require $\mathrm{O}(n^{p^2})$ and $\mathrm{O}(n^p)$ operations respectively. (Note that if f has n terms, computing f^p requires at most $\mathrm{O}(n(p-1))$, even without using successive squaring.) Hence, computing $\psi_2(f)$ requires $\mathrm{O}(n^{p^2})$ operations.

Thus, by Eq. (6.1), we have that computing the Greenberg transform of $\boldsymbol{f}$ when its reduction modulo p, say f, has n terms and $\boldsymbol{f}$ itself has less that n^p terms, takes $\mathrm{O}(n^{p^2})$ operations in $\Bbbk$. Computing using Eq. (6.4) takes $\mathrm{O}(n^{p^2})$ operations in $\boldsymbol{W}_3(\Bbbk)$.

8. Performance improvements

We show some concrete the improvements in processing and memory usage obtained from the results in the previous sections. All the tests were performed on a Dell Precision 690 server with two dual-core 64 bit 3.2

gigahertz Inter Xeon processors, 16 gigabytes of RAM, and 8 gigabytes of swap, running Fedora Core 11 (GNU/Linux) with kernel 2.6.30. Also, we used the softwares MAGMA (version 2.16-1) and Sage (version 4.3) in the tests. Most of the files used to run the tests described in here can be found, at the time of writing, at

`http://www.math.utk.edu/~finotti/comp/`.

Note that neither MAGMA nor Sage takes advantage of the four cores available when processing the computations (a single core is used), which could speed up the computations even further, as observed before. (It should be mentioned that those softwares might make it possible to use more than one core, but if so, the author is unfamiliar with the proper methods.)

We start by the computations of the polynomials S_1 and S_2 for various primes p. The computations of P_1 and P_2 are, relatively speaking, much faster, enough for them to be considered irrelevant in comparison. (While P_2 needs $\mathrm{O}(p)$ computations in either $\mathbb{F}_p$ or $\boldsymbol{W}_3(\mathbb{F}_p) \cong \mathbb{Z}/p^3\mathbb{Z}$, depending on the method used, S_2 needs $\mathrm{O}(p^p)$ computations over the same ring.) Tables 8.1 and 8.2 show the time and memory usage to compute these polynomials, in MAGMA and Sage respectively, in two different ways:

(1) Using formulas (2.6) and (2.8) to expand the $p \cdot S_1$ and $p^2 \cdot S_2$ in polynomial rings over $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p^3\mathbb{Z}$ respectively (instead of $\mathbb{Z}$), dividing the results by p and p^2 respectively, and finally reducing modulo p. The time taken in seconds is denoted by t_1 in Tables 8.1 and 8.2, while the memory usage in megabytes is denoted by m_1. (This method is already considerably more efficient than creating a ring of Witt vectors using MAGMA's built in function. Judging by the comparable times produced in tests, it seems that MAGMA performs the operations above over $\mathbb{Z}$.)

(2) Using Proposition 5.4 and computing η_1 and η_2 using recursion (as in Corollary 5.3). The time taken in seconds is denoted by t_2 in Tables 8.1 and 8.2, while the memory usage in megabytes is denoted by m_2.

As one can see, the first method is not very efficient in Sage, to the point that we did not bother in even computing many of the values of t_1 and m_1. On the other hand, one can see that Sage is more efficient with the second method.

In any event, Tables 8.1 and 8.2 show considerable improvements in both time and memory usage with the second method. Moreover, it should be observed that one can use Proposition 5.4 and the recursive computations of η_1 and η_2 to perform sums and products of Witt vectors without computing (and storing in memory) the potentially large polynomials S_i and P_i (for $i = 1, 2$). This also often yield considerable improvements when computing sums and products of Witt vectors over finite fields. As the fields get larger,

TABLE 8.1. Time and memory usage on computation of S_1 and S_2 in MAGMA.

char.	t_1 (sec)	t_2 (sec)	m_1 (MB)	m_2 (MB)
23	5.589	0.590	26.06	11.96
31	56.100	1.389	68.72	18.38
41	638.029	4.259	210.56	57.80
53	8560.129	14.160	545.75	81.75
71	−−	59.810	−−	240.28
101	−−	363.689	−−	964.91
151	−−	3010.380	−−	4810.53

TABLE 8.2. Time and memory usage on computation of S_1 and S_2 in Sage.

char.	t_1 (sec)	t_2 (sec)	m_1 (MB)	m_2 (MB)
23	211.64	0.57	53.16	4.0
31	3450.87	1.17	115.40	10.5
41	−−	2.99	−−	25.0
53	−−	8.54	−−	63.0
71	−−	31.53	−−	197.5
101	−−	170.04	−−	808.22
151	−−	1266.82	−−	4032.82

computing sums and products this way outperforms the traditional way of evaluating the polynomials S_i and P_i, even though both require $\mathrm{O}(p^2)$ operations in the finite field. For instance, in MAGMA, while over $\boldsymbol{W}(\mathbb{F}_{31^4})$ the recursive method computes sums in 0.280 seconds (on average), in this situation evaluating S_1 and S_2 computes sums in 0.083 seconds. But, for $\boldsymbol{W}(\mathbb{F}_{31^5})$ the recursive method computes (on average) sums in 0.359 seconds, while evaluating S_1 and S_2 computes sums in 5.090 seconds. In Sage the second method is already much more efficient over $\mathbb{F}_{31^4}$. It takes in average 1.600 seconds, while evaluation takes in average 192.681 seconds.

Note that those times do not take into account the extra time needed to compute S_1 and S_2, which will also use more memory. Tables 8.3 and 8.4 show average times to sum two vectors over a finite field using these two methods for some relatively large finite fields in MAGMA and Sage respectively. We computed the times using a few random elements (between 7 and 20, depending on the size of the field), but the individual times don't seem vary much at all from the average shown above.

As one can see, Sage is much less efficient than MAGMA, especially with the first method. But still, one can see a great improvement with the

Table 8.3. Average times to sum two Witt vectors of length 3 in MAGMA.

