COMPUTATIONS WITH WITT VECTORS AND THE GREENBERG TRANSFORM

LUÍS R. A. FINOTTI

ABSTRACT. In this paper we give formulas for the coordinates of the Greenberg transform of a polynomial over rings of Witt vectors. Besides being of independent theoretical interest, these formulas can be used to obtain improvement on computations with Witt vectors of arbitrary length in cases where these cannot be reduced to computation on well known local rings.

Preliminary Version
Last revised: April 20, 2011.

1. Introduction

Computations with Witt vectors can be quite demanding, as the polynomials that define the sum and product of Witt vectors are themselves often enormous. (We review some basic facts about Witt vectors in Section 2.) In some cases one can perform computations efficiently by identifying the ring of Witt vectors with a well known ring. This is the case, for example, for Witt vectors over finite fields, in which case the ring of Witt vectors is canonically isomorphic to an unramified extension of p-adic integers $\mathbb{Z}_p$.

Unfortunately, in most other cases we lack this canonical isomorphism and need to resort to the defining polynomial equations to perform operations. One such case is when one is interested in computing the Greenberg transform of a polynomial. (See Section 3.) For instance, [Fin02] gives an algorithm that uses the Greenberg transform to compute canonical liftings (and the elliptic Teichmüller lift) of elliptic curves. (Notably, it does not use the modular polynomial.) Also, in [Fin10b] and [Fin10a] the Greenberg transform is used to obtain information about the coordinates of the j-invariant of canonical liftings as functions on ordinary j-invariants. (Some details on this can be found in Section 9.)

In fact, in [Fin10a] we give a precise formula for the first three coordinates of the Greenberg transform of a polynomial, making computations with Witt vectors of length at most 3 much more efficient. In particular, it makes it unnecessary to compute the potentially

2000 *Mathematics Subject Classification.* Primary 11Y16; Secondary 11S05.

Key words and phrases. Witt vectors, Greenberg transform, computations.

immense polynomials that define sums and products of Witt vectors in order to evaluate a polynomial at a Witt vector.

The main goal of this paper is to generalize those results for Witt vectors of arbitrary length. It should be said upfront that even though this goal is attained and some great improvement over older methods are obtained, as we show in Section 9, computations can still be quite demanding for large length.

But, the author's main motivation was the generalization of his previous results from [Fin10b] and [Fin10a], which deal with question's by B. Mazur and J. Tate on the coordinate function of the j-invariant of the canonical lifting of an ordinary elliptic curve. (See Section 9.) Some of these generalization were obtained in [Fin10c] by using the results of this paper.

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 [Ser79] or [Jac84]. 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

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

(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 $\boldsymbol{a} = (a_0, a_1, \dots)$ and $\boldsymbol{b} = (b_0, b_1, \dots)$, by

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

and

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

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.

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! One way to make the computation of such polynomials more efficient is to perform most of the computations directly in characteristic p, i.e., to compute $\bar{S}_n$ and $\bar{P}_n$ without computing S_n and P_n by means of Eqs. (2.4) and (2.5). (See Section 7.)

More generally, one can even avoid computing $\bar{S}_n$ and $\bar{P}_n$ altogether by using the Greenberg transform to perform a series of computations with Witt vectors. Computing its coordinates almost entirely in characteristic p also yields considerable improvements on calculations. (See Section 6.)

Another way in which we can improve computations with Witt vectors is to avoid *expanding unnecessary powers*: if one wants to evaluate the polynomial $(X + Y)^{100}$ at (a, b)

with a computer, it is better to first add $a+b$ and then take the 100-th power rather than ask the computer to expand the power, store the resulting polynomial, and then evaluate it at (a,b). This saves memory and computations. It is hard to avoid expanding unnecessary powers when dealing with Eqs. (2.4) and (2.5) though, as we need to expand powers to clear the denominators. But, by using some auxiliary functions (defined in Section 5), we are able to avoid expanding some of them.

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 [Ser79]) 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. (2.6) and (2.7) below), we need to define some notation:

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 *Teichmüller 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) 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.)

(4) 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

$$\boldsymbol{a} = \sum_{k=0}^{\infty} \xi_k(\boldsymbol{a}) p^k = (\pi(\xi_0(\boldsymbol{a})), \pi(\xi_1(\boldsymbol{a}))^p, \pi(\xi_2(\boldsymbol{a}))^{p^2}, \ldots) \tag{2.6}$$

and

$$(a_0, a_1, \ldots) = \sum_{k=0}^{\infty} \tau(a_k)^{1/p^k} p^k. \tag{2.7}$$

(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 [Lan52] and [Gre61].) 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 $\boldsymbol{x}_0 = (x_0, x_1, \ldots), \boldsymbol{y}_0 = (y_0, y_1, \ldots) \in \boldsymbol{W}(\Bbbk[x_0, y_0, x_1, y_1, \ldots])$, then $\boldsymbol{f}(\boldsymbol{x}_0, \boldsymbol{y}_0) = (f_0, f_1, \ldots) \in \boldsymbol{W}(\Bbbk[x_0, y_0, x_1, y_1, \ldots])$ (in fact, $f_n \in \Bbbk[x_0, \ldots, x_n, y_0, \ldots, y_n]$) is 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 f_n of $\mathscr{G}(\boldsymbol{f})$.

It is clear from the definition that there is a bijection between $\boldsymbol{C}(\boldsymbol{W}(\Bbbk))$ and $\mathscr{G}(\boldsymbol{C})(\Bbbk)$, as $\boldsymbol{f}(\boldsymbol{a}, \boldsymbol{b}) = \boldsymbol{0}$ if and only if $f_n(a_0, \ldots, a_n, b_0, \ldots, b_n) = 0$ for all n. 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, proved in Section 3 of [Fin10a].

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*

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

(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.

Theorem 3.2 above allows us to compute the coordinates Greenberg transform recursively, generalizing Eqs. (2.2) and (2.3). More precisely, let $\boldsymbol{f}_0 = \boldsymbol{f}$, and recursively define

$$\boldsymbol{f}_n = \frac{1}{p^n}\left[\boldsymbol{f}^{\sigma^n}(W^{(n)}(\boldsymbol{x}_0, \dots, \boldsymbol{x}_n), W^{(n)}(\boldsymbol{y}_0, \dots, \boldsymbol{y}_n)) - \boldsymbol{f}_0^{p^n}\right] - \sum_{i=1}^{n-1} \frac{1}{p^{n-i}} \boldsymbol{f}_i^{p^{n-i}}. \tag{3.2}$$

Then, f_n is the reduction modulo p of $\boldsymbol{f}_n$.

One of our main goals here is to describe how one can compute the Greenberg transform, i.e., the f_n's, more efficiently. In particular, how to do it mostly in characteristic p. In [Fin10a] this was accomplished for the first three coordinates. In Section 6 we generalize the result to all coordinates.

Note that a formula for the Greenberg transform allows us to evaluate any polynomial in two variables at a pair of Witt vectors directly, without having to perform the sums and products or even needing to compute the polynomials that give the sum and product. This makes computations considerably more efficient. See [Fin10a] for some comparison for length 3 and Section 9 for larger length.

4. Motivation

Although a formula for the Greenberg transform, as well as the improvement in concrete calculations that it yields, should be of independent interest, in this section we describe the problem that motivated the author to obtain a general formula for the Greenberg transform.

Given an ordinary elliptic curve $E/\Bbbk$ (with $\mathrm{char}(\Bbbk) = p > 0$, as above), there is a unique elliptic curve (up to isomorphism), say $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$, which reduces to E modulo p and for which we can lift the Frobenius. $\boldsymbol{E}$ is then called the *canonical lifting* of E. (See, for instance, [Deu41] or [LST64].) 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 $\Bbbk^{ord}$ denotes the set of ordinary values of j-invariants in $\Bbbk$, then we have functions $J_i : \Bbbk^{ord} \to \Bbbk$, for $i = 1, 2, 3, \dots$, such that the j-invariant of the canonical lifting of an elliptic curve with j-invariant $j_0 \in \Bbbk^{ord}$ is $(j_0, J_1(j_0), J_2(j_0), \dots)$.

B. Mazur asked about the nature of these functions J_i and J. Tate asked about the possibility of extending them to supersingular values.

It was proved in [Fin10b] that the functions J_i are rational functions over $\mathbb{F}_p$. Tate's question motivates the following definition:

Definition 4.1. Suppose that $j_0 \notin \Bbbk^{ord}$ 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 $(j_0, J_1(j_0), J_2(j_0), \ldots)$ 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 by the same formulas. On the other hand, we've proved that pseudo-canonical liftings modulo p^2 and p^3 do exist for specific supersingular values. More precisely, we've studied J_1 and J_2 in detail in [Fin10b] (using many results from [KZ98]) and [Fin10a] respectively, proving the following:

Theorem 4.2. *With the notation above and $p \geq 5$:*

1. *$J_1(X)$ is* always *regular at $X = 0$ and $X = 1728$, even when those values are supersingular, and $(0, J_1(0)) \equiv 0 \pmod{p^2}$ and $(1728, J_1(1728)) \equiv 1728 \pmod{p^2}$.*
2. *If $j_0 \notin \Bbbk^{ord} \cup \{0, 1728\}$, then J_1 has a simple pole at j_0.*
3. *$J_2(X)$ is* always *regular at $X = 0$, even if 0 is supersingular, and $(0, J_1(0), J_2(0)) \equiv 0 \pmod{p^3}$.*
4. *If $j_0 \notin \Bbbk^{ord} \cup \{0, 1728\}$, then J_2 has a pole of order $2p + 1$ at j_0.*

In fact, more precise descriptions of J_1 and J_2 are given. All these results were proved using the formulas for the second and third coordinates of the Greenberg transform. Of course, the next natural question is to ask about what happens for $J_3(X)$, i.e., can we give a precise description and find what are its poles? To use the same ideas of the proofs for J_1 and J_2, one then needs the third coordinate of the Greenberg transform.

Moreover, initially to even get some examples of J_3 for different characteristics (to obtain a conjecture, for instance) was nearly impossible due to how much memory and processing power computations with Witt vectors of length 4 over polynomial rings require. In fact, the only example we were able to compute with 24 gigabytes of memory (and using MAGMA) was for $p = 5$. So, this motivated the author to also try to improve computations with Witt vectors of length 4 or larger, as done for length 3 in [Fin10a] by means of the formula for the third coordinate of the Greenberg transform.

The applications of the results of this paper to these questions of Mazur and Tate are dealt with elsewhere. (See [Fin10c].) But with the formula for the third coordinate for the Greenberg transform, we were able to prove, for instance, that J_2 has a pole at 1728 if $1728 \notin \Bbbk^{ord}$ and J_3 has a pole at 0 if $0 \notin \Bbbk^{ord}$, and therefore pseudo-canonical liftings do not exist modulo power greater than p^3, giving a final answer to Tate's question. Also, with regard to Mazur's question, the third coordinate of the Greenberg transform allows us to give a precise description of J_3.

5. Auxiliary Functions

As observed before, we are interested in computing the reductions $\bar{S}_n$ and $\bar{P}_n$ of S_n and P_n directly in characteristic p, or, more generally, we would like to compute the reductions f_n of $\boldsymbol{f}_n$ from Theorem 3.2 directly in characteristic p. In order to do that, we need a way to deal with the divisions by powers of p that appear in their recursive definitions, namely Eqs. (2.4), (2.5), and (3.2). We now introduce some auxiliary functions which will deal with this problem.

