Computational Aspects of Mixed Characteristic Witt Vectors

Jacob Dennerlein

April 12, 2023

Abstract. The ring of p-Witt vectors is typically difficult to study computationally, as the sum and product polynomials grow exponentially in both the prime p and the index n. However, some isomorphisms are known, e.g. $\boldsymbol{W}(\mathbb{F}_q)$ for $q = p^r$ is isomorphic the unique unramified extension of the p-adic integers of degree r. In this paper, we find an analogous result for $\mathbb{Z}/p^\alpha\mathbb{Z}$, including an explicit isomorphism that is computationally useful.

1 Introduction

One of the original motivation for Witt vectors was to provide an isomorphic ring for the p-adic integers that was (in some sense) easier to work with mathematically. While initially the components of the vectors came from finite fields, it turned out that this ring structure could be extended to *any* commutative ring R. However, the calculations for sums and products involve large polynomials (see Definition 2.2 and Definition 2.3 below), which, even on modern computers, heavily restricts the calculations that one can do.

However, we can take advantage of various known isomorphisms, e.g. the p-adic integer isomorphism, to perform these calculations much faster. Finotti also made great strides in [Fin14] to speed up calculations for any base ring of characteristic p, not just finite fields. Our goal in this paper is to study the structure of Witt vectors over arbitrary commutative rings to attempt to find other (computationally useful) isomorphisms. Some such isomorphisms are already known, e.g. for rings where p is a unit. See [Rab14] for more information.

We start by computing the characteristic of the Witt ring in Section 3. Then, in Section 4 we find a way to split the Witt ring into two components if the base ring is not of characteristic zero. Finally, in the last three sections, we build up an explicit isomorphism for the Witt vectors over $\mathbb{Z}/p^\alpha\mathbb{Z}$.

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 many sources such as Hazewinkel's [Haz09] and Borger's [Bor11]. A more friendly introduction can be found in Rabinoff's notes [Rab14]. We start with the following definition.

Definition 2.1. Fix a prime p. Then for each $n \in \mathbb{Z}_{\geq 0}$, the nth *Witt polynomial* is

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

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

Definition 2.2. The *Witt sum polynomials* are $S_i \in \mathbb{Z}[X_0, \ldots, X_i, Y_0, \ldots, Y_i]$, where the S_i are inductively defined by

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

More explicitly,

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

Definition 2.3. The *Witt product polynomials* are $P_i \in \mathbb{Z}[X_0, \ldots, X_i, Y_0, \ldots, Y_i]$, where the P_i are inductively defined by

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

More explicitly,

$$P_n = \frac{1}{p^n}\left[(X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - \left(P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p\right)\right]. \tag{2}$$

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

Definition 2.4. Let R be a commutative ring (with 1) and let p be a prime. *The ring of p-Witt vectors over R* is defined to be the set $R^{\mathbb{Z}_{\geq 0}}$ equipped with the following operations. Let $\boldsymbol{a} = (a_0, a_1, \ldots)$ and $\boldsymbol{b} = (b_0, b_1, \ldots)$. Then

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

and

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

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

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

Definition 2.5. Let R and p be as above and let $n \in \mathbb{N}$. *The ring of p-Witt vectors over R of length n* is defined to be the set R^n equipped with the operations in Definition 2.4 truncated to length n. This makes R^n into a commutative ring (with 1). When p is clear from context, we denote this ring by $\boldsymbol{W}_n(R)$ and call it *the ring of Witt vectors over R of length n*. Otherwise, we denote it by $\boldsymbol{W}_{p,n}(R)$, which is again non-standard.