Field	evaluating S_1 and S_2	recursive method
$\mathbb{F}_{11^{15}}$	0.017 sec.	0.004 sec.
$\mathbb{F}_{13^7}$	0.125 sec.	0.014 sec.
$\mathbb{F}_{23^{10}}$	0.709 sec.	0.058 sec.
$\mathbb{F}_{43^4}$	3.475 sec.	0.847 sec.
$\mathbb{F}_{53^4}$	8.489 sec.	2.428 sec.
$\mathbb{F}_{61^4}$	15.413 sec.	5.055 sec.
$\mathbb{F}_{101^{20}}$	2027.190 sec.	85.779 sec.

Table 8.4. Average times to sum two Witt vectors of length 3 in Sage.

Field	evaluating S_1 and S_2	recursive method
$\mathbb{F}_{11^{15}}$	4.188 sec.	0.282 sec.
$\mathbb{F}_{13^7}$	5.192 sec.	0.271 sec.
$\mathbb{F}_{23^{10}}$	88.346 sec.	1.167 sec.
$\mathbb{F}_{43^4}$	782.754 sec.	3.111 sec.
$\mathbb{F}_{53^4}$	1959.466 sec.	4.953 sec.
$\mathbb{F}_{61^4}$	3509.918 sec.	6.992 sec.
$\mathbb{F}_{101^{20}}$	——	61.317 sec.

second method. (It seems that MAGMA is just much faster performing computations with finite fields, at least at the time of writing.)

Finally we look at computations of Greenberg transform of polynomials with coefficients in rings of Witt vectors over rational function fields, similarly to what is done when computing generic formulas for the canonical liftings. (As mentioned before, we computed J_i's initially using these general formulas.)

First, we consider a quadratic polynomial

$$\boldsymbol{x}^2 + (a_0, a_1, a_2)\boldsymbol{x} + (b_0, b_1, b_2)$$

over $\boldsymbol{W}(\mathbb{F}_p(a_0, a_1, a_2, b_0, b_1, b_2))$, where the a_i's and b_i's are taken to be algebraically independent transcendental elements over $\mathbb{F}_p$. We computed the Greenberg transform in three different ways:

(1) computing S_i and P_i (with the faster method described above) for $i = 1, 2$, and expanding the expression;

(2) computing sums and products of Witt vectors using recursions, as done above;

(3) using the formula given by Theorem 6.1.

TABLE 8.5. Time and memory usage on the computation of the Greenberg transform of quadratic polynomial in MAGMA.

char.	t_1 (sec)	t_2 (sec)	t_3 (sec)	m_1 (MB)	m_2 (MB)	m_3 (MB)
7	0.420	0.410	0.360	11.57	11.28	10.31
11	9.730	4.570	1.909	130.62	107.69	36.38
13	39.929	20.800	7.730	520.12	383.88	94.28
17	758.480	262.910	74.620	4647.69	3032.72	529.75
19	−−	988.269	187.659	−−	7208.94	1124.44
23	−−	−−	1086.250	−−	−−	4185.97

TABLE 8.6. Time and memory usage on the computation of the Greenberg transform of quadratic polynomial in Sage.

char.	t_1 (sec)	t_2 (sec)	t_3 (sec)	m_1 (MB)	m_2 (MB)	m_3 (MB)
7	0.89	0.31	0.29	4.82	5.32	4.32
11	117.84	7.96	1.22	50.32	70.82	27.32
13	833.49	40.47	3.64	153.32	217.82	78.32
17	15559.63	668.95	49.43	922.63	1354.32	458.82
19	−−	2092.06	142.43	−−	2907.32	976.32
23	−−	−−	633.81	−−	−−	3570.12

Tables 8.5 and 8.6 shows the time taken in seconds and memory usage in megabytes for different p in MAGMA and Sage, respectively, with these three different methods. These are denoted by t_1, t_2, and t_3, and m_1, m_2, and m_3 respectively.

Also, one can see that although MAGMA is more efficient with respect to time with the first two methods, Sage is more efficient with the third (and best) method. (It is also more efficient with respect to memory in all tests.)

Note that for $p = 23$, the third coordinate of the Greenberg transform is a polynomial in nine variables, namely the x_i's, a_i's, and b_i's, and has 65553940 terms.

As a second example, we look at the case of a cubic:

$$\boldsymbol{x}^3 + (a_0, a_1, a_2)\boldsymbol{x}^2 + (b_0, b_1, b_2)\boldsymbol{x} + (c_0, c_1, c_2)$$

over $\boldsymbol{W}(\mathbb{F}_p(a_0, a_1, a_2, b_0, b_1, b_2, c_0, c_1, c_2))$. Tables 8.7 and 8.8 show the times and memory usage obtained when using the same three methods described above with MAGMA and Sage, respectively.

It is also worth observing that $t_1 > t_2 > t_3$ in MAGMA and Sage in all cases, with some significant improvement. But while in MAGMA we always have $m_1 > m_2 > m_3$, with Sage we have that $m_2 > m_1 > m_3$.

Table 8.7. Time and memory usage on the computation of the Greenberg transform of cubic polynomial in MAGMA.

char.	t_1 (sec)	t_2 (sec)	t_3 (sec)	m_1 (MB)	m_2 (MB)	m_3 (MB)
5	0.420	0.410	0.370	11.53	13.6	10.62
7	5.490	4.150	1.810	94.12	90.50	44.44
11	2517.389	987.440	240.849	8380.22	7209.50	2110.59
13	−−	−−	2579.769	−−	−−	10516.19

Table 8.8. Time and memory usage on the computation of the Greenberg transform of cubic polynomial in Sage.

char.	t_1 (sec)	t_2 (sec)	t_3 (sec)	m_1 (MB)	m_2 (MB)	m_3 (MB)
5	0.50	0.32	0.29	5.82	6.82	4.82
7	27.48	6.69	1.30	65.82	72.82	33.82
11	10265.87	2211.73	196.01	3566.32	4999.32	1721.82
13	−−	−−	1368.54	−−	−−	8416.57

Note that the third coordinate of the Greenberg transform is a polynomial in twelve variables with 153065983 terms!

