On the Structure of Witt-Burnside Rings Attached to Pro-p Groups

Lance Edward Miller

Received: April 1, 2013

Communicated by Lars Hesselholt

Abstract. The p-typical Witt vectors are a ubiquitous object in algebra and number theory. They arise as a functorial construction that takes perfect fields k of prime characteristic $p > 0$ to p-adically complete discrete valuation rings of characteristic 0 with residue field k and are universal in that sense. A. Dress and C. Siebeneicher generalized this construction by producing a functor $\mathbf{W}_G$ attached to any profinite group G. The p-typical Witt vectors arise as those attached to the p-adic integers. Here we examine the ring structure of $\mathbf{W}_G(k)$ for several examples of pro-p groups G and fields k of characteristic p. We will show that the structure is surprisingly more complicated than the p-typical case.

1 Introduction

The purpose of this article is to explore what kinds of rings lie in the image of the functors $\mathbf{W}_G$ introduced by A. Dress and C. Siebeneicher [DS88] in the case that G is a pro-p group for prime integer p. These functors were originally defined for all profinite groups and are now called Witt-Burnside functors due to the fact that they generalize both the p-typical (recovered when $G = \mathbf{Z}_p$ as an additive group) and 'big' Witt vector construction (recovered when $G = \widehat{\mathbf{Z}}$), as well as Burnside functors (recovered as $\mathbf{W}_G(\mathbf{Z})$). We call rings lying in the image of a Witt-Burnside functor *Witt-Burnside rings.* These functors are of significant interest, and yet to date the types of rings which are produced from this construction lack description. To illustrate some of their recent importance, we remark that Witt-Burnside functors have been used extensively to study equivariant ring spectra as they arise as a left adjoint for Tambara functors [Bru05, Bru07, Str].

Many constructions of Witt-Burnside functors have been given. Specifically, J. Graham's construction utilizes ring valued G-sets [Gra93]. J. Elliott gave a unified construction relating the Graham and Dress and Siebeneicher approaches [Ell06]. Y. Oh has studied some decomposition and q-deformation questions [Oh09, Oh07, Oh12]. Beyond the classical $G = \mathbf{Z}_p$ case, not much about the ring structure of the images of Witt-Burnside functors is known. Motivated by the extensive applications enjoyed by the p-typical and big Witt vectors, this paper addresses structural questions about Witt-Burnside rings under the assumptions that G is an infinite pro-p group and k is a field of characteristic $p > 0$.

The construction of the classical (both p-typical and big) Witt vectors uses the Witt polynomials to define certain addition and multiplication polynomials with rational coefficients which do not obviously have integral coefficients [Wit36]. A. Dress and C. Siebeneicher generalized the Witt polynomials to a family of multivariable polynomials associated to any profinite group G. Like classical Witt polynomials, these polynomials obviously have $\mathbf{Q}$-coefficients and a significant theorem of Dress and Siebeneicher shows that they in fact have integral coefficients. Thus one can use these polynomials, in an analogous way to the construction of classical Witt vectors, to define a functor $\mathbf{W}_G$ on the category of commutative rings for each profinite group G. For infinite pro-p groups G, the functor $\mathbf{W}_G$ retains the surprising property of taking rings of characteristic p to rings of characteristic 0.

For perfect fields k of characteristic p, the ring $\mathbf{W}_{\mathbf{Z}_p}(k)$ is the ring of classical p-typical Witt vectors. These are p-adically complete discrete valuation domains with maximal ideal (p) and residue field k. From [DS88, Thm. 2] it is known that $\mathbf{W}_G(k)$ is a ring of characteristic zero when $G \ncong \mathbf{Z}_p$ is an infinite pro-p group and k is a field. We show as expected that $\mathbf{W}_G(k)$ shares some properties with the p-typical case when G is pro-p and k has characteristic p.

Theorem (Cf., Theorem 2.16) *For G a pro-p group and A a local ring of characteristic $p > 0$, $\mathbf{W}_G(A)$ is a local ring.*

However, the similarities do not run deep!

Theorem (Cf., Theorem 4.5) *For $G = \mathbf{Z}_p^d$, k a field of characteristic $p > 0$ and $d \geq 2$, the maximal ideal of $\mathbf{W}_G(k)$ is not finitely generated, so $\mathbf{W}_G(k)$ is not Noetherian.*

The core reason for the complication in the case $G = \mathbf{Z}_p^d$ when $d \geq 2$ versus $d = 1$ is the existence of more than one maximal subgroup. In general, when G is any pro-p group that is not pro-cyclic there is more than one maximal open subgroup H, necessarily normal. These subgroups describe certain coordinates in the Witt vectors attached to G for which sums and products have repeated values, or redundencies. In particular, $G = \mathbf{Z}_p^d$ has a fairly homogeneous subgroup structure as every open subgroup is (non-canonically) isomorphic to G. This means the redundancy behavior when $d \geq 2$ propagates and manifests as a much smaller square of the maximal ideal than expected. Another consequence of there being more than one maximal subgroup of an infinite pro-p group G when $G \not\cong \mathbf{Z}_p$ is the ability to construct zero divisors. This was essentially known in [DS88]. Our second main goal is to give some control on the zero divisors of $\mathbf{W}_G(k)$ for $G = \mathbf{Z}_p^2$ and k a field of characteristic p.

Theorem (Cf., Theorem 5.17) *For $G = \mathbf{Z}_p^2$ and any field k of characteristic p, the ring $\mathbf{W}_G(k)$ is reduced.*

The methods used here fail for $d > 2$ due to the reliance on a certain property of the subgroup structure of $\mathbf{Z}_p^2$ which is not satisfied more generally.
The rest of the paper is organized as follows. Section 2 develops the preliminary definitions, constructions, and facts about Witt-Burnside rings. We also prove necessary lemmas for the paper and close with the proof that $\mathbf{W}_G(A)$ is local when G is pro-p and A is a local ring of characteristic p. Section 3 discusses in detail the frame of $\mathbf{Z}_p^d$ for $d \geq 2$; these groups form the basic examples of the paper. Section 4 discusses the failure of finite generation in the maximal ideal $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ for $d \geq 2$ when the characteristic of k is p. Finally, Section 5 concerns nilpotent elements in $\mathbf{W}_G(k)$. Unless otherwise stated, G will always be a profinite group and p denotes a prime integer.

2 Preliminaries

Witt-Burnside rings are constructed utilizing generalized Witt polynomials associated to a profinite group G. The index set of these generalized polynomials is the set of isomorphism classes of discrete finite transitive G-sets, called the *frame* of G and denoted $\mathcal{F}(G)$. For example, $\mathcal{F}(\mathbf{Z}_p) = \mathbf{N}$ by the correspondence $\mathbf{Z}_p/p^n\mathbf{Z}_p \leftrightarrow n$. There is a natural partial ordering on $\mathcal{F}(G)$. For T and U in $\mathcal{F}(G)$ we say $U \leq T$ if there is a G-map from T to U. Denote the set of all G-maps from T to U as $\mathrm{Map}_G(T, U)$ and the number of G-maps $\#\mathrm{Map}_G(T, U)$ by $\varphi_T(U)$. Thus $\varphi_T(U) \neq 0$ if and only if $T \leq U$. We summarize some facts about $\mathcal{F}(G)$

1. If T and U in $\mathcal{F}(G)$ with $U \leq T$, then $\#U$ divides $\#T$ and $\#T/\#U$ represents the size of any of the fibers of any element of $\mathrm{Map}_G(T, U)$.
2. If the stabilizer subgroups of the points in T are all equal (we will say in this case that T has normal stabilizers or that T is a normal G-set), then $\varphi_T(U) = \#U$ for $U \leq T$.
3. For each T in $\mathcal{F}(G)$, there are only finitely many U in $\mathcal{F}(G)$ with $U \leq T$.