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

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

Proposition 2.6. *Let R be a commutative ring, p a prime, and $n \in \mathbb{N} \cup \{\infty\}$. Then*

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

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

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

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

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

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

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

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

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

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

Definition 2.7. The *Verschiebung map* on $\boldsymbol{W}(\Bbbk)$ is the map $V : \boldsymbol{W}(R) \to \boldsymbol{W}(R)$ defined by

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

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

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

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

Definition 2.8. The Frobenius map on $\boldsymbol{W}(R)$ is the map $F : \boldsymbol{W}(R) \to \boldsymbol{W}(R)$ defined by

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

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

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

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

Normally, the Frobenius is a map from a ring to itself, which *is* the case for $\boldsymbol{W}(R)$, but not for $\boldsymbol{W}_n(R)$. To further illustrate this, we compute the first couple f_i. Firstly, $w_0 \circ F = w_1$ gives $f_0(X_0, X_1) = X_0^p + pX_1$. Then we have $w_1 \circ F = w_2$, which gives

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

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

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

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

Proposition 2.9. *Let $\boldsymbol{a} \in \boldsymbol{W}(R)$. Then*

1. $F(V(\boldsymbol{a})) = p \cdot \boldsymbol{a}$.

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

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

3 The Characteristic of the Witt Ring

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

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

Proposition 3.1. *Given $c \in \mathbb{Z}$, the image of c in $\boldsymbol{W}_{p,\infty}(R)$ is given by $\boldsymbol{c} = (\overline{c_0}, \overline{c_1}, \overline{c_2}, \ldots)$, where $c_0, c_1, c_2, \ldots \in \mathbb{Z}$ are defined as follows:*

$$c_0 = c$$

and

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

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

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

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

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

So the formulas are correct for c = 1.

Now, let $c > 1$ and suppose the formulas are correct for $c - 1$. For the sake of notation, let $d = c - 1$. Then we have $\boldsymbol{c} = \boldsymbol{d} + \mathbf{1}$. So we apply the Witt sum, i.e., we have

$c_n = S_n(d_0, \ldots, d_n, 1, 0, \ldots, 0)$ for all $n \geq 0$.

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

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

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

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

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

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

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

Then, inductively, we have

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

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

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

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

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

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

$$b = \sum_{i=0}^{n} p^i b_i^{p^{n-i}} \tag{3}$$

so the expression above simplifies to

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

finishing the proof. □

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

Proposition 3.2. *Let $N = char(R)$ and suppose $p \mid N$. Let $v = v_p(N)$. Let $\boldsymbol{N}$ be the image of N in $\boldsymbol{W}_{p,\infty}(R)$. Then for all $j \geq 0$ we have*

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

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

Proof. First, note that this is clearly true for $N = 0$. So assume $N > 0$. We start with $j = 0$ and apply the Proposition 3.1. Firstly, we have $N_0 = N \equiv 0 \pmod{N}$ and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Corollary 3.3. *Let $N = char(R)$ and suppose $p \mid N$. Then $char(\boldsymbol{W}_{p,n}(R)) = p^{n-1}N$ and $char(\boldsymbol{W}_{p,\infty}(R)) = 0$.*

Proof. If $N = 0$, then $\mathbb{Z} \hookrightarrow R$. So for any $c \in \mathbb{Z}$, taking $\boldsymbol{c} = (\overline{c_0}, \overline{c_1}, \ldots)$ as in Proposition 3.1, we have $\overline{c_0} \neq 0$. Thus $\text{char}(\boldsymbol{W}_{p,n}(R)) = 0$ for all $n \in \mathbb{N} \cup \{\infty\}$, which shows the corollary is true for $N = 0$. So let $N > 0$ and let $N_{i,j}$ be as in Proposition 3.2.

We first show that $\dfrac{N}{p}N_{1,j} \not\equiv 0 \pmod{N}$ for all j. Let $M = p^jN$. Let $\boldsymbol{M} = (M_0, M_1, \ldots)$ as in Proposition 3.1. Then we have

$$\frac{N}{p}N_{1,j} = M_{j+1} = \frac{1}{p^{j+1}}\left[M - \sum_{i=0}^{j} p^i M_i^{p^{j+1-i}}\right] = \frac{N}{p} - \sum_{i=0}^{j} \frac{M_i^{p^{j+1-i}}}{p^{j+1-i}}. \tag{4}$$

Since $\boldsymbol{M} = p^j\boldsymbol{N}$, by Proposition 3.2, we have that $M_i \equiv 0 \pmod{N}$ for all $0 \leq i \leq j$, so we can write $M_i = c_iN$ for some $c_i \in \mathbb{Z}$. Letting $N' = N/p$, we have $M_i = c_ipN'$. Then for $k \geq 0$,