9. The function J_2

Finally, we return to the question about the nature of J_2. We shall use the same ideas that gave us Theorem 1.3 to find a simplified formula for J_2 which also allows us to compute it in an efficient way. More precisely:

Theorem 9.1. *Let $\Phi_p(X,Y) \in \mathbb{Z}[X,Y]$ be the modular polynomial and suppose that over $\boldsymbol{W}_3(\mathbb{F}_p)$ we have*

$$\Phi_p = \sum_{i,j} \boldsymbol{a}_{i,j} X^i Y^j, \quad (\Phi_p)_X = \sum_{i,j} \boldsymbol{b}_{i,j} X^i Y^j, \quad \text{and} \quad (\Phi_p)_Y = \sum_{i,j} \boldsymbol{c}_{i,j} X^i Y^j,$$

respectively, with $\boldsymbol{a}_{i,j} = (a_{i,j,0}, a_{i,j,1}, \ldots)$, $\boldsymbol{b}_{i,j} = (b_{i,j,0}, b_{i,j,1}, \ldots)$, $\boldsymbol{c}_{i,j} = (c_{i,j,0}, c_{i,j,1}, \ldots)$. Also, let $f(X_0, Y_0)$ denote the reduction modulo p of Φ_p and

$$g(X_0, Y_0, Y_1) \stackrel{\text{def}}{=} \psi_1((Y_0^p - X_0)^p Y_1 + \sum_{i,j} a_{i,j,1} X_0^{ip} Y_0^{jp}).$$

Then, $g(X, X^p, J_1(X)^p)$ is a p-power and

$$J_2(X) = \frac{-1}{(X^{p^2}-X)^p}\left[\left(\sum_{i,j} b_{i,j,1}X^{ip+jp^2}\right)J_1(X) + \left(\sum_{i,j} c_{i,j,1}X^{ip+jp^2}\right)J_1(X)^p - J_1(X)^{p+1} + \sum_{i,j} a_{i,j,2}X^{ip+jp^2} + g(X,X^p,J_1(X)^p)^{1/p}\right]. \tag{9.1}$$

(Note that when computing g, we first expand $\psi_1((Y_0^p - X_0)^pY_1 + \sum a_{i,j,1}X_0^{ip}Y_0^{jp})$, and then evaluate it, instead of first evaluating $(Y_0^p - X_0)^pY_1 + \sum a_{i,j,1}X_0^{ip}Y_0^{jp}$ and then computing ψ_1.)

Proof. By Theorem 3 of [16], we have that

$$\Phi_p((J_0, J_1, \ldots), (J_0^p, J_1^p, \ldots)) = 0. \tag{9.2}$$

Also, Kronecker's congruence relation tells us that $f = (X_0 - Y_0^p)(X_0^p - Y_0)$.

As observed in [10], this gives us that $\psi_1(f)$ when evaluated at (j_0, j_0^p) yields zero. In a similar way, we also have that $\psi_2(f)$ is zero when evaluated at (j_0, j_0^p). Indeed, we have that the Teichmüller lift of f is $\boldsymbol{f} \overset{\text{def}}{=} (X - Y^p)(X^p - Y)$. Note that $\boldsymbol{f}^{(p)} = (X^p - Y^{p^2})(X^{p^2} - Y^p)$, and let $(X^{p^2} - Y^p) = (X^p - Y)\cdot\boldsymbol{g}$. Then, $\mu(f)$ is the reduction modulo p of

$$\frac{(X^p - Y^{p^2})^p(X^{p^2} - Y^p)^p - (X - Y^p)^{p^2}(X^p - Y)^{p^2}}{p^2} = (X^p - Y)\frac{(X^p - Y^{p^2})^p(X^p - Y)^{p-1}\boldsymbol{g}^p - (X - Y^p)^{p^2}(X^p - Y)^{p^2-1}}{p^2},$$

and hence $\mu(f)(j_0, j_0^p) = 0$. In a similar manner it is easy to show that $\lambda(f)(j_0, j_0^p) = 0$, and hence $\psi_2(f)(j_0, j_0^p) = 0$.

This already reasonably simplifies to computations of J_2, as the last two terms of Eq. (6.1) in the case of $\boldsymbol{f} = \Phi_p$, which are the most demanding in terms of computer power, are irrelevant to the computation of J_2, and hence can be dropped.

Moreover, note that $f_{X_0} = (X_0^p - Y_0)$ and $f_{Y_0} = (Y_0^p - X_0)$, and so the term

$$\psi_1(f_{X_0}^p X_1 + f_{Y_0}^p Y_1 + \sum_{i,j} a_{i,j,1}X_0^{ip}Y_0^{jp})$$

in Eq. (6.1) gives us

$$\psi_1((X_0^p - Y_0)^pX_1 + (Y_0^p - X_0)^pY_1 + \sum_{i,j} a_{i,j,1}X_0^{ip}Y_0^{jp}).$$

Letting $f_1 \overset{\text{def}}{=} (X_0^p - Y_0)^p X_1$ and $f_2 \overset{\text{def}}{=} (Y_0^p - X_0)^p Y_1 + \sum_{i,j} a_{i,j,1} X_0^{ip} Y_0^{jp}$, Eq. (4.1) gives that $\psi_1(f_1 + f_2)(j_0, j_0^p) = \psi_1(f_2)(j_0, j_0^p)$, as f_1 and f_2 are disjoint and $\psi_1(f_1)(j_0, j_0^p) = 0$ (which can be seen with a computation in characteristic zero similar to the one above), which also somewhat simplifies the computation of J_2. So, applying Theorem 6.1 with $\boldsymbol{f} = \Phi_p$, we have:

$$\begin{aligned} (9.3) \qquad J_2(X)^p = \frac{-1}{(X^{p^2} - X)^{p^2}} \Bigg[\left(\sum_{i,j} b_{i,j,1} X^{ip+jp^2} \right)^p J_1(X)^p \\ + \left(\sum_{i,j} c_{i,j,1} X^{ip+jp^2} \right)^p J_1(X)^{p^2} - J_1(X)^{p+p^2} \\ + \sum_{i,j} a_{i,j,2} X^{ip^2+jp^3} + g(X, X^p, J_1(X)^p) \Bigg], \end{aligned}$$

with $g(X_0, Y_0, Y_1)$ as in the statement.