Definition 5.1. Let p be a prime. Define $\eta_0(X_1, \ldots, X_r) \overset{\text{def}}{=} X_1 + \cdots + X_r \in \mathbb{Q}[X_1, \ldots, X_r]$, and recursively for $k \geq 1$

$$\eta_k(X_1, \ldots, X_r) \overset{\text{def}}{=} \frac{X_1^{p^k} + \cdots + X_r^{p^k}}{p^k} - \sum_{i=0}^{k-1} \frac{\eta_i(X_1, \ldots, X_r)^{p^{k-i}}}{p^{k-i}}. \tag{5.1}$$

Also, define $\eta_k(X_1) = 0$ for $k \geq 1$.

These polynomials are in fact over $\mathbb{Z}$, as we will see in Corollary 5.7, and can be computed and stored when performing computations with Witt vectors, and will replace the divisions by powers of p mentioned above. As before, we actually only need their reductions modulo p, and we will see how we can compute these almost entirely in characteristic p. In fact, seen as functions, rather than polynomials, we can evaluate these η_k's "on the fly", without having to first compute (and store in memory) the corresponding polynomials. (See Section 8.)

Remarks 5.2. We have the following immediate remarks about the η_k's.

(1) If τ is a permutation of $\{1, \ldots, r\}$, then $\eta_k(X_1, \ldots, X_r) = \eta_k(X_{\tau(1)}, \ldots, X_{\tau(r)})$.

(2)
$$\frac{(X_1 + \cdots + X_r)^{p^k}}{p^k} = \frac{X_1^{p^k} + \cdots + X_r^{p^k}}{p^k} - \sum_{i=1}^{k} \frac{\eta_i(X_1, \ldots, X_r)^{p^{k-i}}}{p^{k-i}}. \tag{5.2}$$

(3) $\eta_k(X_1, \ldots, X_r, 0, \ldots, 0) = \eta_k(X_1, \ldots, X_r)$. (Together with the first item, this means we can remove any entry equal to zero when computing η_k.)

Less trivially:

Proposition 5.3. *We have that* $\eta_k(X_0, Y_0) = S_k(X_0, 0, \ldots, 0, Y_0, 0, \ldots 0)$. *In particular,* $\eta_k(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$.

Proof. We prove the statement by induction on k. For $k = 0$ the statement is trivial. Now, if the statement holds for $\eta_i(X_1, X_2)$ for all $i \in \{0, \ldots, k-1\}$, then it also holds for $i = k$ by evaluating Eq. (2.4) at $(X_0, 0, \ldots, 0, Y_0, 0, \ldots 0)$. □

Although in practice we need $\eta_k(X_1, \ldots, X_r)$ with $r \geq 2$, one can obtain these from $\eta_k(X_1, X_2)$ by a recursion based on r. More precisely:

Proposition 5.4. *For any $i \geq 1$, let*

$$\mathcal{M}_{i,1} = \eta_i(X_1, \ldots, X_n), \qquad \mathcal{M}_{i,2} = \eta_i(X_{n+1}, \ldots, X_{n+m}),$$
$$\mathcal{M}_{i,3} = \eta_i(X_1 + \cdots + X_n, X_{n+1} + \cdots + X_{n+m}),$$

and, recursively for $i > 1$, define

$$\mathcal{M}_{i,3+j} = \eta_j(\mathcal{M}_{i-j,1}, \ldots, \mathcal{M}_{i-j,i-j+2})$$

for $j \in \{1, \ldots, i-1\}$. Then,

$$\eta_i(X_1, \ldots, X_{n+m}) = \sum_{j=1}^{i+2} \mathcal{M}_{i,j}.$$

Before we prove this proposition, it might be appropriate to make a few observations. Firstly, the notation is somewhat heavy, and it may make it a bit clearer if one write down the first few terms that appear. We have: let $\mathcal{M}_i \overset{\text{def}}{=} (\mathcal{M}_{i,1}, \ldots, \mathcal{M}_{i,i+2})$, $v_1 \overset{\text{def}}{=} (X_1, \ldots, X_n)$, $v_2 \overset{\text{def}}{=} (X_{n+1}, \ldots, X_{n+m})$, $s_1 \overset{\text{def}}{=} X_1 + \cdots + X_n$, and $s_2 \overset{\text{def}}{=} X_{n+1} + \cdots + X_{n+m}$. Then,

$$\begin{aligned}
\mathcal{M}_1 &= (\eta_1(v_1), \eta_1(v_2), \eta_1(s_1, s_2)), \\
\mathcal{M}_2 &= (\eta_2(v_1), \eta_2(v_2), \eta_2(s_1, s_2), \eta_1(\mathcal{M}_1)), \\
\mathcal{M}_3 &= (\eta_3(v_1), \eta_3(v_2), \eta_3(s_1, s_2), \eta_1(\mathcal{M}_2), \eta_2(\mathcal{M}_1)), \\
&\vdots
\end{aligned}$$

Also, we would like to observe that the proposition allows us to avoid expanding unnecessary powers (as explained in Section 1). This might be better understood with an example.

Example 5.5. Let $\Bbbk$ be a field of characteristic $p > 0$ and $a_1, a_2, a_3, a_4 \in \Bbbk$. Suppose also that we have computed and stored the polynomials $\eta_i(X_1, X_2)$ for $i = 1, 2$, which we assume for now have integer coefficients. (This is proved in Corollary 5.7 below.) For instance, we have

$$\eta_1(X, Y) = \sum_{i=1}^{p-1} \left(\frac{1}{p} \binom{p}{i} \right) X^i Y^{p-i}.$$

If we want to compute $\eta_2(a_1, a_2, a_3, a_4)$, we can use Proposition 5.4, which gives us that

$$\begin{aligned}
\eta_2(a_1,a_2,a_3,a_4) &= \eta_2(a_1,a_2) + \eta_2(a_3,a_4) + \eta_2(a_1+a_2, a_3+a_4) \\
&\qquad + \eta_1(\eta_1(a_1,a_2), \eta_1(a_3,a_4), \eta_1(a_1+a_2, a_3+a_4)) \\
&= \eta_2(a_1,a_2) + \eta_2(a_3,a_4) + \eta_2(a_1+a_2, a_3+a_4) \\
&\qquad + \eta_1(\eta_1(a_1,a_2), \eta_1(a_3,a_4)) \\
&\qquad + \eta_1(\eta_1(a_1,a_2) + \eta_1(a_3,a_4), \eta_1(a_1+a_2, a_3+a_4)).
\end{aligned}$$

So, we compute $\eta_1(a_1, a_2)$, $\eta_1(a_3, a_4)$, $\eta_1(a_1 + a_2, a_3 + a_4)$, which give results in $\Bbbk$, thus simplifying the computations of other terms, e.g., $\eta_1(\eta_1(a_1, a_2), \eta_1(a_3, a_4))$. If one would compute first the polynomial $\eta_2(X_1, X_2, X_3, X_4)$, it would be necessary to perform similar computations with polynomials instead, e.g., we would need

$$\eta_1(\eta_1(X_1,X_2), \eta_1(X_3,X_4)) = \sum_{i=1}^{p-1} \left(\frac{1}{p} \binom{p}{i} \right) \eta_1(X_1,X_2)^i \eta_1(X_3,X_4)^{p-i},$$

which would then expand powers of $\eta_1(X_1, X_2)$ and $\eta_1(X_3, X_4)$.

The example above illustrates, in a very simple particular case, how one can obtain $\eta_k(a_1, \ldots, a_n)$ from $\eta_k(X, Y)$ in a very particular case. Algorithm 1 gives the general recursive procedure to compute $\mathcal{M}_i(a_1, \ldots, a_n)$, for $i \in \{1, \ldots, k\}$ using only $\eta_i(X, Y)$. To obtain then $\eta_i(a_1, \ldots, a_n)$, one just need to add all the entries of the computed vector $\mathcal{M}_i(a_1, \ldots, a_n)$.

Before we proceed with the proof of Proposition 5.4, we need a little extra notation:

Definition 5.6. Let R be a ring of characteristic 0 and $f \in R[X_1, \ldots, X_r]$. Then, define $f^{[p^n]}$ to be the sum of the p^n-th powers of the terms of f. (We assume that the terms of f are collected together, e.g., $(X + X + Y)^{[p]} = (2X)^p + Y^p$, and not $X^p + X^p + Y^p$.)

Also, if $f, g \in R[X_1, \ldots, X_r]$, we say that f and g are *disjoint* if there is no monomial in $R[X_1, \ldots, X_r]$ having non-zero R-multiples appearing on both f and g (with terms collected).

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

Proof of Proposition 5.4. We prove the proposition by induction on i. To simplify the notation, let $v \overset{\text{def}}{=} (X_1, \ldots, X_{n+m})$, and as above, let $v_1 \overset{\text{def}}{=} (X_1, \ldots, X_n)$, $v_2 \overset{\text{def}}{=} (X_{n+1}, \ldots, X_{n+m})$, $s_1 \overset{\text{def}}{=} X_1 + \cdots + X_n$, $s_2 \overset{\text{def}}{=} X_{n+1} + \cdots + X_{n+m}$, and $\mathcal{M}_j \overset{\text{def}}{=} (\mathcal{M}_{j,1}, \ldots, \mathcal{M}_{j,j+2})$. For $i = 1$ we

Algorithm 1 Compute $(\mathcal{M}_1(a_1, \dots, a_n), \dots, \mathcal{M}_k(a_1, \dots, a_n))$, using only $\eta_i(X, Y)$

```
function V-ETAS($v = (a_1, \dots, a_n)$, $k$)
    if $n = 1$ then
        return $(0, \dots, 0)$
    end if
    if $n = 2$ then
        return $(\eta_1(a_1, a_2), \dots, \eta_k(a_1, a_2))$
    end if
    $m \leftarrow \lfloor n/2 \rfloor$
    $v_1 \leftarrow (a_1, \dots, a_m)$
    $v_2 \leftarrow (a_{m+1}, \dots, a_n)$
    $s_1 \leftarrow a_1 + \cdots + a_m$
    $s_2 \leftarrow a_{m+1} + \cdots + a_n$
    $x_1 \leftarrow$ V-ETAS$((a_1, \dots, a_m), k)$
    $x_2 \leftarrow$ V-ETAS$((a_{m+1}, \dots, a_n), k)$
    $x_3 \leftarrow$ V-ETAS$((s_1, s_2), k)$
    $R \leftarrow ()$                                            ▷ result
    for $i \leftarrow 1$, $k$ do                                 ▷ add first three entries to all $\mathcal{M}_i$
        $R[i] \leftarrow (x_1[i], x_2[i], x_3[i])$
    end for
    for $i \leftarrow 2$, $k$ do                                 ▷ add the remaining entries
        $T \leftarrow$ V-ETAS$(R[i-1], k - i + 1)$               ▷ temp. var.
        for $t \leftarrow i$, $k$ do
            append $T[t - i + 1]$ to $R[t]$
        end for
    end for
    return $R$
end function
```

have, since s_1 and s_2 are disjoint,

$$\begin{aligned}\eta_1(v) &= \frac{(s_1 + s_2)^{[p]} - (s_1 + s_2)^p}{p} \\ &= \frac{s_1^{[p]} - s_1^p}{p} + \frac{s_2^{[p]} - s_2^p}{p} + \frac{s_1^p + s_2^p - (s_1 + s_2)^p}{p} \\ &= \eta_1(v_1) + \eta_1(v_2) + \eta_1(s_1, s_2) \\ &= \mathcal{M}_{1,1} + \mathcal{M}_{1,2} + \mathcal{M}_{1,3}.\end{aligned}$$