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

Since $p^k - k \geq 1$ for all $k \geq 0$, we have $M_i^{p^k}/p^k \equiv 0 \pmod{N}$. So Equation (4) simplifies to

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

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

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

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

Since $p \nmid c$, we can never have $\dfrac{cN}{p} \equiv 0 \pmod{N}$, since we'll always be missing a factor of p. This shows two things. Firstly, every multiple of $\boldsymbol{N}$ has a non-zero component, which proves $\text{char}(\boldsymbol{W}_{p,\infty}(R)) = 0$. Secondly, the number of zeroes at the beginning of $\boldsymbol{nN}$ is exactly $v_p(n) + 1$. So the smallest integer that maps to 0 in $\boldsymbol{W}_{p,n}(R)$ must be $p^{n-1}N$. □

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

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

and

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

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

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

Proposition 4.1. *Let I be an ideal of R. Thenfor all $n \in \mathbb{N} \cup \{\infty\}$,*

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

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

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

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

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

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

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

Lemma 4.2. *Let* $p, \alpha, M \in \mathbb{Z}_{>0}$ *with* p *prime and* $p \nmid M$. *Let* $a, b \in \mathbb{Z}$ *such that* $ap^\alpha + bM = 1$. *Then for all* $i \geq 0$,

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

Proof. We have

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

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

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

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

Theorem 4.3. *Let R be a commutative ring of characteristic $N > 0$. Write $N = p^\alpha M$ with $p \nmid M$. Then, for all $n \in \mathbb{N} \cup \{\infty\}$,*

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

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

Now we apply a similar argument to $\boldsymbol{W}_{p,n}(R)$. Since $I \cap J = (0)$, we get by construction that $\boldsymbol{W}_{p,n}(I) \cap \boldsymbol{W}_{p,n}(J) = (0)$. If we show that $\boldsymbol{W}_{p,n}(I)$ and $\boldsymbol{W}_{p,n}(J)$ are coprime, we'll have, by the Chinese Remainder Theorem and Proposition 4.1,

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

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

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

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

By Lemma 4.2, $(ap^\alpha)^p + (bM)^p \equiv 1 \pmod{p^{\alpha+1}M}$, which gives $S_1 \equiv 0 \pmod{p^\alpha M}$. Now inductively assume $S_j \equiv 0 \pmod{p^\alpha M}$ for all $j < i$. We have

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

Again by Lemma 4.2, we have that $p^{-i}[(ap^\alpha)^{p^i} + (bM)^{p^i} - 1] \equiv 0 \pmod{p^\alpha M}$. Also, since $S_{i-j} \equiv 0 \pmod{p^\alpha M}$ and $j < p^j$, we have that $p^{-j}S_{i-j}^{p^j} \equiv 0 \pmod{p^\alpha M}$. So $S_i \equiv 0 \pmod{p^\alpha M}$ as well, proving the claim and finishing the proof of the theorem. □

The isomorphism here is hiding in the details of the proof. Combining the isomorphisms from the Chinese Remainder Theorem and Proposition 4.1, we get the explicit form

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

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

Theorem 4.4. *Take R as in Theorem 4.3 and let $a, b \in \mathbb{Z}$ such that $ap^\alpha + bM = 1$. Take ϕ as above and define*

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

Then ϕ and ψ are inverses.

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

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

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

$$\begin{aligned}
&\psi((a_0, a_1, \ldots) \oplus (b_0, b_1, \ldots)) \\
&= ((ap^\alpha)a_0 + (bM)b_0, (ap^\alpha)a_1 + (bM)b_1, \ldots) \\
&= ((ap^\alpha)(a'_0 + k_0 M) + (bM)(b'_0 + \ell_0 p^\alpha), (ap^\alpha)(a'_1 + k_1 M) + (bM)(b'_1 + \ell_1 p^\alpha), \ldots) \\
&= ((ap^\alpha)a'_0 + (bM)b'_0 + (ak_0 + b\ell_0)p^\alpha M, (ap^\alpha)a'_1 + (bM)b'_1 + (ak_1 + b\ell_1)p^\alpha M, \ldots) \\
&= ((ap^\alpha)a'_0 + (bM)b'_0, (ap^\alpha)a'_1 + (bM)b'_1, \ldots) \text{ since } \mathrm{char}(R) = p^\alpha M \\
&= \psi((a'_0, a'_1, \ldots) \oplus (b'_0, b'_1, \ldots)).
\end{aligned}$$