Observe that since $J_2(X) \in \mathbb{F}_p(X)$, we must have that $g(X, X^p, J_1^p)$ is a p-th power in $\mathbb{F}_p(X)$, and the theorem follows. □

Remark 9.2. It should be observed that when using Theorem 9.1 to compute J_2, the only demanding piece is the computation of $g(X, X^p, J_1(X)^p)$ (assuming we have Φ_p).

To make the computation more efficient, it is better to avoid first computing $g(X_0, Y_0, Y_1)$ and then evaluating the result at (X, X^p, J_1^p), and instead evaluate at (X, X^p, J_1^p) as we perform the necessary recursion. More precisely, define $\tilde{\psi}_1(f(X_0, Y_0, Y_1)) \overset{\text{def}}{=} 0$ if f is a monomial, and if $f = f_1 + f_2$, where f_1 and f_2 are disjoint, then define

$$\tilde{\psi}_1(f) = \tilde{\psi}_1(f_1) + \tilde{\psi}_1(f_2) - \sum_{i=1}^{p} \text{bin}_p(i) f_1(X, X^p, J_1^p)^i f_2(X, X^p, J_1^p)^{p-i}.$$

This gives us

$$g(X, X^p, J_1^p) = \tilde{\psi}_1((Y_0^p - X_0)^p Y_1 + \sum_{i,j} a_{i,j,1} X_0^{ip} Y_0^{jp}),$$

and since this computation essentially uses rational functions on one variable, it is much more efficient than computing $g(X_0, Y_0, Y_1)$ and then evaluate it at (X, X^p, J_1^p).

With this method we were able to compute $J_2(X)$ for $p \leq 37$. The results can be found at `http://www.math.utk.edu/~finotti/can_lifts/`. The formulas allowed us to obtain the following conjecture:

Conjecture 9.3. *Let $p \geq 5$ and*

$$S_p(X) \overset{\text{def}}{=} \frac{\mathrm{ss}_p(X)}{X^\delta (X-1728)^\epsilon},$$

where $\mathrm{ss}_p(X)$ *is the* supersingular polynomial *(as in, for instance,* [9]*),*

$$\delta \overset{\text{def}}{=} \begin{cases} 0, & \text{if } p \equiv 1 \pmod 4; \\ 1, & \text{if } p \equiv 3 \pmod 4, \end{cases} \quad \text{and} \quad \epsilon \overset{\text{def}}{=} \begin{cases} 0, & \text{if } p \equiv 1 \pmod 6; \\ 1, & \text{if } p \equiv 5 \pmod 6. \end{cases}$$

(Hence, $S_p(X) \in \mathbb{F}_p[X]$, and $S_p(0), S_p(1728) \neq 0$. See, for instance, [9]*.) Then,*

$$J_2(X) = \frac{F(X)}{(X-1728)^{p\delta} S_p(X)^{2p+1}}, \tag{9.4}$$

where $F(X) \in \mathbb{F}_p[X]$ and satisfies the following conditions:

1. $(F(X), (X-1728)^\delta S_p(X)) = 1$*;*
2. *$F(X)$ has a zero of order $(2\lfloor (p-1)/6 \rfloor + 1)p$ at $X = 0$.*

(A lower bound of the order of zero at $X = 0$ of F and an upper bound for its degree is given in Theorem 9.6 below.)

Although not as precise as the conjecture, a few results on $J_2(X)$ can be derived from Eq. (9.1). It should be observed that the main difficulty in proving the conjecture lies on obtaining information on the term $\sum a_{i,j,2} X^{ip+jp^2}$ from Eq. (9.1). In fact, the results on $\sum a_{i,j,1} X^{i+jp}$ (which is in fact equal to $\bar{H}_p(X)$) from Kaneko and Zagier in [13], obtained by analytic methods, allowed us to prove Theorems 1.2 and 1.3. (In [10] a different proof, more computational and algebraic in nature, is also given.) We do have the following:

Proposition 9.4. *Let $p \geq 5$, v_p denote the valuation at p, $\Phi_p(X,Y) = \sum \boldsymbol{a}_{i,j} X^i Y^j$ be the modular polynomial, $r \overset{\text{def}}{=} \lfloor (2p+1)/3 \rfloor$, and $s \overset{\text{def}}{=} (2\lfloor (p-1)/6 \rfloor + 1)$. Then:*

1. *If $p \equiv 1 \pmod 6$, then $\boldsymbol{a}_{0,0} = \boldsymbol{a}_{1,0} = 0$.*
2. *$\boldsymbol{a}_{0,i}, \boldsymbol{a}_{i,0} \equiv 0 \pmod{p^2}$ for $i \in \{0, \dots, r\}$. In particular, with the notation of Theorem 9.1, we have that $a_{i,0,1} = a_{0,i,1} = 0$ for $i \in \{0, \dots, r\}$, $b_{i,0,1} = c_{0,i,1} = 0$ for $i \in \{0, \dots, r-1\}$.*
3. *$v_p(\boldsymbol{a}_{i,0}) \geq 3$ for $i \in 0, \dots, s$, i.e., $a_{i,0,2} = 0$ for $i \in \{0, \dots, s\}$.*

Before proving the first item of the Proposition, we need to introduce a little notation. Let K be a quadratic imaginary field, $z_0 \in K$ with imaginary part positive, $\Gamma \overset{\text{def}}{=} \mathbb{Z} + z_0\mathbb{Z}$, and $\mathcal{O} \overset{\text{def}}{=} \{\alpha \in K \ : \ \alpha\Gamma \subseteq \Gamma\}$. We say that $\alpha \in \mathcal{O}$ is *primitive* if $\alpha \notin n\mathcal{O}$ for any $n \in \mathbb{Z}_{\geq 2}$. We say that $\alpha, \beta \in \mathcal{O}$ are *equivalent* if $\alpha/\beta \in \mathcal{O}^\times$. Then, here is Theorem 10.11 of [15]:

Theorem 9.5 (Kronecker)**.** *Let z_0, Γ, and $\mathcal{O}$ be as above, and $j(z)$ be the modular function. Then, the multiplicity of $j(z_0)$ as a root of $\Phi_m(X, X)$ is equal to the number of primitive $\mathcal{O}$-equivalence classes of $\alpha \in \mathcal{O}$ such that $\mathrm{N}(\alpha) = m$.*

Proof of Proposition 9.4. We start with item 1. Since $p \equiv 1 \pmod 6$, we have that 0 is ordinary. (This is well known. See, for instance, [9].) Then, since in this case the canonical lifting of the elliptic curve given by $j_0 = 0$ is the curve with $\boldsymbol{j} = 0 = (0, 0, \ldots)$, we have that $0 = \Phi_p((0, 0, \ldots), (0^p, 0^p, \ldots))$ $= \Phi_p(0, 0) = \boldsymbol{a}_{0,0}$. Hence, $0 = j(\rho)$, where $\rho \overset{\text{def}}{=} \mathrm{e}^{2\pi\mathrm{i}/3}$, is a root of $\Phi_p(X, X)$.

Since $\Phi_p(X, X) = \boldsymbol{a}_{0,0} + 2\boldsymbol{a}_{1,0}X + \cdots$, where the omitted terms have degree greater than one, it suffices to show now that 0 is zero of order at least two.

We will apply Theorem 9.5 with $z_0 = \rho$, $K = \mathbb{Q}[\rho]$, and $m = p$. In this case, we have $\mathcal{O} = \mathcal{O}_K = \mathbb{Z}[\rho]$, where $\mathcal{O}_K$ is the ring of integers of K. Indeed, we always have that $\mathcal{O} \subseteq \mathcal{O}_K$, and clearly in this case $\Gamma = \mathcal{O}_K$. Also, since we are taking $m = p$ prime, any $\alpha \in \mathcal{O}$ such that $\mathrm{N}(\alpha) = p$ is automatically primitive.

Since, $j(\rho) = 0$ is a root of $\Phi_p(X, X)$, there exists $\alpha \in \mathcal{O}$ such that $\mathrm{N}(\alpha) = p$. Then, clearly $\mathrm{N}(\bar{\alpha}) = p$. So, by Theorem 9.5, it suffices to show that $\alpha/\bar{\alpha} \notin \mathcal{O} = \mathbb{Z}[\rho]$.

Let $\alpha = a + b\rho$, with $a, b \in \mathbb{Z}$. Then

$$\frac{\alpha}{\bar{\alpha}} = \frac{\alpha^2}{p} = \frac{(a^2 - b^2)}{p} + \frac{b(2a + b)}{p}\rho.$$

A simple elementary analysis shows then that if $\alpha/\bar{\alpha} \in \mathbb{Z}[\rho]$, then $a, b \equiv 0 \pmod p$, which is a contradiction.

We now look at item 2. This is basically a corollary of Theorems 1.2 and 1.3. (In fact, this can be deduced directly from the results of [13].)

First, we have that Kronecker's congruence relation tells us that $\boldsymbol{a}_{i,0}$, $\boldsymbol{a}_{0,i} \equiv 0 \pmod p$ for $i \in \{0, \ldots, p\}$. Now, observe that by Theorems 1.2 and 1.3 we have that $\bar{H}_p(X)$ has a zero at $X = 0$ of order $(r + 1)$. Thus, since $(r + 1) < p$, we obtain

$$H_p(X) = \frac{1}{p}\Phi_p(X, X^p) = \frac{\boldsymbol{a}_{0,0}}{p} + \frac{\boldsymbol{a}_{1,0}}{p}X + \cdots + \frac{\boldsymbol{a}_{r+1,0}}{p}X^{r+1} + \cdots,$$

where all omitted terms have degrees larger than $(r+1)$. Therefore, we must then have that $a_{i,0} \equiv 0 \pmod{p^2}$ for $i \in \{0, \ldots, r\}$, and by the symmetry of Φ_p, we also have that $a_{0,i} \equiv 0 \pmod{p^2}$ for $i \in \{0, \ldots, r\}$. The second part of this item then follows immediately.

We now prove item 3. This result was conjectured by the author and the following proof was then given by A. V. Sutherland. The idea is to work with the third roots of the j-invariants, as proposed by Atkin, which yields the much simpler polynomial, which we shall denote by $\Psi_p(X,Y)$, and satisfies $\Psi_p(j^{1/3},(j')^{1/3}) = 0$ if the elliptic curves associated to j and j' have an isogeny of degree p. (See, for instance, [5]. The notation used in this reference for Ψ_p is $\Phi_p^{(3)}$, but we shall avoid it to not cause any confusion with Definition 4.2.)

This polynomial also satisfies:

$$\Phi_p(X^3,Y^3) = \Psi_p(X,Y)\Psi_p(X,\omega Y)\Psi_p(X,\omega^2 Y), \tag{9.5}$$

where $\omega \overset{\text{def}}{=} \mathrm{e}^{2\pi \mathrm{i}/3}$. (This is Eq. (23) of [5].) This clearly implies that

$$\Phi_p(X^3,0) = (\Psi_p(X,0))^3 \tag{9.6}$$

and, by Kronecker's relation,

$$\Psi_p(X,0) \equiv X^{p+1} \pmod p \tag{9.7}$$

(as $\Phi_p(X,0) \equiv X^{p+1} \pmod p$). Then, Eq. (9.7) implies that all coefficients of $\Psi_p(X,0)$ are divisible by p, except for the coefficient of X^{p+1}. Thus, by Eq. (9.6), we have that $v_p(\boldsymbol{a}_{i,0}) \geq 3$ for all $i < (p+1)/3$. This suffices for the proof in the case of $p \equiv 2 \pmod 3$.