Now, assume the result holds for $j \in \{1, \dots, (i-1)\}$. We have

$$\eta_i(v) = \frac{(s_1+s_2)^{[p^i]} - (s_1+s_2)^{p^i}}{p^i} - \sum_{j=1}^{i-1} \frac{\eta_j(v)^{p^{i-j}}}{p^{i-j}} = \frac{s_1^{[p^i]} - s_1^{p^i}}{p^i} + \frac{s_2^{[p^i]} - s_2^{p^i}}{p^i} + \frac{s_1^{p^i} + s_2^{p^i} - (s_1+s_2)^{p^i}}{p^i} - \sum_{j=1}^{i-1} \frac{(\mathcal{M}_{j,1} + \cdots + \mathcal{M}_{j,j+2})^{p^{i-j}}}{p^{i-j}}. \quad (5.3)$$

Now, for $r = 1$ or 2, by the definitions of η_i and $\mathcal{M}_{i,r}$, we have

$$\frac{s_r^{[p^i]} - s_r^{p^i}}{p^i} = \sum_{j=1}^{i} \frac{\eta_j(v_r)^{p^{i-j}}}{p^{i-j}} = \mathcal{M}_{i,r} + \sum_{j=1}^{i-1} \frac{\mathcal{M}_{j,r}^{p^{i-j}}}{p^{i-j}}$$

and

$$\frac{s_1^{p^i} + s_2^{p^i} - (s_1+s_2)^{p^i}}{p^i} = \sum_{j=1}^{i} \frac{\eta_j(s_1,s_2)^{p^{i-j}}}{p^{i-j}} = \mathcal{M}_{i,3} + \sum_{j=1}^{i-1} \frac{\mathcal{M}_{j,3}^{p^{i-j}}}{p^{i-j}}.$$

Thus, Eq. (5.3) becomes

$$\eta_i(v) = \mathcal{M}_{i,1} + \mathcal{M}_{i,2} + \mathcal{M}_{i,3} + \sum_{j=1}^{i-1} \frac{\mathcal{M}_{j,1}^{p^{i-j}} + \mathcal{M}_{j,2}^{p^{i-j}} + \mathcal{M}_{j,3}^{p^{i-j}} - (\mathcal{M}_{j,1} + \cdots + \mathcal{M}_{j,j+2})^{p^{i-j}}}{p^{i-j}}. \quad (5.4)$$

Now,

$$\frac{\mathcal{M}_{j,1}^{p^{i-j}} + \mathcal{M}_{j,2}^{p^{i-j}} + \mathcal{M}_{j,3}^{p^{i-j}} - (\mathcal{M}_{j,1} + \cdots + \mathcal{M}_{j,j+2})^{p^{i-j}}}{p^{i-j}} = \frac{\mathcal{M}_{j,1}^{p^{i-j}} + \cdots + \mathcal{M}_{j,j+2}^{p^{i-j}} - (\mathcal{M}_{j,1} + \cdots + \mathcal{M}_{j,j+2})^{p^{i-j}}}{p^{i-j}} - \frac{\mathcal{M}_{j,4}^{p^{i-j}} + \cdots + \mathcal{M}_{j,j+2}^{p^{i-j}}}{p^{i-j}},$$

and the first fraction of the right hand side above is, by the definitions of η_{i-j} and $\mathcal{M}_{j+k,r}$, equal to

$$\sum_{k=1}^{i-j} \frac{\eta_k(\mathcal{M}_j)^{p^{i-j-k}}}{p^{i-j-k}} = \sum_{k=1}^{i-j} \frac{\mathcal{M}_{j+k,k+3}^{p^{i-j-k}}}{p^{i-j-k}}.$$

Therefore, Eq. (5.4) becomes

$$\eta_i(v) = \mathcal{M}_{i,1} + \mathcal{M}_{i,2} + \mathcal{M}_{i,3} + \sum_{j=1}^{i-1} \sum_{k=1}^{i-j} \frac{\mathcal{M}_{j+k,k+3}^{p^{i-j-k}}}{p^{i-j-k}} - \sum_{j=2}^{i-1} \sum_{k=4}^{j+2} \frac{\mathcal{M}_{j,k}^{p^{i-j}}}{p^{i-j}}. \quad (5.5)$$

Now, simple manipulations of summations give us

$$\sum_{j=1}^{i-1} \sum_{k=1}^{i-j} \frac{\mathcal{M}_{j+k,k+3}^{p^{i-j-k}}}{p^{i-j-k}} = \sum_{j=1}^{i-1} \sum_{l=j+1}^{i} \frac{\mathcal{M}_{l,l-j+3}^{p^{i-l}}}{p^{i-l}} = \sum_{l=2}^{i} \sum_{j=1}^{l-1} \frac{\mathcal{M}_{l,l-j+3}^{p^{i-l}}}{p^{i-l}} = \sum_{l=2}^{i} \sum_{m=4}^{l+2} \frac{\mathcal{M}_{l,m}^{p^{i-l}}}{p^{i-l}}.$$

This equation together with Eq. (5.5) finishes the proof. □

Corollary 5.7. *We have that $\eta_i(X_1, \dots, X_r) \in \mathbb{Z}[X_1, \dots, X_r]$ for all $r \geq 2$.*

Proof. We prove the statement by induction on r. For $r = 2$ (and all i), the statement follows from Proposition 5.3. So, suppose that $r > 2$ and $\eta_i(X_1, \dots, X_j) \in \mathbb{Z}[X_1, \dots, X_r]$ for all $j \in \{2, \dots, (r-1)\}$ (and for all i).

The statement for r variables now follows from Proposition 5.4 by an induction on i: the case of $i = 1$ follows by the induction hypothesis on r since

$$\eta_1(X_1, \dots, X_r) = \eta_1(X_1, \dots, X_{r-1}) + \eta_1(X_1 + \cdots + X_{r-1}, X_r).$$

For the second step of the induction (on i) we use again $n = 1$ and $m = r - 1$ in Proposition 5.4, which gives $\eta_i(X_1, \dots, X_r)$ as sums and compositions of $\eta_k(X_1, \dots, X_j)$ where either $k = i$ and $j < r$ (and we use the induction hypothesis on r), or $k < i$ (and we use the induction hypothesis on i). □

Although we will carry on with η_k over $\mathbb{Z}$, as it will be convenient in the proofs that follow, what really is of interest to us are their reduction modulo p, which we shall denote by $\bar{\eta}_k$, as these functions will always be evaluated in characteristic p. In Section 8 we discuss how one can compute the $\bar{\eta}_k$'s almost entirely in characteristic p.

We introduce some extra notation.

Definition 5.8. If R is a ring of characteristic p and $v = (a_1, \dots, a_r) \in R^r$, we define $\eta_k(v) = \eta_k(a_1, \dots, a_r)$ as the evaluation $\eta_k(X_1, \dots, X_r)$ at v. (This makes sense as $\eta_k(X_1, \dots, X_r) \in \mathbb{Z}[X_1, \dots, X_r]$.)

Moreover, if f is a polynomial (possibly in many variables) with coefficients in R, we write $\mathrm{vec}\,(f)$ for the vector that contains the terms of f (after some choice of order for the monomials). We then may write $\eta_k(f)$ for $\eta_k(\mathrm{vec}\,(f))$. (It is important to observe that we are assuming that the terms are reduced, i.e., if $f = 1 + X + 2X$, then $\mathrm{vec}\,(f) = (1, 3X)$, not $(1, X, 2X)$.)

With this notation, we have that $\psi_k(f)$ (from [Fin10a]) is just $\eta_k(f)$ as defined above. (The meanings of $\eta_k(v)$ is the same here and in [Fin10a].)

6. The Formula for the Greenberg Transform

We will now give a formula for the Greenberg transform that can be computed, for the most part, directly in characteristic p.

Since the formula is quite involved, we will need to introduce a reasonable ammount of notation.

Definition 6.1. If $\boldsymbol{g} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$ is given by $\boldsymbol{g} = \sum_{i,j} \boldsymbol{a}_{i,j} \boldsymbol{x}^i \boldsymbol{y}^j$, then we write

$$\xi_k(\boldsymbol{g}) \stackrel{\text{def}}{=} \sum_{i,j} \xi_k(\boldsymbol{a}_{i,j}) \boldsymbol{x}^i \boldsymbol{y}^j,$$

with ξ_k as in Definition 2.1. (Hence, $\boldsymbol{g} \equiv \sum_{k=0}^{r} \xi_k(\boldsymbol{g}) p^k \pmod{p^{r+1}}$.) Furthermore, define

$$\boldsymbol{g}^{(i,j)} \stackrel{\text{def}}{=} \frac{1}{i!j!} \frac{\partial^{i+j}}{\partial \boldsymbol{x}^i \partial \boldsymbol{y}^j} \boldsymbol{g}, \quad \text{and} \quad \boldsymbol{g}_{i,j,k} \stackrel{\text{def}}{=} \xi_k(\boldsymbol{g}^{(i,j)}).$$

Definition 6.2. We define $D^{i,j}_{k,n}$ to be the coefficient of $\boldsymbol{t}^k$ in

$$(\boldsymbol{t}\boldsymbol{x}_1^{p^{n-1}} + \boldsymbol{t}^2 \boldsymbol{x}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^n \boldsymbol{x}_n)^i (\boldsymbol{t}\boldsymbol{y}_1^{p^{n-1}} + \boldsymbol{t}^2 \boldsymbol{y}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^n \boldsymbol{y}_n)^j.$$

(E.g., if $n \geq 2$, then $D^{1,2}_{4,n} = 2\boldsymbol{x}_1^{p^{n-1}} \boldsymbol{y}_1^{p^{n-1}} \boldsymbol{y}_2^{p^{n-2}} + \boldsymbol{x}_2^{p^{n-2}} \boldsymbol{y}_1^{2p^{n-1}}$.) Furthermore, we shall denote

$$D^{i,j}_{k,n,l} \stackrel{\text{def}}{=} \xi_l(D^{i,j}_{k,n}).$$

Note that if $k < r$ (and $r \geq i$), then $D^{i,r-i}_{k,n} = 0$ and if $k \neq 0$, then $D^{0,0}_{k,n} = 0$. Also, observe that:

$$\begin{aligned}
&(p\boldsymbol{x}_1^{p^{n-1}} + p^2 \boldsymbol{x}_2^{p^{n-2}} + \cdots + p^n \boldsymbol{x}_n)^i (p\boldsymbol{y}_1^{p^{n-1}} + p^2 \boldsymbol{y}_2^{p^{n-2}} + \cdots + p^n \boldsymbol{y}_n)^{r-i} \\
&\quad = \sum_{k=r}^{\infty} D^{i,r-i}_{k,n} p^k = \sum_{k=r}^{\infty} \sum_{l=0}^{\infty} D^{i,r-i}_{k,n,l} p^{k+l} = \sum_{k=r}^{\infty} \sum_{j=k}^{\infty} D^{i,r-i}_{k,n,j-k} p^j = \sum_{j=r}^{\infty} \sum_{k=r}^{j} D^{i,r-i}_{k,n,j-k} p^j. \quad (6.1)
\end{aligned}$$

Definition 6.3. Let $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$. Then, for a given $n \geq 0$, let $(\mathcal{G}_{n,1}, \ldots, \mathcal{G}_{n,N_n})$ be the vector obtained by joining the vectors $\operatorname{vec}\left((\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D^{i,r-i}_{k,n,j-k}\right)$, for $r \in \{0, \ldots n\}$, $i \in \{0, \ldots, r\}$, $j \in \{r, \ldots n\}$, and $k \in \{r, \ldots, j\}$. (The ordering is not important.) Also, recursively, if $n > 1$, define

$$\mathcal{G}_{n,N_n+i+1} \stackrel{\text{def}}{=} \eta_{n-i}(\mathcal{G}_{i,1}, \ldots, \mathcal{G}_{i,N_i+i}),$$

for $i \in \{0, \ldots, (n-1)\}$. Then, define,

$$\boldsymbol{f}_n \stackrel{\text{def}}{=} \sum_{i=1}^{N_n+n} \mathcal{G}_{n,i},$$

and $\mathcal{G}_n \stackrel{\text{def}}{=} (\mathcal{G}_{n,1}, \ldots, \mathcal{G}_{n,N_n+n})$.