The elements of $\mathcal{F}(G)$ have a concrete description. Every finite transitive G-set T is isomorphic to some coset space G/H with left G-action, where H is an open subgroup of G that can be chosen as the stabilizer subgroup of any point in T. The partial order $\leq$ on coset spaces (considered as G-sets up to isomorphism) can be described concretely by $G/K \leq G/H$ if and only if H is conjugate to a subgroup of K (or equivalently, H is a subgroup of a conjugate of K).

For $T \in \mathcal{F}(G)$, define the T-th *Witt polynomial* to be

$$W_T(\{X_U\}_{U\in\mathcal{F}(G)}) = \sum_{U\leq T} \varphi_T(U) X_U^{\#T/\#U} = X_0^{\#T} + \ldots + \varphi_T(T)X_T, \qquad (1)$$

where 0 denotes the trivial G-set G/G. Trivially $\varphi_T(0) = 1$ for all T in $\mathcal{F}(G)$. This is a finite sum since there are only finitely many $U \leq T$. For instance, if $G = \mathbf{Z}_p$ then the finite transitive G-sets up to isomorphism are $\mathbf{Z}_p/p^n\mathbf{Z}_p$ for $n \geq 0$ and the Witt polynomial associated to $\mathbf{Z}_p/p^n\mathbf{Z}_p$ is the classical n-th p-typical Witt polynomial.

One may gauge the complexity of a given frame by looking at the covering relations. In any partially ordered set, one says that U covers T if $T \leq U$ and there are no elements in between. In the frame of $\mathbf{Z}_p$ each element has exactly one cover and the frame is linearly ordered. Figure 1 displays the frame of $\mathbf{Z}_2^2$. When $G = \mathbf{Z}_p^2$, all G-sets have $p+1$ covers. Other than the trivial G-set, each G-set below the horizontal line in Figure 1 has p covers also below the horizontal line. This line is not part of the frame and depicts a property about the stabilizers of various G-sets described in Definition 5.1.

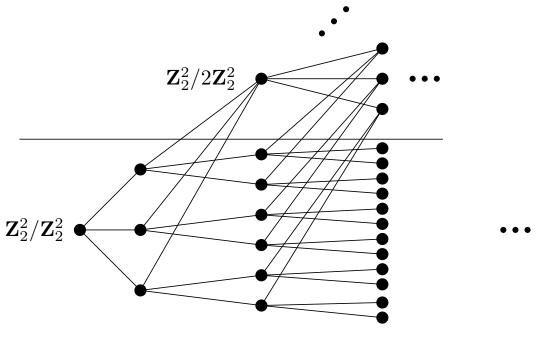
$\mathbf{Z}_2^2/2\mathbf{Z}_2^2$
$\mathbf{Z}_2^2/\mathbf{Z}_2^2$

Figure 1: The frame $\mathcal{F}(\mathbf{Z}_2^2)$.

Remark 2.1. *The picture in Figure 1 is reminiscent of the tree of* $\mathbf{Z}_2$*-lattices in* $\mathbf{Q}_2^2$ *up to scaling, on which* $\mathrm{PGL}_2(\mathbf{Q}_2)$ *acts [Ser77, p. 71]. However, it is different since the* G*-sets* $\mathbf{Z}_2^2/2^r\mathbf{Z}_2^2$ *appear as separate vertices in Figure 1, while the subgroups* $2^r\mathbf{Z}_2^2$ *all correspond to the same vertex in the tree for* $\mathrm{PGL}_2(\mathbf{Q}_2)$.

To simplify notation, write a tuple of variables X_T indexed by all T in $\mathcal{F}(G)$ as $\underline{X}$, e.g., $W_T(\{X_U\}_{U\in\mathcal{F}(G)}) = W_T(\underline{X})$, $\mathbf{Z}[\{X_T\}_{T\in\mathcal{F}(G)}] = \mathbf{Z}[\underline{X}]$, and $\mathbf{Z}[\{X_T, Y_T\}_{T\in\mathcal{F}(G)}] = \mathbf{Z}[\underline{X}, \underline{Y}]$. This underline notation of course depends on G. For any commutative ring A, a polynomial $f(\underline{X}) \in \mathbf{Z}[\underline{X}]$ defines a function from $\prod_{T\in\mathcal{F}(G)} A$ to A, and for a tuple $\mathbf{a} = (a_T)_{T\in\mathcal{F}(G)}$ with coordinates in A

we write $f(\mathbf{a}) = f(\{a_T\}_{T\in\mathcal{F}(G)}) \in A$. A similar meaning is applied to $f(\mathbf{a},\mathbf{b})$ for a polynomial $f(\underline{X},\underline{Y}) \in \mathbf{Z}[\underline{X},\underline{Y}]$. Generally, we write sequences indexed by $\mathcal{F}(G)$ as bold letters (*e.g.*, $\mathbf{a},\mathbf{b},\mathbf{x},\mathbf{y},\mathbf{v}$) and their T-th coordinate is in italics (*e.g.*, a_T, b_T, x_T, y_T, v_T).

Because X_T appears on the right side of (1) just in the linear term $\varphi_T(T)X_T$, and all variables which appear in other terms are X_U for $U < T$, we get the following uniqueness criterion for all the Witt polynomial values together which is equivalent to Lemma 2.1 in [Ell06, p. 331].

Theorem 2.2. *If A is a commutative ring which has no $\varphi_T(T)$-torsion for any $T \in \mathcal{F}(G)$, then the function $\prod_{T\in\mathcal{F}(G)} A \to \prod_{T\in\mathcal{F}(G)} A$ given by $\mathbf{a} \mapsto (W_T(\mathbf{a}))_{T\in\mathcal{F}(G)}$ is injective. This function is bijective provided each $\varphi_T(T)$ is a unit in A.*

Example 2.3. *If G is a pro-p group and $T \cong G/H$, then $\varphi_T(T) = [\mathrm{N}_G(H) : H]$ is a power of p, so if p is invertible in A then every $\mathbf{a} \in \prod_{T\in\mathcal{F}(G)} A$ has the form $(W_T(\mathbf{b}))_{T\in\mathcal{F}(G)}$ for a unique $\mathbf{b} \in \prod_{T\in\mathcal{F}(G)} A$.*

The most important application of Theorem 2.2 is to the ring $A = \mathbf{Q}[\underline{X},\underline{Y}]$ and the vectors $(W_T(\underline{X})+W_T(\underline{Y}))_{T\in\mathcal{F}(G)}$ and $(W_T(\underline{X})W_T(\underline{Y}))_{T\in\mathcal{F}(G)}$. It tells us there are unique families of polynomials $\{S_T(\underline{X},\underline{Y})\}$ and $\{M_T(\underline{X},\underline{Y})\}$ in $\mathbf{Q}[\underline{X},\underline{Y}]$ satisfying

$$W_T(\underline{X}) + W_T(\underline{Y}) = W_T(\underline{S}) \text{ for all } T \in \mathcal{F}(G)$$

and

$$W_T(\underline{X})W_T(\underline{Y}) = W_T(\underline{M}) \text{ for all } T \in \mathcal{F}(G).$$

More explicitly, this says

$$\sum_{U\le T} \varphi_T(U)X_U^{\#T/\#U} + \sum_{U\le T} \varphi_T(U)Y_U^{\#T/\#U} = \sum_{U\le T} \varphi_T(U)S_U^{\#T/\#U} \qquad (2)$$

and

$$\left(\sum_{U\le T} \varphi_T(U)X_U^{\#T/\#U}\right)\left(\sum_{U\le T} \varphi_T(U)Y_U^{\#T/\#U}\right) = \sum_{U\le T} \varphi_T(U)M_U^{\#T/\#U} \qquad (3)$$

for all T. The polynomials S_T and M_T each only depend on the variables X_U and Y_U for $U \le T$.