If $p \equiv 1 \pmod 3$, then we have that $\boldsymbol{a}_{0,0} = \boldsymbol{a}_{0,1} = 0$ by item 1. Then, Eq. (9.6) implies that the coefficients of degree less than or equal to one of $\Psi_p(X,0)$ must also be equal to zero. This implies that the term of degree $(p+2)/3$ of $\Phi_p(X,0)$ must also be divisible by p^3, which finishes the proof. □

With Proposition 9.4, we can now prove the main theorem of this section:

Theorem 9.6. *Let $p \geq 5$ and*

$$J_2(X) = F(X)/G(X), \qquad \text{with } F,G \in \mathbb{F}_p[X] \text{ and } (F,G) = 1,$$

$S_p(X)$ as in Conjecture 9.3, and suppose that the modular polynomial is given by $\Phi_p(X,Y) = \sum \boldsymbol{a}_{i,j}X^iY^j$. We have:

(1)
$$\deg F - \deg G = \begin{cases} p^2-2, & \text{if } p = 31, \\ p^2-1, & \text{if } p \neq 31. \end{cases}$$

(2) *F (and hence J_2) has a zero at 0 of order greater than or equal to sp, where $s \overset{\text{def}}{=} (2\lfloor (p-1)/6 \rfloor + 1)$. In particular, if $0 \notin \Bbbk^{\text{ord}}$, then it yields a pseudo-canonical lifting modulo p^3 with j-invariant $(0,0,0)$.*

(3) *$G(X) = S_p(X)^{2p+1}G_1(X)$, where $G_1(X) \mid (X-1728)^{\delta p}$ (with δ as in Conjecture 9.3). (Hence G is known if $\delta = 0$, i.e., if $p \equiv 1 \pmod 4$).*

(4)

$$\deg F \leq \begin{cases} p^2 - 2 + (2p+1)\deg S_p(X) + p\delta, & \textit{if } p = 31, \\ p^2 - 1 + (2p+1)\deg S_p(X) + p\delta, & \textit{if } p \neq 31. \end{cases}$$

(Note that $\deg S_p(X) = \lfloor (p-1)/4 \rfloor - \lceil (p-1)/6 \rceil$. *See, for instance,* [9]*.)*

Proof. All items follow from the proper analysis Eq. (9.1), which we reproduce here for quicker reference:

$$\begin{aligned} J_2(X) = \frac{-1}{(X^{p^2} - X)^p} \Bigg[& \left(\sum_{i,j} b_{i,j,1} X^{ip+jp^2} \right) J_1(X) \\ & + \left(\sum_{i,j} c_{i,j,1} X^{ip+jp^2} \right) J_1(X)^p - J_1(X)^{p+1} \\ & + \sum_{i,j} a_{i,j,2} X^{ip+jp^2} + g(X, X^p, J_1(X)^p)^{1/p} \Bigg]. \end{aligned}$$

To prove item 1, it suffices to show that the order of the pole of J_2 at infinity is either $p^2 - 1$ or $p^2 - 2$, which shall be done my checking the order of poles of the terms of Eq. (9.1).

We know from Theorem 1.3 that $J_1(X) = \bar{H}_p(X)/(X^{p^2} - X)$. Assume that $p \neq 31$, i.e., that p doesn't divide 744. As observed in [3], we then have that $\deg \bar{H}_p = p^2 + p - 1$, and hence J_1 has a pole of order $p - 1$ at infinity in this case.

Also, one can easily deduced from the degrees that appear in Φ_p that

$$\deg(\Phi_p)_X(X, X^p) \leq p^2 + p - 1 \qquad \text{and} \qquad \deg(\Phi_p)_Y(X, X^p) \leq p^2,$$

and hence the polynomials

$$\sum_{i,j} b_{i,j,1} X^{ip+jp^2} \qquad \text{and} \qquad \sum_{i,j} c_{i,j,1} X^{ip+jp^2}$$

from Eq. (9.1) have degrees less than or equal to $p^3 + p^2 - p$ and p^3 respectively. In the same way we see that

$$\deg \left(\sum_{i,j} a_{i,j,2} X^{ip^2+jp^3} \right) \leq p^4 + p^3.$$

On the other hand, since

$$\Phi_p(X, Y) = X^{p+1} + Y^{p+1} - X^p Y^p + \cdots \tag{9.8}$$

(for instance, use Theorem 5.3 of [15] together with Kronecker's congruence relation) we have that $a_{p,p,2} = a_{0,p+1,2} = 0$, and hence $\deg(\sum a_{i,j,2} X^{ip^2+jp^3}) \leq p^4 + p^3 - p^2$.

Moreover, Eq. (9.8) gives us that the coefficient of $X^{p-1}Y^p$ in $(\Phi_p)_X$ is $-p \equiv (0,-1) \pmod{p^2}$, and thus we have that $\deg(\sum b_{i,j,1}X^{ip+jp^2}) = p^3+p^2-p$.

Finally, observe that the order of the pole of $g(X, X^p, J_1^p)$ is strictly less than the order of the pole of

$$[(X^{p^2}-X)^pJ_1^p + \sum_{i,j} a_{i,j,1}X^{ip+jp^2}]^p = [(X^{p^2}-X)^pJ_1^p + (\bar{H}_p(X))^p]^p.$$

With these observations on the degrees (and order of poles) of the terms of Eq. (9.1), one can see that if $p \neq 31$, then the order of the pole of J_2 is indeed p^2-1.

The case $p = 31$ follows from the same analysis observing only that the order of the pole of J_1 in this case is $p-2$.

For item 2, we look at the order of the zeros of the terms in Eq. (9.1) at $X = 0$.