Then, we have:

Theorem 6.4. *With the notation above, we have that $\mathscr{G}(\boldsymbol{f}) = (f_0, f_1, \ldots)$, where f_n is the reduction modulo p of*

$$\boldsymbol{f}_n = \sum_{i=1}^{N_n+n} \mathcal{G}_{n,i} = \sum_{r=0}^{n} \sum_{i=0}^{r} \sum_{j=r}^{n} \sum_{k=r}^{j} (\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D^{i,r-i}_{k,n,j-k} + \sum_{i=0}^{n-1} \eta_{n-i}(\mathcal{G}_i). \quad (6.2)$$

Note that although

$$\sum_{i=1}^{N_n} \mathcal{G}_{n,i} = \sum_{r=0}^{n} \sum_{i=0}^{r} \sum_{j=r}^{n} \sum_{k=r}^{j} (\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D_{k,n,j-k}^{i,r-i},$$

the vector $(\mathcal{G}_{n,1}, \ldots, \mathcal{G}_{n,N_n})$ is *not*, in general, just a reordering of

$$\operatorname{vec}\left(\sum_{r=0}^{n} \sum_{i=0}^{r} \sum_{j=r}^{n} \sum_{k=r}^{j} (\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D_{k,n,j-k}^{i,r-i} \right)$$

as cancellations will likely occur when summing. Defining

$$(\mathcal{G}_{n,1}, \ldots, \mathcal{G}_{n,N_n}) = \operatorname{vec}\left(\sum_{r=0}^{n} \sum_{i=0}^{r} \sum_{j=r}^{n} \sum_{k=r}^{j} (\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D_{k,n,j-k}^{i,r-i} \right)$$

does not work in general!

Although Eq. (6.2) is quite complicated, it simplifies greatly in some particular cases, such as if we just want up to the third coordinate. In that case, the reduction modulo p of $\boldsymbol{f}_2$ given here is just Eq. (6.1) in [Fin10a]. See also the examples in Section 7.

Moreover, since we are only interested in the reduction modulo p of the $\boldsymbol{f}_n$, say f_n, we can compute these mostly in characteristic p. For instance, using the bar to denote reduction modulo p and assuming we have already computed $\bar{\mathcal{G}}_i$ for $i \in \{1, \ldots, (n-1)\}$, we can compute $\bar{\mathcal{G}}_{n,N_n+i+1}$ for $i \in \{0, \ldots, (n-1)\}$ directly with $\bar{\mathcal{G}}_{n,N_n+i+1} = \bar{\eta}_{n-i}(\bar{\mathcal{G}}_i)$.

For $\bar{\mathcal{G}}_{n,i}$ with $i \in \{1, \ldots, N_n\}$ some computations not in characteristic p are necessary. We need to compute the reductions modulo p of $(\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D_{k,n,j-k}^{i,r-i}$, for $r \in \{0, \ldots n\}$, $i \in \{0, \ldots, r\}$, $j \in \{r, \ldots n\}$, and $k \in \{r, \ldots, j\}$. Now,

$$(\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) = \xi_{n-j}((\boldsymbol{f}^{(i,r-i)})^{\sigma^n})(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}),$$

and if $\boldsymbol{g} = \sum_{i,j} \boldsymbol{b}_{i,j} \boldsymbol{x}^i \boldsymbol{y}^j$ and $\boldsymbol{b}_{i,j} = (b_{i,j,0}, b_{i,j,1}, \ldots)$, then

$$\pi(\xi_k(\boldsymbol{g}^{\sigma^n}(\boldsymbol{x}^{p^n}, \boldsymbol{y}^{p^n}))) = \sum_{i,j,k} b_{i,j,k}^{p^{k+n}} x_0^{ip^n} y_0^{jp^n}.$$

Thus, we need to compute the coefficients of the partial derivatives $\boldsymbol{f}^{(i,r-i)}$ modulo p^{n-j+1}. So, one needs to convert integers to Witt vectors (of length p^{n-j}) and multiply then by the corresponding coefficients of $(\boldsymbol{f}^{(i,r-i)})^{\sigma^n}$. If $j = 0$, then we must have that $r = i = 0$, and hence no partial derivative is needed. Therefore, the necessary products of Witt vectors are done with lengths less than or equal to n instead of $(n+1)$. More precisely, first order partial derivatives (i.e., $r = 1$) are needed only modulo p^n, second order ones (i.e,, $r = 2$) are needed only modulo p^{n-1}, and so on.

For the terms $D^{i,r-i}_{k,n,j-k}$, we also need some computations not in characteristic p. Since $(j-k) \in \{0,\dots,n-r\}$, we need to compute the products

$$(\boldsymbol{t}\boldsymbol{x}_1^{p^{n-1}} + \boldsymbol{t}^2\boldsymbol{x}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^n\boldsymbol{x}_n)^i(\boldsymbol{t}\boldsymbol{y}_1^{p^{n-1}} + \boldsymbol{t}^2\boldsymbol{y}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^n\boldsymbol{y}_n)^{r-i},$$

over $\mathbb{Z}/p^{n-r+1}\mathbb{Z}$ and convert the coefficients to Witt vectors of length $n-r+1$.

On the other hand, it should be observed that all these computations not in characteristic p are in fact relatively fast, and do not slow down the algorithm. (Most of the time is spent computing the $\bar{\eta}_{n-i}(\bar{\mathcal{G}}_i)$'s.)

Before we proceed with the proof, we introduce some extra notation.

Definition 6.5. Let K be the field of fractions of $\boldsymbol{W}(\mathbb{k})$. (Note that $K = \boldsymbol{W}(\mathbb{k})[1/p]$.) If $\boldsymbol{f}, \boldsymbol{g} \in K[\boldsymbol{x},\boldsymbol{y}]$, then we write $\boldsymbol{f} \equiv \boldsymbol{g} \pmod p$ if $\boldsymbol{f} - \boldsymbol{g} \in (p) = p\boldsymbol{W}(\mathbb{k})[\boldsymbol{x},\boldsymbol{y}]$.

Proof of Theorem 6.4. By Theorem 3.2, it suffices to show that $\boldsymbol{f}_i$'s satisfy Eq. (3.1) for all n. We prove this by induction on n.

For $n = 0$ the result is clear. So, assume now that if $r < n$, then

$$W^{(r)}(\boldsymbol{f}_0,\dots,\boldsymbol{f}_r) \equiv \boldsymbol{f}^{\sigma^r}(W^{(r)}(\boldsymbol{x}_0,\dots,\boldsymbol{x}_r), W^{(r)}(\boldsymbol{y}_0,\dots,\boldsymbol{y}_r)) \pmod{p^{r+1}}.$$

To simplify the notation, let $\boldsymbol{g} \overset{\text{def}}{=} \boldsymbol{f}^{\sigma^n}$. To prove that the equation above holds for $r = n$ it suffices to show that

$$\boldsymbol{f}_n \equiv \frac{1}{p^n}\boldsymbol{g}(\boldsymbol{x}_0^{p^n} + \cdots + p^n\boldsymbol{x}_n, \boldsymbol{y}_0^{p^n} + \cdots + p^n\boldsymbol{y}_n) - \sum_{i=0}^{n-1} \frac{\boldsymbol{f}_i^{p^{n-i}}}{p^{n-i}} \pmod p. \tag{6.3}$$

Using Eq. (5.2), we obtain

$$\sum_{i=0}^{n-1} \frac{\boldsymbol{f}_i^{p^{n-i}}}{p^{n-i}} = \sum_{i=0}^{n-1} \left[\sum_{r=1}^{N_i+i} \frac{\mathcal{G}_{i,r}^{p^{n-i}}}{p^{n-i}} - \sum_{l=1}^{n-i} \frac{\eta_l(\mathcal{G}_i)^{p^{n-i-l}}}{p^{n-i-l}} \right]. \tag{6.4}$$

But

$$\begin{aligned} \sum_{i=0}^{n-1}\sum_{l=1}^{n-i} \frac{\eta_l(\mathcal{G}_i)^{p^{n-i-l}}}{p^{n-i-l}} &= \sum_{i=0}^{n-1}\sum_{j=i+1}^{n} \frac{\eta_{j-i}(\mathcal{G}_i)^{p^{n-j}}}{p^{n-j}} \\ &= \sum_{j=1}^{n}\sum_{i=0}^{j-1} \frac{\eta_{j-i}(\mathcal{G}_i)^{p^{n-j}}}{p^{n-j}} = \sum_{j=1}^{n}\sum_{i=0}^{j-1} \frac{\mathcal{G}_{j,N_j+i+1}^{p^{n-j}}}{p^{n-j}} = \sum_{j=1}^{n}\sum_{r=N_j+1}^{N_j+j} \frac{\mathcal{G}_{j,r}^{p^{n-j}}}{p^{n-j}}. \end{aligned} \tag{6.5}$$

Putting Eqs. (6.4) and (6.5) together, we obtain

$$\begin{aligned}\sum_{i=0}^{n-1} \frac{\boldsymbol{f}_i^{p^{n-i}}}{p^{n-i}} &= \sum_{i=0}^{n-1}\sum_{r=1}^{N_i} \frac{\mathcal{G}_{i,r}^{p^{n-i}}}{p^{n-i}} + \sum_{i=1}^{n-1}\sum_{r=N_i+1}^{N_i+i} \frac{\mathcal{G}_{i,r}^{p^{n-i}}}{p^{n-i}} - \sum_{i=1}^{n}\sum_{r=N_i+1}^{N_i+i} \frac{\mathcal{G}_{i,r}^{p^{n-i}}}{p^{n-i}} \\ &= \sum_{i=0}^{n-1}\sum_{r=1}^{N_i} \frac{\mathcal{G}_{i,r}^{p^{n-i}}}{p^{n-i}} - \sum_{r=N_n+1}^{N_n+n} \mathcal{G}_{n,r}. \qquad (6.6)\end{aligned}$$