A significant theorem of Dress and Siebeneicher [DS88, p. 107], which generalizes Witt's theorem ($G = \mathbf{Z}_p$), says that the polynomials S_T and M_T have coefficients in $\mathbf{Z}$. We call the S_T's and M_T's the Witt addition and multiplication polynomials, respectively. (Obviously they depend on G, but that dependence will not be part of the notation).

Example 2.4. *Taking $T = 0$, one has*

$$S_0(\underline{X}, \underline{Y}) = X_0 + Y_0 \text{ and } M_0(\underline{X}, \underline{Y}) = X_0 Y_0.$$

If $T \cong G/H$ where H is a maximal open subgroup, so $\{U \in \mathcal{F}(G) \colon U \leq T\}$ is just $\{0, T\}$ solving for S_T and M_T in (2) and (3) yields

$$S_T = X_T + Y_T + \frac{(X_0 + Y_0)^{\#T} - X_0^{\#T} - Y_0^{\#T}}{\varphi_T(T)},$$

$$M_T = X_0^{\#T} Y_T + X_T Y_0^{\#T} + \varphi_T(T) X_T Y_T.$$

Compare with the first two classical Witt addition and multiplication polynomials in [Ser79, p. 42]. Further addition and multiplication polynomials could be very complicated to write out explicitly, as is already apparent for the classical Witt vectors if you try to go past the first two polynomials.

Since S_T and M_T have integral coefficients, they can be evaluated on any ring, including rings where the hypotheses of Theorem 2.2 break down, like a ring of characteristic p when G is a pro-p group.

Definition 2.5. *Let G be a profinite group. For any commutative ring A, define the Witt–Burnside ring $\mathbf{W}_G(A)$ to be the product space $\prod_{T \in \mathcal{F}(G)} A$ as a set, with elements written as $\mathbf{a} = (a_T)_{T \in \mathcal{F}(G)}$. The ring operations on $\mathbf{W}_G(A)$ are defined using the Witt addition and multiplication polynomials:*

$$\mathbf{a} + \mathbf{b} = (S_T(\mathbf{a}, \mathbf{b}))_{T \in \mathcal{F}(G)}$$

and

$$\mathbf{a} \cdot \mathbf{b} = (M_T(\mathbf{a}, \mathbf{b}))_{T \in \mathcal{F}(G)}.$$

The additive (resp. multiplicative) identity is $(0, 0, 0, \dots)$ (resp. $(1, 0, 0, \dots)$).

We remark that $\mathbf{W}_G(A) = \varprojlim_N \mathbf{W}_{G/N}(A)$ where the inverse limit runs over open normal subgroups of G and, that giving each $\mathbf{W}_{G/N}(A)$ the discrete topology induces a natural profinite topology on $\mathbf{W}_G(A)$ in which $\mathbf{W}_G(A)$ is complete, which follows from the proof of [DS88, Thm 3.3.2], see also [Ell06, pg. 357]. Even when G is not abelian, $\mathbf{W}_G(A)$ is a commutative ring. For $G = \mathbf{Z}_p$, the addition and multiplication polynomials are the classical p-typical Witt addition and multiplication polynomials and $\mathbf{W}_{\mathbf{Z}_p}(A)$ is the p-typical Witt vectors.

For any ring homomorphism $f \colon A \to B$ define $\mathbf{W}_G(f) \colon \mathbf{W}_G(A) \to \mathbf{W}_G(B)$ by applying f to the coordinates:

$$\mathbf{W}_G(f)(\mathbf{a}) = (f(a_T))_{T \in \mathcal{F}(G)} \in \mathbf{W}_G(B).$$

This is a ring homomorphism and makes $\mathbf{W}_G$ a covariant functor from commutative rings to commutative rings.

Packaging all the Witt polynomials together, we get a ring homomorphism $W : \mathbf{W}_G(A) \to \prod_{T\in\mathcal{F}(G)} A$ which is W_T in the T-th coordinate:

$$W(\mathbf{a}) = (W_T(\mathbf{a}))_{T\in\mathcal{F}(G)} = \left(\sum_{U\leq T} \varphi_T(U) a_U^{\#T/\#U}\right)_{T\in\mathcal{F}(G)}.$$

This homomorphism is called the *ghost map* and its coordinates $W_T(\mathbf{a})$ are called the *ghost components* of $\mathbf{a}$. In some cases it is quite useless: if G is pro-p and A has characteristic p then $W(\mathbf{a}) = (a_0^{\#T})_{T\in\mathcal{F}(G)}$, whose dependence on $\mathbf{a}$ only involves a_0. If A fits the hypothesis of Theorem 2.2 then the ghost map is injective (i.e., the ghost components of $\mathbf{a}$ determine $\mathbf{a}$). Also from Theorem 2.2 the ghost map is bijective if every integer $\varphi_T(T)$ is invertible in A so $\mathbf{W}_G(A) \cong \prod_{T\in\mathcal{F}(G)} A$ by the ghost map. That means $\mathbf{W}_G(A)$ is a new kind of ring only if some $\varphi_T(T)$ is not invertible in A, and especially if A has $\varphi_T(T)$-torsion for some T (e.g., G is a nontrivial pro-p group and A has characteristic p).

The coordinates on which a Witt vector is nonzero is called its *support*. While the ring operations in $\mathbf{W}_G(A)$ are generally not componentwise, addition in $\mathbf{W}_G(A)$ is componentwise on two Witt vectors with disjoint support.

Theorem 2.6. *Let $\{R, S\}$ be a partition of $\mathcal{F}(G)$, i.e., $R \cup S = \mathcal{F}(G)$ and $R \cap S = \emptyset$. For every ring A and any $\mathbf{a} \in \mathbf{W}_G(A)$, define $\mathbf{r}(\mathbf{a})$ and $\mathbf{s}(\mathbf{a})$ to be the Witt vectors derived from $\mathbf{a}$ with support in R and S:*

$$\mathbf{r}(\mathbf{a}) = \begin{cases} a_T & \text{if } T \in R, \\ 0 & \text{if } T \in S, \end{cases} \quad \text{and} \quad \mathbf{s}(\mathbf{a}) = \begin{cases} 0 & \text{if } T \in R, \\ a_T & \text{if } T \in S. \end{cases}$$

Then $\mathbf{a} = \mathbf{r}(\mathbf{a}) + \mathbf{s}(\mathbf{a})$ in $\mathbf{W}_G(A)$.