We have, by item 2 of Proposition 9.4, that the term $\sum c_{i,j,1}X^{ip+jp^2}$ in Eq. (9.1) has zero of order at least p, $\sum b_{i,j,1}X^{ip+jp^2}$ has a zero of order at least rp, and $\sum a_{i,j,2}X^{ip+jp^2}$ has a zero of order at least $(s+1)p$.

We now look at the term $g(X, X^p, J_1^p)$. Using the recursion of $\tilde{\psi}_1$ (as in Remark 9.2), we have

$$\begin{aligned} g(X, X^p, J_1^p) &= \tilde{\psi}_1((Y_0^p - X_0)^pY_1 + \sum a_{i,j,1}X_0^{ip}Y_0^{jp}) \\ &= J_1^{p^2}\,\tilde{\psi}_1(Y_0^{p^2} - X_0^p) + \tilde{\psi}_1\left(\sum a_{i,j,1}X_0^{ip}Y_0^{jp}\right) \\ &\quad - \sum_{t=1}^{p-1} \mathrm{bin}_p(t)(J_1^p(X^{p^3}-X^p))^t\bar{H}_p(X^p)^{p-t}. \end{aligned}$$

Clearly, by Theorems 1.2 and 1.3, the first and last summand have zeros of order at least rp^2 and $(r+1)p^2$ respectively. For the second summand, since $a_{0,0,1} = \cdots = a_{r,0,1} = 0$ (by item 2 of Proposition 9.4), we obtain

$$\begin{aligned} \tilde{\psi}_1\left(\sum a_{i,j,1}X_0^{ip}Y_0^{jp}\right) &= X^{p^3}\tilde{\psi}_1\left(\sum_{j\geq 1} a_{i,j,1}X_0^{ip}Y_0^{(j-1)p}\right) \\ &\quad + X^{(r+1)p^2}\tilde{\psi}_1\left(\sum_{i\geq r+1} a_{i,0,1}X_0^{(i-r-1)p}\right) \\ &\quad - X^{(r+1)p^2}\sum_{t=1}^{p-1}\mathrm{bin}_p(t)X^{pt(p-r-1)}\left(\sum_{j\geq 1} a_{i,j,1}X^{ip+(j-1)p^2}\right)^t \\ &\qquad \times \left(\sum_{i\geq r+1} a_{i,0,1}X^{(i-r-1)p}\right)^{p-t}. \end{aligned}$$

Thus, this term has a zero of order at least $(r+1)p^2$, and we have that $g(X, X^p, J_1^p)$ has a zero of order greater than rp^2.

Hence, since $\sum a_{i,j,2} X^{ip+jp^2}$ has a zero of order at least $(s+1)p$, and $s < (r-1)$, by Eq. (9.1) we have that J_2 has a zero of order at least sp, which finishes the proof of item 2.

We now prove item 3. By the nature of J_2, we know that J_2 is regular at all ordinary values of j_0. Hence, the zeros of G, which correspond to poles of J_2, have to be among the supersingular values.

Now, by Theorems 1.2 and 1.3, we can write $J_1(X) = F_1(X)/S_p(X)$, with $F_1 \in \mathbb{F}_p[X]$ and $(F_1, S_p) = 1$. Using then Eq. (9.1), we obtain that $G(X) \mid (X^{p^2} - X)^p \cdot S_p(X)^{p+1}$. But since G has only supersingular values as its zeros, we obtain that $G \mid \mathrm{ss}_p^p \cdot S_p^{p+1} = X^{\epsilon p}(X-1728)^{\delta p} \cdot S_p^{2p+1}$. (Remember that $\mathrm{ss}_p \mid (X^{p^2} - X)$. See , for instance Theorem V.3.1 of [18].)

To show that $S_p^{2p+1} \mid G$, it suffices to show that if $S_p(\alpha) = 0$, then α is a pole of order $2p+1$ of J_2. But this follows again from Eq. (9.1), as the term J_1^{p+1} has a pole of order $p+1$ at such α, while all other terms inside the brackets have poles of smaller order.

Finally, since by item 2 we have that $X \nmid G$, the result follows.

Item 4 now follows immediately from items 1 and 3. □

Note that the proof of item 2 allows us to reformulate the second item of Conjecture 9.3 in the following way:

Conjecture 9.7. *With the notation of Proposition 9.4, we have that* $v_p(a_{s+1,0}) = 2$.

The pattern from this conjecture was observed by the author using the formulas for the modular polynomials $\Phi_p(X, Y)$ for $p \leq 353$ computed by M. Rubinstein, which are available at

`http://www.math.uwaterloo.ca/~mrubinst/modularpolynomials/phi_l.html`

Later, A. V. Sutherland, using methods from [1], was able to verify it for $p < 2500$. (He also observed that his methods would actually allow him go much further.)

In conclusion, regarding pseudo-canonical liftings, Theorem 9.6 above gives us:

(1) $J_2(X)$ always has a zero of order at least $(2\lfloor (p-1)/6 \rfloor + 1)$ at $X = 0$ (even if $0 \notin \Bbbk^{\mathrm{ord}}$) and $(0, J_1(0), J_2(0)) \equiv 0 \pmod{p^3}$, i.e., 0 always yields pseudo-canonical liftings modulo p^3.

(2) If $j_0 \notin \Bbbk^{\mathrm{ord}} \cup \{0, 1728\}$, then $J_2(X)$ has a pole at $X = j_0$ of order $2p+1$.

Also, Conjecture 9.3 states that if $1728 \notin \Bbbk^{\mathrm{ord}}$, then $J_2(X)$ has a pole of order p at $X = 1728$, and hence there would be no pseudo-canonical lifting modulo p^3 in this case.

10. Pseudo-canonical liftings modulo p^4

As seen in the previous section, unlike what happens to J_1, we have that J_2 has poles at $X = 1728$ whenever this value is supersingular, at least for $p \leq 37$ (or in general if Conjecture 9.3 is true). In the language of [10], this says that a pseudo-canonical can possibly exist only for $j_0 = 0$. But the failure of $j_0 = 1728$ to yield these pseudo-canonical liftings strengthens any suspicion that $j_0 = 0$ (when supersingular) will also eventually fail to yield pseudo-canonical liftings, i.e., that J_n will have a pole at $j_0 = 0$ for some n large enough.