Using Taylor expansion and Eq. (6.1), and with the notation of Definition 6.5, we obtain:

$$\begin{aligned}&\frac{1}{p^n}\boldsymbol{g}(\boldsymbol{x}_0^{p^n} + \cdots + p^n\boldsymbol{x}_n, \boldsymbol{y}_0^{p^n} + \cdots + p^n\boldsymbol{y}_n) \\ &\quad\equiv \frac{1}{p^n}\sum_{r=0}^{n}\sum_{i=0}^{r} \boldsymbol{g}^{(i,r-i)}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n})(p\boldsymbol{x}_1^{p^{n-1}} + \cdots p^n\boldsymbol{x}_n)^i(p\boldsymbol{y}_1^{p^{n-1}} + \cdots + p^n\boldsymbol{y}_n)^{r-i} \\ &\quad\equiv \sum_{r=0}^{n}\sum_{i=0}^{r}\sum_{j=r}^{n}\sum_{k=r}^{j} \boldsymbol{g}^{(i,r-i)}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n})\frac{D_{k,n,j-k}^{i,r-i}}{p^{n-j}} \pmod{p}.\end{aligned}$$

Taking into account the factors of p in $\boldsymbol{g}^{(i,r-i)}$ and manipulating the summations, the above equation becomes

$$\begin{aligned}&\frac{1}{p^n}\boldsymbol{g}(\boldsymbol{x}_0^{p^n} + \cdots + p^n\boldsymbol{x}_n, \boldsymbol{y}_0^{p^n} + \cdots + p^n\boldsymbol{y}_n) \\ &\qquad\equiv \sum_{r=0}^{n}\sum_{i=0}^{r}\sum_{j=r}^{n}\sum_{k=r}^{j}\sum_{s=0}^{n-j} \boldsymbol{g}_{i,r-i,s}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n})\frac{D_{k,n,j-k}^{i,r-i}}{p^{n-j-s}} \\ &\qquad= \sum_{r=0}^{n}\sum_{i=0}^{r}\sum_{j=r}^{n}\sum_{k=r}^{j}\sum_{l=j}^{n} \boldsymbol{g}_{i,r-i,l-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n})\frac{D_{k,n,j-k}^{i,r-i}}{p^{n-l}} \\ &\qquad= \sum_{l=0}^{n}\sum_{r=0}^{l}\sum_{i=0}^{r}\sum_{j=r}^{l}\sum_{k=r}^{j} \boldsymbol{g}_{i,r-i,l-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n})\frac{D_{k,n,j-k}^{i,r-i}}{p^{n-l}} \pmod{p}.\end{aligned}$$

Now, by definition of $\mathcal{G}_{n,r}$, for $i \in \{1, \dots, N_i\}$, we obtain

$$\begin{aligned}&\frac{1}{p^n}\boldsymbol{g}(\boldsymbol{x}_0^{p^n} + \cdots + p^n\boldsymbol{x}_n, \boldsymbol{y}_0^{p^n} + \cdots + p^n\boldsymbol{y}_n) \equiv \\ &\qquad \sum_{i=1}^{N_n}\mathcal{G}_{n,i} + \sum_{l=0}^{n-1}\sum_{r=0}^{l}\sum_{i=0}^{r}\sum_{j=r}^{l}\sum_{k=r}^{j} \boldsymbol{g}_{i,r-i,l-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n})\frac{D_{k,n,j-k}^{i,r-i}}{p^{n-l}} \pmod{p}. \qquad (6.7)\end{aligned}$$

Hence, by Eqs. (6.3), (6.6), and (6.7), it suffices to show that

$$\sum_{r=0}^{l}\sum_{i=0}^{r}\sum_{j=r}^{l}\sum_{k=r}^{j} (\boldsymbol{f}^{\sigma^n})_{i,r-i,l-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D_{k,n,j-k}^{i,r-i} = \sum_{r=1}^{N_l} \mathcal{G}_{l,r}^{p^{n-l}}.$$

Now, by the definition of the $\mathcal{G}_{l,i}$ (and with the notation from Definition 5.6), we have that

$$\sum_{r=1}^{N_l} \mathcal{G}_{l,r}^{p^{n-l}} = \sum_{r=0}^{l}\sum_{i=0}^{r}\sum_{j=r}^{l}\sum_{k=r}^{j}((\boldsymbol{f}^{\sigma^l})_{i,r-i,l-j}(\boldsymbol{x}_0^{p^l}, \boldsymbol{y}_0^{p^l}) D_{k,l,j-k}^{i,r-i})^{[p^{n-l}]}.$$

Moreover, since $D_{j,l,j-k}^{i,r-i}$ and $(\boldsymbol{f}^{\sigma^l})_{i,r-i,l-j}(\boldsymbol{x}_0^{p^l}, \boldsymbol{y}_0^{p^l})$ are disjoint and involve different variables, we have that

$$((\boldsymbol{f}^{\sigma^l})_{i,r-i,l-j}(\boldsymbol{x}_0^{p^l}, \boldsymbol{y}_0^{p^l}) D_{k,l,j-k}^{i,r-i})^{[p^{n-l}]} = ((\boldsymbol{f}^{\sigma^l})_{i,r-i,l-j}(\boldsymbol{x}_0^{p^l}, \boldsymbol{y}_0^{p^l}))^{[p^{n-l}]} (D_{k,l,j-k}^{i,r-i})^{[p^{n-l}]}.$$

Thus, our problem reduces to proving that

$$(\boldsymbol{f}^{\sigma^n})_{i,r-i,l-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) = \left((\boldsymbol{f}^{\sigma^l})_{i,r-i,l-j}(\boldsymbol{x}_0^{p^l}, \boldsymbol{y}_0^{p^l})\right)^{[p^{n-l}]}$$

and

$$D_{k,n,j-k}^{i,r-i} = (D_{k,l,j-k}^{i,r-i})^{[p^{n-l}]}.$$

For the former, first observe that the Frobenius homomorphism σ acts trivially on $\mathbb{Z}$, and hence, $(\boldsymbol{f}^{\sigma^s})^{(i,r-i)} = (\boldsymbol{f}^{(i,r-i)})^{\sigma^s}$. Moreover, with the $\boldsymbol{a}_{i,j} \in \boldsymbol{W}(\Bbbk)$ and $\boldsymbol{a}_{i,j,k} \overset{\text{def}}{=} \xi_k(\boldsymbol{a}_{i,j})$, we have that $\sigma^s(\boldsymbol{a}_{i,j}) = \sum_{k=0}^{\infty} \boldsymbol{a}_{i,j,k}^{p^s} p^k$. So, $(\boldsymbol{f}^{\sigma^s})_{i,r-i,l-j} = \xi_{l-j}((\boldsymbol{f}^{(i,r-i)})^{\sigma^s})$ has as coefficients the p^s-powers of the coefficients of $\boldsymbol{f}_{i,r-i,l-j} = \xi_{l-j}(\boldsymbol{f}^{(i,r-i)})$. With these observations, the (first) desired equality follows immediately.

For the latter, first observe that if $s > l$ (and since $l \geq k$), then there is no term in either $\boldsymbol{x}_s$ or $\boldsymbol{y}_s$ from

$$(\boldsymbol{t}\boldsymbol{x}_1^{p^{n-1}} + \boldsymbol{t}^2\boldsymbol{x}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^n\boldsymbol{x}_n)^i(\boldsymbol{t}\boldsymbol{y}_1^{p^{n-1}} + \boldsymbol{t}^2\boldsymbol{y}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^n\boldsymbol{y}_n)^{r-i}$$

appearing in $D_{k,n}^{i,r-i}$, as such a term would have degree (in $\boldsymbol{t}$) at least $s > l \geq k$. So, $D_{k,n}^{i,r-i}$ is the coefficient of the term of degree k (in $\boldsymbol{t}$) of

$$(\boldsymbol{t}\boldsymbol{x}_1^{p^{n-1}} + \boldsymbol{t}^2\boldsymbol{x}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^l\boldsymbol{x}_l^{p^{n-l}})^i(\boldsymbol{t}\boldsymbol{y}_1^{p^{n-1}} + \boldsymbol{t}^2\boldsymbol{y}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^l\boldsymbol{y}_l^{p^{n-l}})^{r-i},$$

while $D_{k,l}^{i,r-i}$ the coefficient of the term of degree k of

$$(\boldsymbol{t}\boldsymbol{x}_1^{p^{l-1}} + \boldsymbol{t}^2\boldsymbol{x}_2^{p^{l-2}} + \cdots + \boldsymbol{t}^l\boldsymbol{x}_l)^i(\boldsymbol{t}\boldsymbol{y}_1^{p^{l-1}} + \boldsymbol{t}^2\boldsymbol{y}_2^{p^{l-2}} + \cdots + \boldsymbol{t}^l\boldsymbol{y}_l)^{r-i}.$$

Now, since the coefficients of $D_{k,l}^{i,r-i}$ are integers, the coefficients of $D_{k,l,j-k}^{i,r-i}$ are invariant by powers of p. Therefore, it becomes clear that

$$D_{k,n,j-k}^{i,r-i} = (D_{k,l,j-k}^{i,r-i})^{[p^{n-l}]},$$

finishing the proof. □

7. Sums and Products

As seen in Section 3, the Greenberg transform generalizes the sum and products of Witt vectors. Thus, we can apply Theorem 6.4 to obtain the $\bar{S}_i$ and $\bar{P}_i$.

It should be observed that these equations have less importance now, as they are not necessary, in general, to perform computations with Witt vectors. On the other hand, the propositions below also give a method to compute sums and products of Witt vectors directly, i.e., without computing the polynomials S_i and P_i, but using the auxiliary functions η_i instead. (See Example 7.2 below.)

Proposition 7.1. *Define recursively for $k \geq 0$ (and a given prime p):*

$$\mathcal{S}_{k,1} \overset{\text{def}}{=} \boldsymbol{x}_k, \qquad \mathcal{S}_{k,2} \overset{\text{def}}{=} \boldsymbol{y}_k,$$

and for $k > 0$ and $i \in \{0, \dots, k-1\}$,

$$\mathcal{S}_{k,2+i} \overset{\text{def}}{=} \eta_{k-i}(\mathcal{S}_{i,1}, \dots, \mathcal{S}_{i,i+2}).$$

Then:

$$S_n \equiv \sum_{i=1}^{n+2} \mathcal{S}_{n,i} = \boldsymbol{x}_n + \boldsymbol{y}_n + \sum_{i=0}^{n-1} \eta_{n-i}(\mathcal{S}_{i,1}, \dots, \mathcal{S}_{i,i+2}) \pmod{p}.$$

Proof. We just apply Theorem 6.4 with $\boldsymbol{f} = \boldsymbol{x} + \boldsymbol{y}$. So, $\boldsymbol{f}^{\sigma^n}_{i,r-i,n-j}$ is zero unless r is either 0 or 1, and $j = n$. Moreover, for r equal to 0 or 1 (and $0 \leq i \leq r$), we have that $D^{i,r-i}_{k,n,j-k}$ is zero unless $k = j$. Since $j = n$, we then have $k = n$. Hence, for $n > 0$,

$$\begin{aligned}\sum_{i=1}^{N_n} \mathcal{G}_{n,i} &= \sum_{r=0}^{n} \sum_{i=0}^{r} \sum_{j=r}^{n} \sum_{k=r}^{j} (\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D^{i,r-i}_{k,n,j-k} \\ &= (\boldsymbol{x}_0^{p^n} + \boldsymbol{y}_0^{p^n}) D^{0,0}_{n,n,0} + D^{0,1}_{n,n,0} + D^{1,0}_{n,n,0} \\ &= 0 + \boldsymbol{y}_n + \boldsymbol{x}_n.\end{aligned}$$

Recalling now Remark 5.2, the proposition follows immediately. □

Maybe it is worth seeing an example of how one can use this proposition to perform sums of Witt vectors.