Proof. First we will show the result in $\mathbf{W}_G(\mathbf{Z}[\underline{X}])$ for the particular Witt vector $\mathbf{x} = (X_T)_{T\in\mathcal{F}(G)}$: $\mathbf{x} = \mathbf{r}(\mathbf{x}) + \mathbf{s}(\mathbf{x})$ in $\mathbf{W}_G(\mathbf{Z}[\underline{X}])$. If we prove this then given any ring A and $\mathbf{a} \in \mathbf{W}_G(A)$, there is a ring homomorphism $f\colon \mathbf{Z}[\underline{X}] \to A$ such that $f(X_T) = a_T$ for all T, and applying the ring homomorphism $\mathbf{W}_G(f)\colon \mathbf{W}_G(\mathbf{Z}[\underline{X}]) \to \mathbf{W}_G(A)$ to the identity $\mathbf{x} = \mathbf{r}(\mathbf{x}) + \mathbf{s}(\mathbf{x})$ turns it into $\mathbf{a} = \mathbf{r}(\mathbf{a}) + \mathbf{s}(\mathbf{a})$.

Since $\mathbf{Z}[\underline{X}]$ is a domain of characteristic 0, the ghost map

$$W\colon \mathbf{W}_G(\mathbf{Z}[\underline{X}]) \to \prod_{T\in\mathcal{F}(G)} \mathbf{Z}[\underline{X}]$$

is an injective ring homomorphism, so it suffices to prove

$$W(\mathbf{x}) = W(\mathbf{r}(\mathbf{x}) + \mathbf{s}(\mathbf{x})).$$

The right side is $W(\mathbf{r}(\mathbf{x})) + W(\mathbf{s}(\mathbf{x}))$, which is a sum in the product ring

$\prod_{T\in\mathcal{F}(G)}\mathbf{Z}[\underline{X}]$, so its T-th coordinate for any T is

$$W_T(\mathbf{r}(\mathbf{x}))+W_T(\mathbf{s}(\mathbf{x}))=\sum_{\substack{U\leq T\\ U\in R}}\varphi_T(U)X_U^{\#T/\#U}+\sum_{\substack{U\leq T\\ U\in S}}\varphi_T(U)X_U^{\#T/\#U}.$$

Since $R\cup S=\mathcal{F}(G)$ and $R\cap S=\emptyset$, each U with $U\leq T$ will lie in exactly one of R or S, so

$$W_T(\mathbf{r}(\mathbf{x}))+W_T(\mathbf{s}(\mathbf{x}))=\sum_{U\leq T}\varphi_T(U)X_U^{\#T/\#U}=W_T(\mathbf{x}).$$

Therefore $W(\mathbf{r}(\mathbf{x})+\mathbf{s}(\mathbf{x}))$ and $W(\mathbf{x})$ have the same T-th component for all T, so they are equal, which shows $\mathbf{r}(\mathbf{x})+\mathbf{s}(\mathbf{x})=\mathbf{x}$. □

One typically proves an algebraic identity in $\mathbf{W}_G(A)$ by reformulating it as an identity in a ring of Witt vectors over a polynomial ring over $\mathbf{Z}$. From now on, we will usually prove the reformulation but may not go through the deduction of the identity we want over A from the identity proved over a polynomial ring; instead simply invoke functoriality.

Definition 2.7. *For $a\in A$ and $T\in\mathcal{F}(G)$, denote by $\omega_T(a)\in\mathbf{W}_G(A)$ the Witt vector with T-coordinate a and all other coordinates 0. We call $\omega_T(a)$ the T-th Teichmüller lift of a.*

We denote the trivial G-set G/G as 0 and by $\omega_0(a)$ the G/G-th Teichmüller lift. The function $\omega_0\colon A\to\mathbf{W}_G(A)$ generalizes the classical Teichmüller lift. Like the classical Teichmüller lift, ω_0 is multiplicative. For a general formula for $\omega_T(a)\omega_{T'}(b)$, see [Ell06, p. 355].
An easy consequence of Theorem 2.6 is that any Witt vector $\mathbf{a}$ of finite support satisfies $\mathbf{a}=\sum_{U\in\mathrm{Supp}(\mathbf{a})}\omega_U(a_U)$ where $\mathrm{Supp}(\mathbf{a})$ is the support of $\mathbf{a}$.

Theorem 2.8. *For any $a\in A$ and $\mathbf{b}\in\mathbf{W}_G(A)$,*

$$\omega_0(a)\mathbf{b}=(a^{\#T}b_T)_{T\in\mathcal{F}(G)}.$$

In particular, $\omega_0(a)\omega_0(b)=\omega_0(ab)$.

Proof. By functoriality, it suffices to show in $\mathbf{W}_G(\mathbf{Z}[\underline{X},\underline{Y}])$ that

$$(X_0,0,0,0,\ldots)(Y_T)_{T\in\mathcal{F}(G)}=(X_0^{\#T}Y_T)_{T\in\mathcal{F}(G)},$$

and to show this equation it suffices to prove the ghost components (Witt polynomial values) of both sides are equal. Since $W_T\colon\mathbf{W}_G(\mathbf{Z}[\underline{X},\underline{Y}])\to\mathbf{Z}[\underline{X},\underline{Y}]$ is multiplicative,

$$\begin{aligned}W_T((X_0,0,0,0,\ldots)(Y_U)_{U\in\mathcal{F}(G)}) &= W_T(X_0,0,0,0,\ldots)W_T((Y_U)_{U\in\mathcal{F}(G)})\\ &= X_0^{\#T}\sum_{U\leq T}\varphi_T(U)Y_U^{\#T/\#U}\end{aligned}$$

and

$$\begin{aligned} W_T((X_0^{\#U}Y_U)_{U\in\mathcal{F}(G)}) &= \sum_{U\le T}\varphi_T(U)(X_0^{\#U}Y_U)^{\#T/\#U} \\ &= \sum_{U\le T}\varphi_T(U)X_0^{\#T}Y_U^{\#T/\#U}. \end{aligned}$$

□

The Witt polynomial $W_T(\underline{X})$ becomes homogeneous of degree $\#T$ if we give X_U degree $\#U$ (e.g., X_0 has degree 1, not 0). This grading makes the addition and multiplication polynomials homogeneous as well.

Theorem 2.9. *Give the ring $\mathbf{Z}[\underline{X},\underline{Y}]$ the grading in which the degree of X_U and Y_U is $\#U$.*

(*a*) *For all T, the polynomial S_T is homogeneous of degree $\#T$ and M_T is homogeneous of degree $2\#T$.*

(*b*) *For all T, we have $S_T(\underline{X},\mathbf{0}) = X_T$, $S_T(\mathbf{0},\underline{Y}) = Y_T$, $M_T(\underline{X},\mathbf{0}) = 0$, and $M_T(\mathbf{0},\underline{Y}) = 0$.*

The second part of the theorem is saying S_T equals $X_T + Y_T$ plus monomials $X_U^iY_V^j$ where $U < T$ and $V < T$ (we cannot have $U = T$ or $V = T$ by homogeneity), while M_T contains no monomials that are pure $\underline{X}$-terms or pure $\underline{Y}$-terms.