Although computations modulo p^4 are mostly beyond our reach at this point (except for Eq. (5.5)), Conjecture 9.7 seems to indicate $j_0 = 0$ will already yield poles for J_3. In fact, we have the following conjecture:

Conjecture 10.1. *If* $0 \notin \Bbbk^{\mathrm{ord}}$, *then* $J_3(X)$ *has a pole of order* p^2 *at* $X = 0$.

Although we do not have the equivalent formulas as the ones given by Theorems 6.1 and 9.6, it seems it would be likely that we would have an equation analogous to Eq. (9.3), i.e., J_3^p will be a quotient of a term involving J_1, J_2, $\sum b_{i,j,2} X^{ip^2+jp^3}$, $\sum c_{i,j,2} X^{ip^2+jp^3}$, etc., and the crucial term $\sum_{i,j} a_{i,j,3} X^{ip^3+jp^4}$, divided by $(X^{p^2} - X)^{p^3}$. More precisely, we expect to have something like:

$$
\begin{aligned}
J_3(X)^p = \frac{-1}{(X^{p^2} - X)^{p^3}} \Bigg[& \left(\sum_{i,j} b_{i,j,2} X^{ip^2+jp^3} \right)^p J_1(X)^{p^2} \\
& + \left(\sum_{i,j} c_{i,j,2} X^{ip^2+jp^3} \right)^{p^2} J_1(X)^{p^3} + \left(\sum_{i,j} b_{i,j,1} X^{ip+jp^2} \right)^{p^2} J_2(X)^p \\
& + \left(\sum_{i,j} c_{i,j,1} X^{ip+jp^2} \right)^{p^2} J_2(X)^{p^2} + \sum_{i,j} a_{i,j,3} X^{ip^3+jp^4} + \cdots \Bigg],
\end{aligned} \tag{10.1}
$$

where the omitted terms can get quite complicated. But, if Conjecture 9.7 holds, then all explicit terms inside the brackets above, expect for $\sum_{i,j} a_{i,j,3} X^{ip^3+jp^4}$, have zeros of order high enough at $X = 0$, while the latter does *not* have a zero. We also believe that the omitted terms will have zeros of order greater than p^3, and hence we would have a pole if, and only if, $a_{0,0,3} \neq 0$, and in this case, which is predicted by Conjecture 9.7, we would have a pole of order p^2.

This assumption that the omitted terms above would have zeros of order greater than p^3 is indeed quite a leap, but it is reinforced by the fact that when we know $j_0 = 0$ is ordinary (i.e., $p \equiv 1 \pmod 6$), and hence J_i is regular at $X = 0$ for all i, we have, by item 1 of Proposition 9.4, that $a_{0,0}$ and $a_{1,0}$ both to be zero. This is relevant as it tells us that $\sum a_{i,j,k} X^{ip^k + jp^{k+1}}$, $\sum b_{i,j,k} X^{ip^k + jp^{k+1}}$, $\sum c_{i,j,k} X^{ip^k + jp^{k+1}}$ will always yield zeros at $X = 0$, and hence this seems to be a necessary condition to not have a pole.

We could confirm that this is indeed the case when $p = 5$, the only case we were able to compute J_3 directly from the modular polynomial. The formula is also available at

`http://www.math.utk.edu/~finotti/can_lifts/`.

In any event, we have to admit that we have much less evidence for Conjecture 10.1.

Acknowledgement. The author would like to thank A. V. Sutherland for his invaluable contribution, W. M. Miyata for the help with a Python script to read Rubinstein's modular polynomials which were stored as compressed binary files, and the *Centre de Recherches Mathématique* for its hospitality during the final stages of the writing.

References

[1] R. Broker, K. Lauter, and A. V. Sutherland, *Modular polynomials via isogeny volcanoes.* Available at `http://arxiv.org/abs/1001.0402v1`, 2010.

[2] K. Davis and W. Webb, *A binomial coefficient congruence modulo prime powers.* J. Number Theory **43(1)** (1993), 20–23.

[3] E. de Shalit, *Kronecker's polynomial, supersingular elliptic curves, and p-adic periods of modular curves.* In p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), volume **165** of Contemp. Math., pages 135–148. Amer. Math. Soc., Providence, RI, 1994.

[4] M. Deuring, *Die typen der multiplikatorenringe elliptischer funktionenköper.* Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272.

[5] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues.* In Computational perspectives on number theory (Chicago, IL, 1995), volume **7** of AMS/IP Stud. Adv. Math., pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

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

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

[8] L. R. A. Finotti, *Minimal degree liftings in characteristic 2.* J. Pure Appl. Algebra, 207(3):631–673, 2006.

[9] L. R. A. Finotti, *A formula for the supersingular polynomial.* Acta Arith. **139(3)** (2009), 265–273.

[10] L. R. A. Finotti, *Lifting the j-invariant: Questions of Mazur and Tate.* J. Number Theory **130(3)** (2010), 620 – 638.

[11] M. J. Greenberg, *Schemata over local rings.* Ann. of Math. (2) **73** (1961), 624–648.

[12] N. Jacobson, *Basic Algebra*, volume 2. W. H. Freeman and Company, second edition, 1984.

[13] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials.* In Computational perspectives on number theory (Chicago, IL,

1995), volume **7** of AMS/IP Stud. Adv. Math., pages 97–126. Amer. Math. Soc., Providence, RI, 1998.

[14] S. Lang, *On quasi algebraic closure.* Ann. of Math. (2) **55** (1952), 373–390.

[15] S. Lang, *Elliptic Functions.* Volume **112** of Garduate Texts in Mathematics, Springer-Verlag, second edition, 1986.

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

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

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

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

Luís R. A. Finotti
Department of Mathematics
University of Tennessee
Knoxville, TN 37996, USA
E-mail: `finotti@math.utk.edu`
URL: `http://www.math.utk.edu/~finotti/`