Example 7.2. Assume we have computed the polynomials $\bar{\eta}_k(X, Y) \in \mathbb{F}_p[X, Y]$ for $k = 1, 2$. To add $(1, 1, 1)$ and $(2, 0, 1)$ in $\boldsymbol{W}_3(\mathbb{F}_3)$, say $(c_0, c_1, c_2) = (1, 1, 1) + (2, 0, 1)$, we have $\mathcal{S}_{0,1} = 1$ and $\mathcal{S}_{0,2} = 2$. So,

$$c_0 = \mathcal{S}_{0,1} + \mathcal{S}_{0,2} = 1 + 2 = 0.$$

Then, we compute $\bar{\eta}_k(\mathcal{S}_{0,1}, \mathcal{S}_{0,2}) = \bar{\eta}_k(1, 2)$, for $k = 1, 2$. In this particular case, both of these are equal to zero. Thus,

$$\begin{aligned} c_1 &= \mathcal{S}_{1,1} + \mathcal{S}_{1,2} + \mathcal{S}_{1,3} \\ &= 1 + 0 + \bar{\eta}_1(1, 2) = 1 + 0 + 0 = 1. \end{aligned}$$

Finally, we need $\bar{\eta}_1(\mathcal{S}_{1,1}, \mathcal{S}_{1,2}, \mathcal{S}_{1,3}) = \bar{\eta}_1(1, 0, \bar{\eta}_1(1, 2)) = \bar{\eta}_1(1, 0, 0) = 0$. Then,

$$\begin{aligned} c_2 &= \mathcal{S}_{2,1} + \mathcal{S}_{2,2} + \mathcal{S}_{2,3} + \mathcal{S}_{2,4} \\ &= 1 + 1 + \bar{\eta}_1(\mathcal{S}_{1,1}, \mathcal{S}_{1,2}, \mathcal{S}_{1,3}) + \bar{\eta}_2(1, 2) \\ &= 1 + 1 + 0 + 0 = 2. \end{aligned}$$

The formula for P_n is similar.

Proposition 7.3. *Define recursively for $k \geq 0$ (and a given prime p): for $i \in \{1, \dots, k+1\}$,*

$$\mathcal{P}_{k,i} \overset{\text{def}}{=} \boldsymbol{x}_i^{p^{k-i}} \boldsymbol{y}_{k-i}^{p^i}$$

and for $k > 1$ and $i \in \{1, \dots, k-1\}$,

$$\mathcal{P}_{k,k+1+i} \overset{\text{def}}{=} \eta_{k-i}(\mathcal{P}_{i,1}, \dots, \mathcal{P}_{i,2i}).$$

Then, for $n > 0$:

$$P_n \equiv \sum_{i=1}^{2n} \mathcal{P}_{n,i} = \sum_{i=0}^{n} \boldsymbol{x}_i^{p^{k-i}} \boldsymbol{y}_{k-i}^{p^i} + \sum_{i=0}^{n-1} \eta_{n-i}(\mathcal{P}_{i,1}, \dots, \mathcal{P}_{i,2i}) \pmod{p}.$$

Proof. We just apply Theorem 6.4 with $\boldsymbol{f} = \boldsymbol{x}\boldsymbol{y}$. So, $\boldsymbol{f}_{i,r-i,n-j}^{\sigma^n}$ is zero unless r is either 0, 1, or 2 (in which case we need $i = 1$), and $j = n$. Moreover, since i and $r - i$ are either 0 or 1, we have that $D_{k,n,j-k}^{i,r-i}$ is zero unless $k = j$. Since $j = n$, we then have $k = n$. Hence, for $n > 0$,

$$\begin{aligned} \sum_{i=1}^{N_n} \mathcal{G}_{n,i} &= \sum_{r=0}^{n} \sum_{i=0}^{r} \sum_{j=r}^{n} \sum_{k=r}^{j} (\boldsymbol{f}^{\sigma^n})_{i,r-i,n-j}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) D_{k,n,j-k}^{i,r-i} \\ &= (\boldsymbol{x}_0^{p^n} \boldsymbol{y}_0^{p^n}) D_{n,n,0}^{0,0} + \boldsymbol{x}_0^{p^n} D_{n,n,0}^{0,1} + \boldsymbol{y}_0^{p^n} D_{n,n,0}^{1,0} + D_{n,n,0}^{1,0} \\ &= 0 + \boldsymbol{x}_0^{p^n} \boldsymbol{y}_n + \boldsymbol{x}_n \boldsymbol{y}_0^{p^n} + \left(\sum_{i=1}^{n-1} \boldsymbol{x}_i^{p^{n-i}} \boldsymbol{y}_{n-i}^{p^i} \right). \end{aligned}$$

Recalling now Remark 5.2, the proposition follows immediately. □

8. Computing $\bar{\eta}_k$ in Characteristic p

In this section we show how one can compute $\bar{\eta}_k(X, Y)$ almost entirely in characteristic p. (We do need to convert some binomial coefficients to Witt vectors, which is not done in characteristic p.) In fact, this new method, together with Proposition 5.4, allows us to not have to store these polynomials at all and compute $\bar{\eta}_k(a_1, \ldots, a_r)$, for a_i's in a ring of characteristic p, on the fly.

We will need the following elementary lemmas:

Lemma 8.1. *Let* v_p *denote the valuation at* p. *Then, if* $1 < a < p^k$, *we have that*

$$\mathrm{v}_p \binom{p^k}{a} = k - \mathrm{v}_p(a).$$

Proof. We prove it by induction on k. The case of $k = 1$ is trivial.

Now, suppose that for all $q \in \{1, \ldots, p^{k-1} - 1\}$, we have $\mathrm{v}_p\binom{p^{k-1}}{q} = (k-1) - \mathrm{v}_p(q)$. Since

$$\binom{p^k}{a} = \left(\prod_{i=1}^{a} (p^k - a + i) \right) \left(\prod_{i=1}^{a} i \right)^{-1},$$

we have

$$\mathrm{v}_p \binom{p^k}{a} = \sum_{i=1}^{a} \mathrm{v}_p(p^k - a + i) - \sum_{i=1}^{a} \mathrm{v}_p(i). \tag{8.1}$$

Let $a = qp + r$, with $r \in \{0, \ldots, (p-1)\}$ and define ϵ as 1 if $r = 0$ and 0 otherwise. Thus, $\mathrm{v}_p(a) = \epsilon(\mathrm{v}_p(q) + 1)$. Then, Eq. (8.1) and the induction hypothesis give:

$$\begin{aligned}
\mathrm{v}_p \binom{p^k}{a} &= \sum_{j=\epsilon}^{q} \mathrm{v}_p(p^k - a + (jp + r)) - \sum_{j=1}^{q} \mathrm{v}_p(jp) \\
&= (1 - \epsilon)\mathrm{v}_p(p^k - qp) + \sum_{j=1}^{q} \mathrm{v}_p(p^{k-1} - q + j) - \sum_{j=1}^{q} \mathrm{v}_p(j) \\
&= (1 - \epsilon)(\mathrm{v}_p(q) + 1) + \mathrm{v}_p \binom{p^{k-1}}{q} \\
&= (1 - \epsilon)(\mathrm{v}_p(q) + 1) + (k - 1) - \mathrm{v}_p(q) \\
&= k - \epsilon(\mathrm{v}_p(q) + 1) = k - \mathrm{v}_p(a).
\end{aligned}$$

□

Lemma 8.2. *We have that if* $0 < t \leq k$, *then* $(X+1)^{p^k} \equiv (X^{p^{k-t}} + 1)^{p^t} \pmod{p^{t+1}}$. *In particular, if* $0 < j \leq t$ *and* $i \in \{1, \ldots, p^j - 1\}$ *with* $p \nmid i$, *then*

$$\frac{1}{p^j} \binom{p^k}{ip^{k-j}} \equiv \frac{1}{p^j} \binom{p^t}{ip^{t-j}} \pmod{p^{t-j+1}}.$$

Proof. Clearly $(X+1)^{p^{k-t}} = X^{p^{k-t}} + 1 + pf(X)$ for some $f \in \mathbb{Z}[X]$. The result follows from raising both sides to the p^t-th power.

For the second part, use the first part and Lemma 8.1 to compare the coefficients of $X^{ip^{k-j}}$ from $(X+1)^{p^k}$ and $(X^{p^{k-t}} + 1)^{p^t}$. □

We now introduce yet some more notation.

Definition 8.3. Let $0 < j \leq k$ and $i \in \{1, \ldots, p^j - 1\}$ with $p \nmid i$, and define $\mathbf{Bin}_{i,j,k} \overset{\text{def}}{=} -\frac{1}{p^j}\binom{p^k}{ip^{k-j}}$, $\mathbf{bin}_{i,j,k} \overset{\text{def}}{=} \xi_{k-j}(\mathbf{Bin}_{i,j,k})$, and $\mathrm{bin}_{i,j,k} \overset{\text{def}}{=} \pi(\mathbf{bin}_{i,j,k})$. (Remember π denotes the reduction modulo p.)

Lemma 8.4. *Let $0 < r < k$ and $i \in \{1, \ldots, p^r - 1\}$ with $p \nmid i$. We have that*

$$\mathbf{Bin}_{i,r,k} \equiv \sum_{l=0}^{k-r} \mathbf{bin}_{i,r,r+l}\, p^l \pmod{p^{k-r+1}}.$$

Proof. By Lemma 8.2, we have that $\mathbf{Bin}_{i,r,k} \equiv \mathbf{Bin}_{i,r,r+l} \pmod{p^{l+1}}$ for $0 \leq l < k - r$. Then,

$$\begin{aligned}\mathbf{Bin}_{i,r,k} \equiv \sum_{t=0}^{l} \xi_t(\mathbf{Bin}_{i,r,k})p^t &\equiv \sum_{t=0}^{l} \xi_t(\mathbf{Bin}_{i,r,r+l})p^t \\ &= \sum_{t=0}^{l-1} \xi_t(\mathbf{Bin}_{i,r,r+l})p^t + \mathbf{bin}_{i,r,r+l}\, p^l \pmod{p^{l+1}}.\end{aligned}$$

Thus, by the uniqueness of the representation, we have $\xi_l(\mathbf{Bin}_{i,r,k}) = \mathbf{bin}_{i,r,r+l}$ for $0 \leq l < k - r$. Since also $\xi_{k-r}(\mathbf{Bin}_{i,r,k}) = \mathbf{bin}_{i,r,k}$ by definition, the lemma follows. □

Definition 8.5. Let

$$(\mathcal{N}_{k,1}, \ldots, \mathcal{N}_{k,N_k}) = \operatorname{vec}\left(\sum_{j=1}^{k} \sum_{\substack{i=1 \\ p\nmid i}}^{p^j-1} \mathbf{bin}_{i,j,k} x_0^{ip^{k-j}} y_0^{p^k - ip^{k-j}} \right).$$

Inductively, for $k > 1$ and $l \in \{1, \ldots, (k-1)\}$, let $\mathcal{N}_{k,N_k+l} \overset{\text{def}}{=} \eta_l(\mathcal{N}_{k-l,1}, \ldots, \mathcal{N}_{k-l,N_{k-l}+k-l-1})$.