Proof. (a) We will work out the homogeneity for M_T; the argument for S_T is similar. Clearly $M_0(X_0,Y_0) = X_0Y_0$, which is homogeneous of degree 2 and its only monomial term contains the factors X_0 and Y_0. Let $n \ge 2$ and assume by induction for all transitive G-sets U with $\#U < n$ that M_U is homogeneous of degree $2\#U$. Pick a transitive G-set T with $\#T = n$. (If there are no such G-sets then we are vacuously done.) Solving for M_T in (3) in $\mathbf{Q}[\underline{X},\underline{Y}]$,

$$\begin{aligned} M_T &= \frac{1}{\varphi_T(T)}\left(\sum_{U_1\le T}\varphi_T(U_1)X_{U_1}^{\frac{\#T}{\#U_1}}\sum_{U_2\le T}\varphi_T(U_2)Y_{U_2}^{\frac{\#T}{\#U_2}} - \sum_{U<T}\varphi_T(U)M_U^{\frac{\#T}{\#U}}\right) \\ &= \frac{1}{\varphi_T(T)}\left(\sum_{U_1,U_2\le T}\varphi_T(U_1)\varphi_T(U_2)X_{U_1}^{\frac{\#T}{\#U_1}}Y_{U_2}^{\frac{\#T}{\#U_2}} - \sum_{U<T}\varphi_T(U)M_U^{\frac{\#T}{\#U}}\right). \end{aligned}$$

By the inductive hypothesis, each M_U for $U < T$ is homogeneous of degree $2\#U$, so $M_U^{\#T/\#U}$ is homogeneous of degree $2\#T$. By the definition of the grading, $X_{U_1}^{\#T/\#U_1}$ has degree $\#T$ and $Y_{U_2}^{\#T/\#U_2}$ has degree $\#T$, so $X_{U_1}^{\#T/\#U_1}Y_{U_2}^{\#T/\#U_2}$ has degree $2\#T$.

(b) We will work out the result for multiplication polynomials. Since $M_0(\underline{X}, \mathbf{0})$ is $X_0 0 = 0$, we may assume $T \neq 0$. Set every Y_U to 0 in the recursive formula for M_T above. Then the formula tells us $M_T(\underline{X}, \mathbf{0})$ is equal to

$$\frac{1}{\varphi_T(T)} \left(\sum_{U_1, U_2 \leq T} \varphi_T(U_1)\varphi_T(U_2) X_{U_1}^{\#T/\#U_1} \cdot 0 - \sum_{U<T} \varphi_T(U) M_U(\underline{X}, \mathbf{0})^{\#T/\#U} \right).$$

Using the inductive hypothesis, each term is 0. □

So the polynomials $S_T(\{X_U^{\#U}, Y_U^{\#U}\}_{U\in\mathcal{F}(G)})$ are genuine homogeneous polynomials of degree $\#T$ (replace X_U and Y_U with their $\#U$-th powers everywhere), and similarly for the multiplication polynomials.

2.1 Units

The present goal is to demonstrate that $\mathbf{W}_G(k)$ is a local ring when G is pro-p and k is a field of characteristic p. We state a couple of needed lemmas about divisibility relationships among $\varphi_T(U)$ for $U, T \in \mathcal{F}(G)$ whose proofs are straightforward and left to the reader.

Lemma 2.10. *If G is a pro-p group and $T \geq U$ in $\mathcal{F}(G)$ with U nontrivial, then $\varphi_T(U) \equiv 0 \bmod p$.*

Lemma 2.11. *Let G be a nontrivial pro-p group, $U < T$ in $\mathcal{F}(G)$ and $s \in p\mathbf{Z}$. Then*

$$\frac{\varphi_T(U)}{\varphi_T(T)} s^{\#T/\#U} \in p\mathbf{Z}.$$

We apply these to study a particularly important family of ideals in $\mathbf{W}_G(A)$.

Definition 2.12. *For $n \in \mathbf{Z}^+$, set*

$$I_n(G, A) = \{\mathbf{a} \in \mathbf{W}_G(A) : a_T = 0 \textit{ for } \#T < n\}.$$

These are the Witt vectors $\mathbf{a}$ with support in $\{T : \#T \geq n\}$.

Lemma 2.13. *Each $I_n(G, A)$ is an ideal in $\mathbf{W}_G(A)$.*

Proof. Each addition polynomial S_T depends only on variables indexed by (isomorphism classes of) finite transitive G-sets $U \leq T$ and has no constant term by Theorem 2.9. So if two Witt vectors are in $I_n(G, A)$ then their sum is also in $I_n(G, A)$.

It remains to show for any $\mathbf{a} \in \mathbf{W}_G(A)$ and $\mathbf{b} \in I_n(G, A)$ that $\mathbf{ab} \in I_n(G, A)$. Set $\mathbf{c} = \mathbf{ab}$. By the definition of multiplication in $\mathbf{W}_G(A)$, $c_T = M_T(\mathbf{a}, \mathbf{b})$ for any T. If $\#T < n$, $b_U = 0$ for $U \leq T$ by hypothesis. Since $M_T(\underline{X}, \underline{Y})$ only depends on Y_U for $U \leq T$, $c_T = M_T(\mathbf{a}, \mathbf{b}) = M_T(\mathbf{a}, \mathbf{0})$ and $M_T(\mathbf{a}, \mathbf{0}) = 0$ by Theorem 2.9. □

Lemma 2.14. *Let G be a pro-p group. For all rings A of characteristic p and nonnegative integers n,*

$$I_p(G,A)I_{p^n}(G,A) \subset I_{p^{n+1}}(G,A)$$

in $\mathbf{W}_G(A)$.

Proof. If $n=0$ the result is clear since $I_1(G,A)=\mathbf{W}_G(A)$, so without loss of generality assume $n \geq 1$.

We will derive a mod p congruence for particular Witt vectors over the ring $R=\mathbf{Z}[\underline{X},\underline{Y}]$, which will be sufficient using functoriality. Define $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{W}_G(R)$ by

$$x_T = \begin{cases} 0, & \text{if } T = 0, \\ X_T, & \text{if } T \neq 0, \end{cases} \qquad \text{and} \qquad y_T = \begin{cases} 0, & \text{if } \#T < p^n, \\ Y_T, & \text{otherwise.} \end{cases}$$

Set $\mathbf{z}=\mathbf{xy}$. Our aim is to show

$$\#T < p^{n+1} \Longrightarrow z_T \equiv 0 \bmod pR. \tag{4}$$

We argue by induction on $\#T$. Clearly $z_0 = x_0y_0 = 0$. Let $\#T = p^r < p^{n+1}$ with $r \geq 1$ and assume by induction that for all $\#U < p^r$, $z_U \equiv 0 \bmod pR$. Since the T-th Witt polynomial is a multiplicative function $W_T \colon \mathbf{W}_G(R) \to R$, $W_T(\mathbf{z}) = W_T(\mathbf{x})W_T(\mathbf{y})$:

$$\sum_{U \leq T} \varphi_T(U) z_U^{\#T/\#U} = \sum_{T_1,T_2 \leq T} \varphi_T(T_1)\varphi_T(T_2) x_{T_1}^{\#T/\#T_1} y_{T_2}^{\#T/\#T_2}.$$

Solving this equation for z_T in $\mathbf{Q}[\underline{X},\underline{Y}]$,

$$z_T = \sum_{T_1,T_2 \leq T} \frac{\varphi_T(T_1)\varphi_T(T_2)}{\varphi_T(T)} x_{T_1}^{\#T/\#T_1} y_{T_2}^{\#T/\#T_2} - \sum_{U<T} \frac{\varphi_T(U)}{\varphi_T(T)} z_U^{\#T/\#U}. \tag{5}$$

Since $z_U \in pR$ for $U<T$, the second term in (5) is 0 mod pR by Lemma 2.11. In the first term in (5), we can assume $T_1 \neq 0$ since $x_0 = 0$. If $\#T_2 < p^n$ then $y_{T_2} = 0$, so we only need to consider T_2 where $\#T_2 \geq p^n$. Since $\#T < p^{n+1}$, $T_2 = T$. Then (5) becomes

$$z_T = \sum_{0<T_1 \leq T} \varphi_T(T_1) x_{T_1}^{\#T/\#T_1} y_T - \sum_{U<T} \frac{\varphi_T(U)}{\varphi_T(T)} z_U^{\#T/\#U}.$$

Since $\varphi_T(T_1)$ is an integral multiple of p by Lemma 2.10, $z_T \equiv 0 \bmod pR$. □

An immediate useful corollary follows.