Therefore ψ is well-defined. Now we compute

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

and

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

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

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

Corollary 4.5. *Take R as in Theorem 4.3. Then*

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

Proof. Since $\operatorname{char}(R/MR) = M$, and $p \nmid M$, $p \in (R/MR)^\times$. So by [Rab14] Remark 2.5, which is restated in Proposition 2.6, $\boldsymbol{W}_{p,n}(R/MR) \cong (R/MR)^n$ via $(w_0, w_1, \ldots)$. □

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

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

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

with multiplication given by

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

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

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

Theorem 5.1. *For all $n \in \mathbb{N}$, the additive group of $\boldsymbol{W}_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/p^{n+\alpha-1}\mathbb{Z}) \oplus (\mathbb{Z}/p^{\alpha-1}\mathbb{Z})^{n-1}$.*

By Corollary 3.3, we know the first piece is the image of $\mathbb{Z}$, and so is generated by one. So we will start by constructing elements of order $\alpha - 1$, then prove that these elements do in fact generate subgroups with trivial intersection. After that, we will show that these elements have "nice" multiplicative properties and use these properties to construct an isomorphism that is computationally useful.

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

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

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

$$\sum_{j=0}^{i} p^j g_j^{p^{i-j}} = 0. \tag{5}$$

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

Lemma 5.2. *The g_i defined above are integers and $\nu_p(g_i) = p^i - p^{i-1} - \cdots - p - 1$.*

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

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

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

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

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

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

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

and so

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

which is positive, proving both statements in the lemma. □

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

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

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

Lemma 5.3. *For any* $c \in \mathbb{Z}$, $\boldsymbol{c}\gamma_i = (\underbrace{0, \ldots, 0}_{i-1 \textit{ zeroes}}, cg_0, c^p g_1, c^{p^2} g_2, \ldots)$.

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

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

So we consider

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

This last equality comes from Equation (3). Now, for $j \geq i$, we have

$$\begin{aligned}P_j(\boldsymbol{c},\gamma_i) &= \frac{1}{p^j}\left[(c_0^{p^j}+\cdots+p^j c_j)(\underbrace{p^{i-1}g_0^{j-(i-1)}+\cdots+p^j g_{j-(i-1)}}_{=0 \text{ by Equation (5)}}) - \sum_{k=i-1}^{j-1}p^k P_k^{p^{j-k}}\right]\\ &= -\frac{1}{p^j}\sum_{k=i-1}^{j-1}p^k P_k^{p^{j-k}}\end{aligned}$$

Then inductively we have

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

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

Proposition 5.4. *For each i, the additive order of γ_i is $p^{\alpha-1}$.*

Proof. By the above Lemma 5.3, for any $c \in \mathbb{Z}$, the component at index $i-1$ is $cg_0 = cp$. For any $c < p^{\alpha-1}$, $cp \not\equiv 0 \pmod{p^\alpha}$. So $|\gamma_i| \geq p^{\alpha-1}$. Now, letting $c = p^{\alpha-1}$, we have $cp \equiv 0 \pmod{p^\alpha}$. Also, since $p^i(\alpha-1) \geq \alpha$ for all $i \geq 1$, we have that $c^{p^i} \equiv 0 \pmod{p^\alpha}$. So each component of $\boldsymbol{c}\gamma_i$ is 0, and thus $|\gamma_i| = p^{\alpha-1}$. □

We've shown that the γ's have the correct order, so now we need to show that $\langle\gamma_i\rangle$ has trivial intersection with the integers and the groups generated by the other γ_j. We can see right away that for $i \neq j$, $\langle \gamma_i \rangle \cap \langle \gamma_j \rangle = \{0\}$: Lemma 5.3 shows that the first non-zero component of respective elements occur at different indices. So we only need to show that the intersection with the integers is trivial. For this, we again need another lemma.