Also, let $\mathcal{N}_k \overset{\text{def}}{=} (\mathcal{N}_{k,1}, \ldots, \mathcal{N}_{k,N_k+k-1})$, $\bar{\mathcal{N}}_{k,i} \overset{\text{def}}{=} \pi(\mathcal{N}_{k,i}) \in \mathbb{F}_p[x_0, y_0]$, and $\bar{\mathcal{N}}_k \overset{\text{def}}{=} (\bar{\mathcal{N}}_{k,1}, \ldots, \bar{\mathcal{N}}_{k,N_k+k-1})$.

Theorem 8.6. *With the notation above, we have that*

$$\bar{\eta}_k(x_0, y_0) = \sum_{i=1}^{N_k+k-1} \bar{\mathcal{N}}_{k,i} = \sum_{j=1}^{k} \sum_{\substack{i=1 \\ p\nmid i}}^{p^j-1} \mathrm{bin}_{i,j,k} x_0^{ip^{k-j}} y_0^{p^k - ip^{k-j}} + \sum_{l=1}^{k-1} \bar{\eta}_l(\bar{\mathcal{N}}_{k-l}).$$

Remark 8.7. Note that

$$\begin{aligned}\sum_{j=1}^{k} \sum_{\substack{i=1 \\ p\nmid i}}^{p^j-1} \mathrm{bin}_{i,j,k} x_0^{ip^{k-j}} y_0^{p^k - ip^{k-j}} &= \sum_{i=1}^{p^k-1} \pi\left(\xi_k\left(-\binom{p^k}{i}\right)\right) x_0^i y_0^{p^k-i} \\ &= \sum_{i=1}^{p^k-1} \pi\left(\xi_{\mathrm{v}_p(i)}\left(-\frac{1}{p^{k-\mathrm{v}_p(i)}}\binom{p^k}{i}\right)\right) x_0^i y_0^{p^k-i}.\end{aligned}$$

Proof. We prove the theorem by induction on k. The case $k = 1$ is trivial.

Assume now that the statement is true for any integer from 1 to $(k-1)$. We then have, by the induction hypothesis and using Eq. (5.2), that

$$\begin{aligned}\eta_k(\boldsymbol{x},\boldsymbol{y}) &= \frac{\boldsymbol{x}^{p^k}+\boldsymbol{y}^{p^k}-(\boldsymbol{x}+\boldsymbol{y})^{p^k}}{p^k} - \sum_{j=1}^{k-1}\frac{\eta_j(\boldsymbol{x},\boldsymbol{y})^{p^{k-j}}}{p^{k-j}} \\ &= \sum_{j=1}^{k}\frac{1}{p^{k-j}}\sum_{\substack{i=1\\ p\nmid i}}^{p^j-1}\mathbf{Bin}_{i,j,k}\boldsymbol{x}^{ip^{k-j}}\boldsymbol{y}^{p^k-ip^{k-j}} - \sum_{j=1}^{k-1}\left(\sum_{r=1}^{N_j+j-1}\frac{\mathcal{N}_{j,r}^{p^{k-j}}}{p^{k-j}} - \sum_{l=1}^{k-j}\frac{\eta_l(\mathcal{N}_j)^{p^{k-j-l}}}{p^{k-j-l}}\right).\end{aligned}$$

We also have by definition of $\mathcal{N}_{j,r}$ that

$$\sum_{r=1}^{N_j+j-1}\frac{\mathcal{N}_{j,r}^{p^{k-j}}}{p^{k-j}} = \frac{1}{p^{k-j}}\left(\sum_{r=1}^{j}\sum_{\substack{i=1\\ p\nmid i}}^{p^r-1}\mathbf{bin}_{i,r,j}^{p^{k-j}}\boldsymbol{x}^{ip^{k-r}}\boldsymbol{y}^{p^k-ip^{k-r}} + \sum_{l=1}^{j-1}\eta_l(\mathcal{N}_{j-l})^{p^{k-j}}\right).$$

Also, note that, again by definition, we have $\eta_l(\mathcal{N}_{j-l}) = \mathcal{N}_{j,N_j+l}$ and

$$\sum_{l=1}^{k-j}\frac{\eta_l(\mathcal{N}_j)^{p^{k-j-l}}}{p^{k-j-l}} = \sum_{t=j+1}^{k}\frac{\eta_{t-j}(\mathcal{N}_j)^{p^{k-t}}}{p^{k-t}} = \sum_{t=j+1}^{k}\frac{\mathcal{N}_{t,N_t+t-j}^{p^{k-t}}}{p^{k-t}}.$$

Thus, we get

$$\begin{aligned}\eta_k(\boldsymbol{x},\boldsymbol{y}) = \sum_{j=1}^{k}\sum_{\substack{i=1\\ p\nmid i}}^{p^j-1}\frac{\mathbf{Bin}_{i,j,k}}{p^{k-j}}\boldsymbol{x}^{ip^{k-j}}\boldsymbol{y}^{p^k-ip^{k-j}} &- \sum_{j=1}^{k-1}\sum_{r=1}^{j}\sum_{\substack{i=1\\ p\nmid i}}^{p^r-1}\frac{\mathbf{bin}_{i,r,j}^{p^{k-j}}}{p^{k-j}}\boldsymbol{x}^{ip^{k-r}}\boldsymbol{y}^{p^k-ip^{k-r}} \\ &- \sum_{j=1}^{k-1}\sum_{l=1}^{j-1}\frac{\mathcal{N}_{j,N_j+l}^{p^{k-j}}}{p^{k-j}} + \sum_{j=1}^{k-1}\sum_{t=j+1}^{k}\frac{\mathcal{N}_{t,N_t+t-j}^{p^{k-t}}}{p^{k-t}}. \end{aligned}\tag{8.2}$$

But,

$$\begin{aligned}&-\sum_{j=1}^{k-1}\sum_{l=1}^{j-1}\frac{\mathcal{N}_{j,N_j+l}^{p^{k-j}}}{p^{k-j}} + \sum_{j=1}^{k-1}\sum_{t=j+1}^{k}\frac{\mathcal{N}_{t,N_t+t-j}^{p^{k-t}}}{p^{k-t}} \\ &\qquad = -\sum_{j=2}^{k-1}\sum_{l=1}^{j-1}\frac{\mathcal{N}_{j,N_j+l}^{p^{k-j}}}{p^{k-j}} + \sum_{t=2}^{k}\sum_{j=1}^{t-1}\frac{\mathcal{N}_{t,N_t+t-j}^{p^{k-t}}}{p^{k-t}} = \sum_{j=1}^{k-1}\mathcal{N}_{k,N_k+k-j} = \sum_{j=1}^{k-1}\mathcal{N}_{k,N_k+j}.\end{aligned}\tag{8.3}$$

Also,

$$
\begin{aligned}
&\sum_{j=1}^{k}\sum_{\substack{i=1\\p\nmid i}}^{p^j-1}\frac{\mathbf{Bin}_{i,j,k}}{p^{k-j}}\boldsymbol{x}^{ip^{k-j}}\boldsymbol{y}^{p^k-ip^{k-j}}-\sum_{j=1}^{k-1}\sum_{r=1}^{j}\sum_{\substack{i=1\\p\nmid i}}^{p^r-1}\frac{\mathbf{bin}_{i,r,j}^{p^{k-j}}}{p^{k-j}}\boldsymbol{x}^{ip^{k-r}}\boldsymbol{y}^{p^k-ip^{k-r}}\\
&\qquad=\sum_{j=1}^{k}\sum_{\substack{i=1\\p\nmid i}}^{p^j-1}\frac{\mathbf{Bin}_{i,j,k}}{p^{k-j}}\boldsymbol{x}^{ip^{k-j}}\boldsymbol{y}^{p^k-ip^{k-j}}-\sum_{r=1}^{k-1}\sum_{\substack{i=1\\p\nmid i}}^{p^r-1}\left(\sum_{j=r}^{k-1}\frac{\mathbf{bin}_{i,r,j}}{p^{k-j}}\right)\boldsymbol{x}^{ip^{k-r}}\boldsymbol{y}^{p^k-ip^{k-r}} \qquad (8.4)\\
&\qquad=\sum_{\substack{i=1\\p\nmid i}}^{p^k-1}\mathbf{Bin}_{i,k,k}\boldsymbol{x}^{i}\boldsymbol{y}^{p^k-i}+\sum_{r=1}^{k-1}\sum_{\substack{i=1\\p\nmid i}}^{p^r-1}\left(\frac{\mathbf{Bin}_{i,r,k}}{p^{k-r}}-\sum_{j=r}^{k-1}\frac{\mathbf{bin}_{i,r,j}}{p^{k-j}}\right)\boldsymbol{x}^{ip^{k-r}}\boldsymbol{y}^{p^k-ip^{k-r}}.
\end{aligned}
$$

Now, applying Lemma 8.4,

$$\frac{\mathbf{Bin}_{i,r,k}}{p^{k-r}}-\sum_{j=r}^{k-1}\frac{\mathbf{bin}_{i,r,j}}{p^{k-j}}=\frac{1}{p^{k-r}}\left(\mathbf{Bin}_{i,r,k}-\sum_{l=0}^{k-r-1}\mathbf{bin}_{i,r,r+l}\,p^l\right)\equiv\mathbf{bin}_{i,r,k}\pmod{p}.$$

Since also $\mathbf{Bin}_{i,k,k}\equiv\mathbf{bin}_{i,k,k}\pmod{p}$, Eq. (8.4) is congruent modulo p to

$$\sum_{r=1}^{k}\sum_{\substack{i=1\\p\nmid i}}^{p^r-1}\mathbf{bin}_{i,r,k}\boldsymbol{x}^{ip^{k-r}}\boldsymbol{y}^{p^k-ip^{k-r}}=\sum_{i=1}^{N_k}\mathcal{N}_{k,i}.$$

Together with Eqs. (8.2) and (8.3), this gives the desired result. □

Theorem 8.6 gives an algorithm, made explicit as Algorithm 2 below, that allows us to compute $\bar{\eta}_k(a_1,\ldots,a_n)$ directly in characteristic p, except for the $\mathrm{bin}_{i,j,k}$, and without having to pre-compute or store in memory any auxiliary polynomials.

It should be noted Algorithm 2, as described, computes some terms many times over, due to the numerous recursions involved. One could probably improve it by storing the terms which will be needed later, but this is not entirely trivial. One could also just save all terms which have been computed, which might be wasteful, but could save some computing time. But, although there is certainly room for improvement, Algorithm 2 can still be useful, as one can see in the examples in Section 9.