Corollary 2.15. *For any pro-p group G and ring A of characteristic p, $I_p(G,A)^m \subset I_{p^m}(G,A)$.*

Proof. This follows directly from repeated applications of Lemma 2.14. □

We are now set to prove the main result of this section.

Theorem 2.16. *Let G be a pro-p group and A be a ring of characteristic p. The units in $\mathbf{W}_G(A)$ are $\mathbf{W}_G(A)^\times = \{\mathbf{a} : a_0 \in A^\times\}$. Consequently, when $(A, \mathfrak{n})$ is local, $\mathbf{W}_G(A)$ is a local ring with maximal ideal $\mathfrak{m} = \{\mathbf{a} \in \mathbf{W}_G(A) : a_0 \in \mathfrak{n}\}$.*

Proof. Obviously $\mathbf{W}_G(A)^\times \subset \{\mathbf{a} : a_0 \in A^\times\}$. To prove the reverse inclusion, let $\mathbf{a} \in \mathbf{W}_G(A)$ have $a_0 \in A^\times$. By Theorem 2.8 the Witt vector $(a_0, 0, 0, \dots)$ is a unit, with inverse $(a_0^{-1}, 0, 0, \dots)$, so it suffices to show $(a_0^{-1}, 0, 0, \dots)\mathbf{a}$ is a unit. The first coordinate of this product is 1, so we are reduced to showing a Witt vector with first coordinate 1 is a unit. That is, we can assume $a_0 = 1$. By Theorem 2.6,

$$\mathbf{a} = (1, 0, 0, \dots) + (0, \{a_T\}_{T \neq 0}) \in 1 + I_p(G, A).$$

Since $I_p(G, A)^m \subset I_{p^m}(G, A)$ by Corollary 2.15, we can invert $\mathbf{a}$ using a geometric series since $\mathbf{W}_G(A)$ is complete in the profinite topology. □

3 The Frame of $\mathbf{Z}_p^d$

The subgroup structure of $\mathbf{Z}_p^d$ is homogeneous in the sense that every open subgroup is isomorphic to $\mathbf{Z}_p^d$ (although there is not a canonical choice of isomorphism, unlike the case when $d = 1$). A subgroup is open if and only if it has finite index. If H is an open subgroup there is a $\mathbf{Z}_p$-basis $\{e_1, e_2, \dots, e_d\}$ for G such that $G = \mathbf{Z}_p e_1 \oplus \mathbf{Z}_p e_2 \oplus \cdots \oplus \mathbf{Z}_p e_d$ and $H = \mathbf{Z}_p p^{a_1} e_1 \oplus \mathbf{Z}_p p^{a_2} e_2 \oplus \cdots \oplus \mathbf{Z}_p p^{a_d} e_d$ for some $a_1, \dots, a_d \geq 0$. The G-set G/H has the form

$$G/H \cong \mathbf{Z}_p/p^{a_1}\mathbf{Z}_p \times \mathbf{Z}_p/p^{a_2}\mathbf{Z}_p \times \cdots \times \mathbf{Z}_p/p^{a_d}\mathbf{Z}_p. \tag{6}$$

As a group, G/H is usually a product of d nontrivial cyclic p-groups. For some H, $a_i = 0$ for all but one i, making $T = G/H$ a cyclic group.

Definition 3.1. *Let G be any profinite group and N be an open normal subgroup. A G-set $T \cong G/N$ where G/N is a cyclic group is called a cyclic G-set.*

An important property about cyclic G-sets T when G is a pro-p group is that $\{U \in \mathcal{F}(G) \colon U < T\}$, which is called the *strict downset of* T, with its induced order is a chain.

Throughout the rest of this section $G = \mathbf{Z}_p^d$ with $d \geq 2$.

From the large number of $\mathbf{Z}_p$-bases of G it is reasonable to expect that there are many cyclic G-sets of each size as the size grows. We will use cyclic G-sets later (Lemma 3.4) to find nonisomorphic G-sets of the same size with the same strict downsets, i.e., the G-sets lying below them in the frame of G are the same, which will be important in Section 4.

For each $T \in \mathcal{F}(G)$, there is an open subgroup $H \subset G$ with $T \cong G/H$, and H is uniquely determined by T since G is abelian: H is the common stabilizer of all points in T. Using a $\mathbf{Z}_p$-basis $\{e_1, e_2, \ldots, e_d\}$ of G we can identify H with $p^{a_1}\mathbf{Z}_p \times p^{a_2}\mathbf{Z}_p \times \cdots \times p^{a_d}\mathbf{Z}_p$ (this amounts to applying an automorphism of G), so the G-sets below G/H in $\mathcal{F}(G)$ are in one-to-one correspondence with the (open) subgroups of G that contain $p^{a_1}\mathbf{Z}_p \times p^{a_2}\mathbf{Z}_p \times \cdots \times p^{a_d}\mathbf{Z}_p$.

The frame of $\mathcal{F}(\mathbf{Z}_p)$ is linearly ordered so every element has a unique cover (G-set lying directly above it). Since every subgroup of $\mathbf{Z}_p^d$ is isomorphic to $\mathbf{Z}_p^d$ and there are $p^{d-1} + \ldots + p + 1$ maximal subgroups of $\mathbf{Z}_p^d$ the number of covers of each element of $\mathcal{F}(G)$ is the same which we now show.

Theorem 3.2. *Let $T \in \mathcal{F}(\mathbf{Z}_p^d)$. It has $p^{d-1} + \ldots + p + 1$ covers in $\mathcal{F}(\mathbf{Z}_p^d)$ and in the case $T \geq \mathbf{Z}_p^d/p\mathbf{Z}_p^d$, it covers $p^{d-1} + \ldots + p + 1$ elements of $\mathcal{F}(\mathbf{Z}_p^d)$.*

Proof. Let H be the stabilizer of T. Covers of T correspond to subgroups of H with index p, which correspond to maximal subgroups of $H/pH \cong (\mathbf{Z}/p\mathbf{Z})^d$. By duality the number of such subgroups is the number of subgroups of H/pH with size p, namely the number of linear subspaces of $(\mathbf{Z}/p\mathbf{Z})^d$. That is $(p^d - 1)/(p-1) = 1 + p + \ldots + p^{d-1}$.

Similarly, if T covers U then $U = \mathbf{Z}_p^d/K$ where $H \subset K$ and $[K : H] = p$, so the sets which T covers correspond to subgroups of size p in $\mathbf{Z}_p^d/H$. The number of such subgroups is the same as the number of subgroups of index p. When $\mathbf{Z}_p^d/H \geq \mathbf{Z}_p^d/p\mathbf{Z}_p^d$, we have $H \subset p\mathbf{Z}_p^d$. All subgroups of $\mathbf{Z}_p^d$ with index p contain $p\mathbf{Z}_p^d$, so the number of subgroups of index p in $\mathbf{Z}_p^d/H$ and $\mathbf{Z}_p^d/p\mathbf{Z}_p^d$ is the same. □

In some calculations, it was noticed that many pairs of coordinates in sums or products of certain Witt vectors are equal. This is described formally by Lemmas 4.1 and 4.2 below and motivates the following definition.