Lemma 5.5. *Let $c \in \mathbb{Z}$ with $c \neq 0$. Let $\beta = \nu_p(c)$ and define the c_i as in Proposition 3.1. Then for $i \in \{0, \ldots, \beta\}$, $\nu_p(c_i) = \beta - i$.*

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

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

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

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

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

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

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

Proposition 5.6. *For all i, $\langle \gamma_i \rangle \cap \langle 1 \rangle = \{0\}$.*

Proof. Suppose $m = c\gamma_i$ for some non-zero $m, c \in \mathbb{Z}$. Then by Lemma 5.3, we have $m = (0, \ldots, 0, cg_0, c^p g_1, \ldots)$ where $m_{i-1} = cg_0$, $m_i = c^p g_1$ and so on. Since $m_0, \ldots, m_{i-2}$ are all equivalent to 0 (mod p^α), we get that $\nu_p(m_0), \ldots, \nu_p(m_{i-2}) \geq \alpha$. Also, since $c^p g_0 \neq 0$, we have that $\nu_p(m_{i-1}) < \alpha$. Applying Lemma 5.5, we must have that $\nu_p(m_{i-2}) = \alpha$, which gives that $\nu_p(m) = \alpha + i - 2$ and $\nu_p(m_{i-1}) = \alpha - 1$.

Now, let $\beta = \nu_p(c)$. Since $m \neq 0$ and $|\gamma_i| = p^{\alpha-1}$, we get that $\beta < \alpha - 1$. We also get that $\alpha - 1 = \nu_p(m_{i-1}) = \beta + 1$. Using Lemma 5.2, we get

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

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

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

Proof of Theorem 5.1. From Corollary 3.3, we have that $|1| = p^{\alpha+n-1}$. From Proposition 5.4, we have that $|\gamma_1| = \cdots = |\gamma_{n-1}| = p^{\alpha-1}$. Furthermore, these elements generate subgroups whose pairwise intersections are always zero. So we have

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

But also

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

which completes the proof. □

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

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

Proposition 6.1. *For $i \neq j$, $\gamma_i \gamma_j = 0$.*

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

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

Since $k > i$, the first factor inside the brackets is $p^{i-1}\sum_{\ell=0}^{k-i+1} p^\ell g_\ell^{p^{k-i+1-\ell}}$, which is 0 by Equation (5). This holds for all $k \geq j$, so each $P_k = 0$. Thus $\gamma_i\gamma_j = 0$. □

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

Proposition 6.2. *For all i, $\gamma_i^2 = p^i\gamma_i$.*

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

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

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

$$P_k(\gamma_i, \gamma_i) = \frac{1}{p^k}\left[\underbrace{(p^{i-1}g_0^{p^{k-i+1}} + \cdots + p^k g_{k-i+1})}_{=0 \text{ by Equation (5)}}{}^2 - (p^i P_i^{p^{k-i}} + \cdots + p^{k-1}P_{k-1}^p)\right]$$
$$= -\frac{1}{p^k}\sum_{j=i-1}^{k} p^j P_j^{k-j}$$

Now we turn our attention to $p^i\gamma_i$. From Lemma 5.3, we have that the first non-zero component is also $p^i g_0$. Then we can perform the same computation as above and the first term inside the brackets will *again* be zero by Equation (5). So the resulting expression has exactly the same form. That is, inductively, for $k \geq i$, we have

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

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

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

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

This *greatly* simplifies the multiplication compared to using the product polynomials. We can also see from the formula that it's not quite component-wise multiplication, but it's close: the only coefficient that is affecting the other components is the integer part at the start. As far as the authors can tell (through computer testing), this seems unavoidable.

That is, there seems to be no alternative choice for γ_i where the multiplication can be done component-wise.