9. Some Concrete Computations

In this section we show how the methods from the previous sections yield great improvements in some concrete examples. The computer used was a Dell Precision 690 server with two dual-core 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 (64 bit). The software used in the computations was MAGMA (versions 2.16-6 and 2.16-11). More examples can be

Algorithm 2 Compute $(\mathcal{M}_1(a_1,\dots,a_n),\dots,\mathcal{M}_k(a_1,\dots,a_n))$, given $\mathrm{bin}_{i,j,k}$ for $j \in \{1,\dots,k\}$, $i \in \{1,\dots p^j-1\} \setminus p\mathbb{Z}$.

```
function V-ETAS-P($v = (a_1,\dots,a_n)$, $k$)
    if $n = 1$ then
        return $(0,\dots,0)$
    end if
    if $n = 2$ then
        $R \leftarrow ()$                                                      ▷ result
        for $t \leftarrow 1, k$ do
            $R[t] \leftarrow (\mathrm{bin}_{i,j,t}\, a_1^{ip^{t-j}} a_2^{p^t - ip^{t-j}} \ : \ j \in \{1,\dots,t\}$ and $i \in \{1,\dots,p^j-1\} \setminus p\mathbb{Z})$
        end for
        for $t = 1, k-1$ do
            $T \leftarrow$ V-ETAS-P$(R, k-t)$                                   ▷ temp. var.
            for $s = 1, k-t$ do
                append $T[s]$ to $R[t+s]$
            end for
        end for
        return $R$
    end if
    $m \leftarrow \lfloor n/2 \rfloor$
    $v_1 \leftarrow (a_1,\dots,a_m)$
    $v_2 \leftarrow (a_{m+1},\dots,a_n)$
    $s_1 \leftarrow a_1 + \cdots + a_m$
    $s_2 \leftarrow a_{m+1} + \cdots + a_n$
    $x_1 \leftarrow$ V-ETAS-P$((a_1,\dots,a_m), k)$
    $x_2 \leftarrow$ V-ETAS-P$((a_{m+1},\dots,a_n), k)$
    $x_3 \leftarrow$ V-ETAS-P$((s_1, s_2), k)$
    $R \leftarrow ()$                                                          ▷ result
    for $i \leftarrow 1$, $k$ do                            ▷ add first three entries to all $\mathcal{M}_i$
        $R[i] \leftarrow (x_1[i], x_2[i], x_3[i])$
    end for
    for $i \leftarrow 2$, $k$ do                                   ▷ add the remaining entries
        $T \leftarrow$ V-ETAS-P$(R[i-1], k-i+1)$                               ▷ temp. var.
        for $t \leftarrow i$, $k$ do
            append $T[t-i+1]$ to $R[t]$
        end for
    end for
    return $R$
end function
```

found at [Fin10a] in the case of length 3, where the formulas and algorithms are particularly simpler.

As we have seen there are two ways to compute $\bar{\eta}_k(a_1,\dots,a_r)$: using Algorithm 1, in which we first have to compute and store the needed $\bar{\eta}_i$'s, or using Algorithm 2, in which we just need to compute and store the $\mathrm{bin}_{i,j,k}$, which is much faster and requires much less memory.

As a first example, for $p = 11$ we've computed S_3 using the recursive formula (2.4) and using Proposition 7.1 with Algorithm 1. The former took approximately 130.56 hours, while the latter took approximately 7.20 hours. The computation of $\bar{\eta}_i(X, Y)$ for $i = 1, 2, 3$, necessary for this second method, takes only 0.19 seconds in this case.

The 24 gigabytes of memory available were not enough to compute S_4 with either method. On the other hand, we do not need S_4 to add Witt vectors with our new methods. Using Proposition 7.1, we can add Witt vectors using the $\bar{\eta}_i$'s. For instance, we can add two vectors in $\boldsymbol{W}_6(\mathbb{F}_{11^{10}})$ in about a second (on average) using Algorithm 1, after we spend approximately 3.61 hours to compute the $\bar{\eta}_i(X, Y)$ for $i \in \{1, 2, 3, 4, 5\}$. (Although this might seem as long time, remember that it took 7.20 hours to compute S_3 and we cannot even compute S_4 with the memory available.) Using Algorithm 2, we need only 5.750 seconds to compute the necessary $\mathrm{bin}_{i,j,k}$ (from Theorem 8.6), but then it takes us about 26 seconds on average to add two Witt vectors in $\boldsymbol{W}_6(\mathbb{F}_{11^{10}})$. So, in this case Algorithm 2 would certainly be more efficient if we ones does not need too many additions.

Also, as observed in Section 3, one can evaluate a polynomial in two variables at a pair of Witt vectors directly using Theorem 6.4, thus avoiding computing sums and power of Witt vectors. Let then

$$\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{0 \leq i,j \leq d} \boldsymbol{a}_{i,j} \boldsymbol{x}^i \boldsymbol{x}^j \in \boldsymbol{W}_{n+1}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}] \tag{9.1}$$

and $\boldsymbol{x}_0, \boldsymbol{y}_0 \in \boldsymbol{W}_{n+1}(\Bbbk)$. Table 9.1 shows the time and memory usage in examples with $\boldsymbol{a}_{i,j}$'s, $\boldsymbol{x}_0$, and $\boldsymbol{y}_0$ randomly chosen in the finite field $\Bbbk$ with the two approaches, i.e., performing the sums and products of Witt vectors and using the formula for the Greenberg transform. *Note that the addition and multiplication of Witt vectors performed in these tests were done in the improved way described above*, i.e., using the $\bar{\eta}_i$'s instead of computing the S_i's and P_i's. We've used Algorithm 1 for both, and it should also be observed that the times to compute the $\bar{\eta}_i$'s (for $i \leq n$), which are then used in both methods, are shown separately in Table 9.1.

As observed above, there are more efficient methods to perform operation with Witt vector over finite fields, namely, by identifying $\boldsymbol{W}_{n+1}(\mathbb{F}_q)$ with $\mathbb{Z}_q/p^{n+1}$, as observed in Section 1 and made explicit in Section 2. If it then seems somewhat artificial to use Witt vector over finite fields in our examples, note that the running time of the algorithm basically depends on the number of operations in the field (or ring) of the entries of the Witt vector, and therefore these examples give an idea of how these new methods require fewer operations. In the case of, say, polynomial rings, the operations will demand a lot more time, but

				Sum and Prod.		GT form.	
$\Bbbk$	n	d	$\bar{\eta}_i$ time (sec)	time (sec)	mem. (MB)	time (sec)	mem. (MB)
$\mathbb{F}_{3^{10}}$	9	20	108.78	433.31	12.22	130.28	16.40
$\mathbb{F}_{7^{10}}$	6	20	3554.78	2410.49	28.00	600.23	28.62
$\mathbb{F}_{11^{10}}$	5	20	5794.89	3564.62	37.44	839.37	30.88
$\mathbb{F}_{13^{10}}$	5	15	29854.75	4608.84	70.63	1045.08	49.00
$\mathbb{F}_{19^{10}}$	4	15	2760.36	2301.17	32.44	983.08	26.72

TABLE 9.1. Times and memory usages to evaluate random $\boldsymbol{f} \in \boldsymbol{W}_{n+1}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$, where $\deg_{\boldsymbol{x}} \boldsymbol{f}, \deg_{\boldsymbol{y}} \boldsymbol{f} \leq d$, at random $(\boldsymbol{x}_0, \boldsymbol{y}_0)$.

Characteristic	time (in sec.)	memory usage (in MB)
7	7.300	40.97
11	421.09	1010.03
13	6542.590	4175.28

TABLE 9.2. Times and memory usages to compute J_3.

one can expect comparable improvements in relative terms. (It will also be more efficient in terms of memory!) Choosing finite fields for these tests allowed us to have some quick examples, as computations can take a long time and a lot of memory in other examples.

In any event, we now provide some examples over different rings. As an example over polynomial rings, we computed the Greenberg transform of a polynomial as in Eq. (9.1) with $\Bbbk = \mathbb{F}_3$, $n = 3$, and $d = 5$, again with coefficients $\boldsymbol{a}_{i,j}$'s randomly chosen. In this case, using sums and products of Witt vectors (with $\boldsymbol{x} = (x_0, x_1, x_2, x_3)$ and $\boldsymbol{y} = (y_0, y_1, y_2, y_3)$, where x_i and y_j are indeterminates) the computation took 6590.43 seconds and used 636.44 megabytes of memory. On the other hand, using the formula for the Greenberg, it took 359.07 seconds and used 255.59 megabytes of memory. So, the gains are even more significant in this case.

Another example would be the one mentioned in Section 4. As mentioned there, using simply the polynomials for sums and products of Witt vectors, we could only compute J_3 for $p = 5$. (Remember that the J_i's are the rational functions such that given an ordinary j-invariant j_0, the j-invariant of its canonical lifting is $(j_0, J_1(j_0), J_2(j_0), \ldots)$. This computation involves computing the Greenberg transform of the modular polynomial.) This computation took 407.089 seconds and used 376.78 megabytes of memory. Now, with Theorem 6.4 above, we can compute J_3 in 0.480 seconds and using only 21.28 megabytes, and we could compute some new examples. The time and memory usage for these are shown in Table 9.2. (The case of $p = 17$ used over 24 gigabytes of memory and therefore crashed still incomplete.) In particular, these computations were useful to show that Conjecture 10.1 from [Fin10a] holds $p = 11$, i.e., J_3 has a pole of order 11^2 at zero in this case.)

It should be also noted that these computations of the J_3's can be improved by studying what happens with the Greenberg transform of $\Phi_p(X, Y)$ when evaluated at $((x_0, \dots, x_3), (x_0^p, \dots, x_3^p))$, as likely many of the terms that appear will vanish, as happens for J_2. (See Theorem 5.5 and Table 5.1 of [Fin10c].) These improvements come from analyzing the fourth coordinate of the Greenberg transform in this particular case, and therefore Theorem 6.4 was crucial.

Thus, despite still often requiring a lot of resources, the results presented here can still yield considerable improvements over previous methods. The MAGMA routines that were used on the tests presented here, including implementations of Algorithm 1 and Algorithm 2, are available at the time of writing at

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

Acknowledgment. The author would like to thank the *Centre de Recherches Mathématiques* for the hospitality and during the preparation of this manuscript.

References

[Deu41] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenköper. *Abh. Math. Sem. Univ. Hamburg*, 14:197–272, 1941.

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

[Fin10a] L. R. A. Finotti. Computations with Witt vectors of length 3. To appear at the "Journal de Théorie des Nombres de Bordeaux". Available at `http://www.math.utk.edu/~finotti/`, 2010.

[Fin10b] L. R. A. Finotti. Lifting the j-invariant: Questions of Mazur and Tate. *J. Number Theory*, 130(3):620 – 638, 2010.

[Fin10c] L. R. A. Finotti. Nonexistence of pseudo-canonical liftings. Submitted. Available at `http://www.math.utk.edu/~finotti/`, 2010.

[Gre61] M. J. Greenberg. Schemata over local rings. *Ann. of Math. (2)*, 73:624–648, 1961.

[Jac84] N. Jacobson. *Basic Algebra*, volume 2. W. H. Freeman and Company, second edition, 1984.

[KZ98] 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.

[Lan52] S. Lang. On quasi algebraic closure. *Ann. of Math. (2)*, 55:373–390, 1952.

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

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

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