Definition 3.3. *A nonisomorphic pair of G-sets T and T', whose strict downsets agree, is called linked.*

For a linked pair of G-sets T and T', $\#T = \#T'$ since for any $U < T$ of maximal size, $\#T = p\#U$. Therefore $\#T' = p\#U = \#T$. An example of such a pair T and T' is labeled in Figure 2. The pair V_1 and V_2 in Figure 2 is not linked since the G-set U is below V_2 and not below V_1.

Our first task is to show that linked pairs of G-sets of arbitrarily large size exist for $G = \mathbf{Z}_p^d$ for $d \geq 2$. Of course, for $d = 1$, there are no linked $\mathbf{Z}_p$-sets.

Lemma 3.4. *For each $n \geq 1$ and cyclic G-set T of size p^{n-1}, there is a linked pair of cyclic G-sets T_1 and T_2 covering T.*

Proof. Since G is abelian, G-sets G/H for different (open) subgroups H are nonisomorphic. Since $d \geq 2$, there is more than one subgroup of index p. That settles the case $n = 1$.

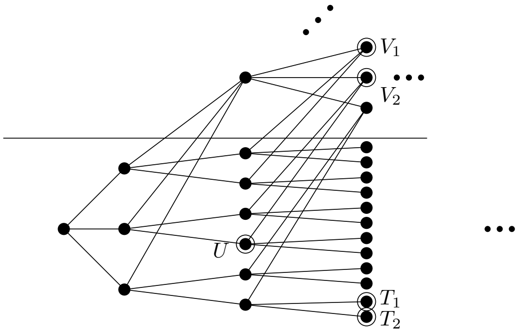

Figure 2: Linked and non-linked $\mathbf{Z}_2^2$-sets.

Now let $n \geq 2$ and write $T = G/H$. There is a unique maximal chain of subgroups

$$H = K_0 \subset K_1 \subset \cdots \subset K_{n-1} = G$$

where $[K_i : H] = p^i$ for all i. There is a $\mathbf{Z}_p$-basis of $\mathbf{Z}_p^d$, $\{e_1, \ldots, e_d\}$, such that $H = \bigoplus_{i=1}^{d-1} \mathbf{Z}_p e_i \oplus \mathbf{Z}_p p^{n-1} e_d$. Consider the subgroups $H_1 = \bigoplus_{i=1}^{d-1} \mathbf{Z}_p e_i \oplus \mathbf{Z}_p p^n e_d$ and $H_2 = \bigoplus_{i=1}^{d-2} \mathbf{Z}_p e_i \oplus \mathbf{Z}_p p e_{d-1} \oplus \mathbf{Z}_p(e_{d-1} + p^{n-1} e_d)$. Clearly $H_1 \subset H$ and $H_2 \subset H$, and both G/H_1 and G/H_2 are cyclic. Since $\#G/H_1$ and $\#G/H_2$ are both p^n, G/H_1 and G/H_2 are covers of G/H.

Set $T_1 = G/H_1$ and $T_2 = G/H_2$. Since $H_1 \neq H_2$, T_1 and T_2 are nonisomorphic. To show their strict downsets agree, we use the cyclic condition. The G-sets $U < T_1$ are G/K_i for $i = 0, \ldots, n-1$ since we the given maximal chain of subgroups is unique. The same argument applies to T_2, so the same G-sets lie strictly below T_1 and T_2 in the frame of G. □

4 $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is not Noetherian for $d \geq 2$

When k is a perfect field of characteristic p and $d \geq 2$, one might expect the rings $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ generalize the classical Witt vectors $\mathbf{W}_{\mathbf{Z}_p}(k)$ in the same way that $k[[X_1, \ldots, X_d]]$ generalizes $k[[X_1]]$: the power series ring in d variables over a field is a complete local Noetherian domain with dimension d.

It essentially follows from [DS88] that $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is not a domain but is a local ring whether or not k is perfect. Since it is also complete in its profinite topology it is plausible to guess, by analogy to $k[[X_1, \ldots, X_d]]$, that the maximal ideal of $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is generated by the Witt vectors $\omega_T(1)$ for $\#T = p$, but we will see this is false in a very strong way: $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is not Noetherian, whether or not k is perfect. This is because, as we will see, the square of the maximal ideal of $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is much smaller than intuition suggests.

To prove $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is not Noetherian when $d \geq 2$, note that Lemma 3.4 guarantees lots of linked paris of $\mathbf{Z}_p^d$-sets and we next prove two lemmas that describe

the behavior of sums and products on these linked pairs of coordinates.. The upshot, Theorem 4.4, is that Witt vectors in the square of the maximal ideal of $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ have built-in redundancies in linked coordinates which occur arbitrarily far out into the frame of $\mathbf{Z}_p^d$ when $d \geq 2$.
We continue to use the convention that G stands for $\mathbf{Z}_p^d$.

Lemma 4.1. *Let A be a ring. Given linked G-sets T and T' and a finite collection of Witt vectors $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m \in \mathbf{W}_G(A)$ such that $(\mathbf{a}_i)_T = (\mathbf{a}_i)_{T'}$ for $1 \leq i \leq m$, set $\mathbf{s} = \sum_{i=1}^{m} \mathbf{a}_i$. Then $s_T = s_{T'}$.*

Proof. By induction it suffices to check the case $m = 2$.
Since T and T' are linked i.e., the G-sets strictly below T and T' in $\mathcal{F}(G)$ are the same, $\#T = \#T'$ and the Witt polynomials $W_T(\underline{X})$ and $W_{T'}(\underline{X})$ are the same up to the roles of X_T, Y_T and $X_{T'}, Y_{T'}$ in them. Therefore the two sum polynomials S_T and $S_{T'}$ are the same up to the roles of X_T, Y_T, $X_{T'}$, and $Y_{T'}$ in them (and we know how X_T, Y_T, $X_{T'}$ and $Y_{T'}$ appear in S_T and $S_{T'}$ by Theorem 2.9). So when Witt vectors $\mathbf{a}_1$ and $\mathbf{a}_2$ have the same T and T' coordinates, since T and T' are linked we have $S_T(\mathbf{a}_1, \mathbf{a}_2) = S_{T'}(\mathbf{a}_1, \mathbf{a}_2)$. Thus $(\mathbf{a}_1 + \mathbf{a}_2)_T = (\mathbf{a}_1 + \mathbf{a}_2)_{T'}$. □

Unlike the previous lemma, the next one is specific to rings of characteristic p.