7 The Coefficients of γ_i

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

Theorem 7.1. *Let $\boldsymbol{v} \in \boldsymbol{W}_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$. Define $c_0 = w_{n-1}(\boldsymbol{v})$ and for $i \in \{1, \dots, n-1\}$, $c_i = p^{-i}(w_{i-1}(\boldsymbol{v}) - c_0)$, where w_j is the jth Witt polynomial. Then, with the γ_i defined as above,*

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

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

As with the g_i in Section 5, by construction, these c_i are rational numbers with denominators divisible by p. However, we want $c_i \in \mathbb{Z}/p^{\alpha-1}\mathbb{Z}$, and so we need denominators *not* divisible by p. For this, we have the following lemma.

Lemma 7.2. *The c_i defined in Theorem 7.1 are integers for all $\boldsymbol{v} \in \boldsymbol{W}_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$.*

Proof. We consider the numerator of c_i,

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

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

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

Since $i < n$, we have, by Fermat's Little Theorem, $v_j^{p^{n-i}-1} \equiv 1 \mod p$, since $(p-1) \mid (p^{n-i}-1)$. Then, by Lemma 1.4 of [Rab14], this gives $v_j^{p^{(i-1)-j}(p^{n-i}-1)} \equiv 1 \mod p^{i-j}$. So $p^{i-j} \mid \left(1 - v_j^{p^{(i-1)-j}(p^{n-i}-1)}\right)$, and thus p^i divides the entire term because we're multiplying by p^j at the front. Therefore p^i divides every term in the numerator, and so c_i is an integer. □

So we know it makes sense to use these c_i as the coefficients. Before we prove Theorem 7.1, we need the following lemma about what happens when we add an element of $\langle \gamma_i \rangle$ to an arbitrary Witt vector.

Lemma 7.3. *Let $\boldsymbol{v} = (v_0, \ldots, v_{n-1}) \in \boldsymbol{W}_{p,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$ and let $c \in \mathbb{Z}$. Define $\boldsymbol{w} = (w_0, \ldots, w_{n-1}) = \boldsymbol{v} + c\gamma_i$. Then $w_j = v_j$ for $0 \leq j < i-1$, $w_{i-1} = v_{i-1} + cp$, and for $j \geq i$,*

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

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

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

Since $g_0 = p$, this shows the first two of the three statements in the lemma. So now we let

$j \geq i$ and consider

$$\begin{aligned}
w_j &= S_j(\boldsymbol{v}, c\gamma_i) \\
&= v_j + c^{p^{j-(i-1)}} g_{j-(i-1)} + \sum_{k=1}^{j-(i-1)} \frac{1}{p^k} \left(v_{j-k}^{p^k} + (c^{p^{j-(i-1)-k}} g_{j-(i-1)-k})^{p^k} - w_{j-k}^{p^k} \right) \\
&= v_j + \sum_{k=1}^{j-(i-1)} \frac{1}{p^k} \left(v_{j-k}^{p^k} - w_{j-k}^{p^k} \right) + \sum_{k=0}^{j-(i-1)} \frac{1}{p^k} (c^{p^{j-(i-1)-k}} g_{j-(i-1)-k})^{p^k} \\
&= v_j + \sum_{k=1}^{j-(i-1)} \frac{1}{p^k} \left(v_{j-k}^{p^k} - w_{j-k}^{p^k} \right) + \frac{c^{p^{j-(i-1)}}}{p^{j-(i-1)}} \underbrace{\sum_{k=0}^{j-(i-1)} p^{j-(i-1)-k} g_{j-(i-1)-k}^{p^k}}_{0 \text{ by Equation (5)}} \\
&= v_j + \sum_{k=i-1}^{j-1} \frac{1}{p^{j-k}} \left(v_k^{p^{j-k}} - w_k^{p^{j-k}} \right). \qquad \square
\end{aligned}$$

This is the final tool we need to prove Theorem 7.1.

Proof of Theorem 7.1. For the sake of notation, let $\boldsymbol{a_0} = (a_{0,0}, \ldots, a_{0,n-1}) := \boldsymbol{c_0}$. Then, for $i \in 1, \cdots, n-1$, recursively define

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

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

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

Our goal is to show that $\boldsymbol{a_{n-1}} = \boldsymbol{v}$. By Lemma 7.3, we have

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

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

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

since the first $i-1$ components of $c_i\gamma_i$ are 0. Then, repeatedly using Lemma 7.3, we have

$$\begin{aligned}
a_{i,i-1} &= S_{i-1}(\boldsymbol{a_{i-1}}, c_i\gamma_i) \\
&= a_{i-1,i-1} + pc_i \\
&= S_{i-1}(\boldsymbol{a_{i-2}}, c_{i-1}\gamma_{i-1}) + pc_i \\
&= a_{i-2,i-1} + \sum_{k=i-2}^{i-2} \frac{1}{p^{(i-1)-k}} \left(a_{i-2,k}^{p^{(i-1)-k}} - a_{i-1,k}^{p^{(i-1)-k}} \right) + pc_i \\
&= a_{i-3,i-1} + \sum_{m=i-3}^{i-2} \sum_{k=m}^{i-2} \frac{1}{p^{(i-1)-k}} \left(a_{m,k}^{p^{(i-1)-k}} - a_{m+1,k}^{p^{(i-1)-k}} \right) + pc_i \\
&= \vdots \\
&= a_{0,i-1} + \sum_{m=0}^{i-2} \sum_{k=m}^{i-2} \frac{1}{p^{(i-1)-k}} \left(a_{m,k}^{p^{(i-1)-k}} - a_{m+1,k}^{p^{(i-1)-k}} \right) + pc_i \\
&= a_{0,i-1} + \sum_{k=0}^{i-2} \frac{1}{p^{(i-1)-k}} \underbrace{\sum_{m=0}^{k} \left(a_{m,k}^{p^{(i-1)-k}} - a_{m+1,k}^{p^{(i-1)-k}} \right)}_{\text{telescoping}} + pc_i \\
&= a_{0,i-1} + \sum_{k=0}^{i-2} \frac{1}{p^{(i-1)-k}} \left(a_{0,k}^{p^{(i-1)-k}} - a_{k+1,k}^{p^{(i-1)-k}} \right) + pc_i \\
&= \sum_{k=0}^{i-1} \frac{1}{p^{(i-1)-k}} a_{0,k}^{p^{(i-1)-k}} + pc_i - \sum_{k=0}^{i-2} \frac{1}{p^{(i-1)-k}} a_{k+1,k}^{p^{(i-1)-k}} \\
&= \frac{1}{p^{i-1}} \left[\sum_{k=0}^{i-1} p^k a_{0,k}^{p^{(i-1)-k}} - c_0 + w_{i-1}(\boldsymbol{v}) - \sum_{k=0}^{i-2} p^k a_{k+1,k}^{p^{(i-1)-k}} \right] \\
&= \frac{1}{p^{i-1}} \left[a_{0,0} - c_0 + p^{i-1} v_{i-1} \right] = v_{i-1}.
\end{aligned}$$

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

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

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

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

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

and the final component is given by

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

References

[Bor11] James Borger. The basic geometry of Witt vectors, I: The affine case. Algebra Number Theory, 5(2):231–285, 2011. 1

[DK14] Christopher Davis and Kiran S. Kedlaya. On the Witt vector Frobenius. Proc. Amer. Math. Soc., 142(7):2211–2226, 2014. 5, 6, 10

[Fin14] Luís R. A. Finotti. Computations with Witt vectors and the Greenberg transform. Int. J. Number Theory, 10(6):1431–1458, 2014. 1, 13

[Haz09] Michiel Hazewinkel. Witt vectors. I. In Handbook of algebra. Vol. 6, volume 6 of Handb. Algebr., pages 319–472. Elsevier/North-Holland, Amsterdam, 2009. 1

[Hes15] Lars Hesselholt. The big de Rham–Witt complex. Acta mathematica, 214(1):135–207, 2015. 17

[Rab14] Joseph Rabinoff. The Theory of Witt Vectors, 2014. 1, 3, 4, 6, 10, 12, 13, 17, 26

Acknowledgements

I'd like to thank Dr. Luís Finotti for his guidance and suggestions and for spending so much of his time listening to my ramblings and reviewing my writing. I would also like to thank Dr. Christopher Davis for reviewing some of my work and pointing me in the direction of relevant results.