Lemma 4.2. *Let A be a ring of characteristic p. Given a pair of linked G-sets T and T' and elements $\mathbf{a}$ and $\mathbf{b}$ of $\mathbf{W}_G(A)$ such that $a_0 = b_0 = 0$, the product $\mathbf{m} = \mathbf{ab}$ satisfies $m_T = m_{T'}$.*

Proof. Let $R = \mathbf{Z}[\underline{X}, \underline{Y}]$ and define $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{W}_G(R)$ by $x_U = X_U$ and $y_U = Y_U$ for all U. Set $\mathbf{z} = \mathbf{xy}$. We will show

$$z_T - z_{T'} \equiv (x_T - x_{T'})y_0^{p^n} + (y_T - y_{T'})x_0^{p^n} \bmod pR.$$

Since A has characteristic p, it would then follow by functoriality that $\mathbf{ab}$ has equal T and T' coordinates in $\mathbf{W}_G(A)$.
Since the T-th Witt polynomial is a multiplicative function $W_T \colon \mathbf{W}_G(R) \to R$, $W_T(\mathbf{z}) = W_T(\mathbf{x})W_T(\mathbf{y})$:

$$\sum_{U \leq T} \#U z_U^{\#T/\#U} = \left(\sum_{U \leq T} \#U x_U^{\#T/\#U}\right)\left(\sum_{U \leq T} \#U y_U^{\#T/\#U}\right).$$

Isolating the z_T term,

$$\#T z_T = \left(\sum_{U \leq T} \#U x_U^{\#T/\#U}\right)\left(\sum_{U \leq T} \#U y_U^{\#T/\#U}\right) - \sum_{U < T} \#U z_U^{\#T/\#U}. \quad (7)$$

Likewise looking at the T' coordinate we have

$$\#T' z_{T'} = \left(\sum_{U \leq T'} \#U x_U^{\#T'/\#U}\right)\left(\sum_{U \leq T'} \#U y_U^{\#T'/\#U}\right) - \sum_{U<T'} \#U z_U^{\#T'/\#U}. \tag{8}$$

Since T and T' are linked, $\#T = \#T'$ and $\{U < T\} = \{U < T'\}$ so the z-terms being subtracted on the right side of (7) and (8) are the same. Subtracting (8) from (7) and setting $\#T = \#T' = p^n$, we have

$$\begin{aligned}
p^n z_T - p^n z_{T'} &= \left(\sum_{U \leq T} \#U x_U^{\frac{p^n}{\#U}}\right)\left(\sum_{U \leq T} \#U y_U^{\frac{p^n}{\#U}}\right) - \sum_{U<T} \#U z_U^{\frac{p^n}{\#U}} \\
&\quad - \left(\sum_{U \leq T'} \#U x_U^{\frac{p^n}{\#U}}\right)\left(\sum_{U \leq T'} \#U y_U^{\frac{p^n}{\#U}}\right) + \sum_{U<T'} \#U z_U^{\frac{p^n}{\#U}} \\
&= p^{2n} x_T y_T + p^n x_T \sum_{U<T} \#U y_U^{\frac{p^n}{\#U}} + p^n y_T \sum_{U<T} \#U x_U^{\frac{p^n}{\#U}} \\
&\quad - p^{2n} x_{T'} y_{T'} - p^n x_{T'} \sum_{U<T'} \#U y_U^{\frac{p^n}{\#U}} - p^n y_{T'} \sum_{U<T'} \#U x_U^{\frac{p^n}{\#U}} \\
&\equiv p^n x_T y_0^{p^n} + p^n x_0^{p^n} y_T - p^n x_{T'} y_0^{p^n} - p^n x_0^{p^n} y_{T'} \bmod p^{n+1}R \\
&\equiv p^n (x_T y_0^{p^n} + x_0^{p^n} y_T - x_{T'} y_0^{p^n} - x_0^{p^n} y_{T'}) \bmod p^{n+1}R \\
&\equiv p^n ((x_T - x_{T'}) y_0^{p^n} + (y_T - y_{T'}) x_0^{p^n}) \bmod p^{n+1}R.
\end{aligned}$$

So $z_T - z_{T'} \equiv (x_T - x_{T'}) y_0^{p^n} + (y_T - y_{T'}) x_0^{p^n} \bmod pR$. □

Remark 4.3. *The characteristic p hypothesis in Lemma 4.2 is necessary. Consider the case $G = \mathbf{Z}_p^d$ for $d \geq 2$ and $\mathbf{W}_G(\mathbf{Z})$. Any pair of nonisomorphic G-sets of size p is linked. Given two vectors $\mathbf{a}, \mathbf{b} \in \mathbf{W}_G(\mathbf{Z})$ such that $a_0 = b_0 = 0$, set $\mathbf{m} = \mathbf{ab}$. For $T \in \mathcal{F}(G)$ such that $\#T = p$, the formula for M_T in Example 2.4 implies $m_T = pa_T b_T$, which depends on T for suitable choices of* $\mathbf{a}$ *and* $\mathbf{b}$.

The point of these last two lemmas is that for linked G-sets T and T', the T and T' coordinates of a sum are the same if we make an assumption about the T and T' coordinates of the summands, while the T and T' coordinates of a product are the same if we make an assumption about the coordinates of the factors at the trivial G-set.

Let k be a field of characteristic p. For $n \geq 0$, recall the notation

$$I_{p^n} = I_{p^n}(G,k) = I_{p^n}(\mathbf{Z}_p^d, k) = \{\mathbf{a} \in \mathbf{W}_{\mathbf{Z}_p^d}(k); a_T = 0 \text{ if } \#T < p^n\}.$$

The unique maximal ideal of $\mathbf{W}_G(k)$ is $\mathfrak{m} = I_p(G,k)$.

Theorem 4.4. *Let T and T' be linked G-sets. Any element of $\mathfrak{m}^2$ has equal T and T' coordinates.*

Proof. Any element of $\mathfrak{m}^2$ is $\mathbf{a}_1\mathbf{b}_1+\cdots+\mathbf{a}_r\mathbf{b}_r$ for some $\mathbf{a}_i$ and $\mathbf{b}_i$ in $\mathfrak{m}$. Lemma 4.2 shows that $\mathbf{a}_i\mathbf{b}_i$ has the same T and T' coordinates for all i. Applying Lemma 4.1 shows that this equality of coordinates is preserved when passing to the sum of these products over all i. □

Since Lemma 3.4 shows that there are linked G-sets of arbitrarily large size, Theorem 4.4 puts infinitely many constraints on elements of $\mathfrak{m}^2$. Theorem 4.4 was first observed in examples, where many redundancies were noticed in different coordinates of a product of elements of $\mathbf{W}_{\mathbf{Z}_2^2}(\mathbf{F}_2[\underline{X}, \underline{Y}])$ that each have first coordinate 0. This is also how the importance of linked G-sets was discovered. We are now set to use them to prove our first main structural theorem.

Theorem 4.5. *The maximal ideal of $\mathbf{W}_G(k)$ is not finitely generated, so $\mathbf{W}_G(k)$ is not Noetherian.*

Proof. Using Lemma 3.4, for each $n \geq 1$ there are linked G-sets T_n and T'_n in $\mathcal{F}(G)$ of size p^n. In particular, $\{U : U < T_n\} = \{U : U < T'_n\}$. The Witt vector $\omega_{T_n}(1)$ lies in $\mathfrak{m}$. For each $r \geq 1$ we will show the r Witt vectors $\omega_{T_1}(1), \ldots, \omega_{T_r}(1)$ are linearly independent over k in $\mathfrak{m}/\mathfrak{m}^2$.
In $\mathfrak{m}/\mathfrak{m}^2$, suppose we have a k-linear relation

$$\alpha_1\omega_{T_1}(1) + \cdots + \alpha_r\omega_{T_r}(1) \equiv 0 \bmod \mathfrak{m}^2,$$

for some $\alpha_i \in k$. The product $\alpha_i\omega_{T_i}(1)$ in $\mathfrak{m}/\mathfrak{m}^2$ really means, as a Witt vector, $\omega_0(\alpha_i)\omega_{T_i}(1) \bmod \mathfrak{m}^2$. By Theorem 2.8, $\omega_0(\alpha_i)\omega_{T_i}(1) = \omega_{T_i}(\alpha_i^{p^i})$. Therefore

$$\omega_{T_1}(\alpha_1^p) + \cdots + \omega_{T_r}(\alpha_r^{p^r}) \equiv 0 \bmod \mathfrak{m}^2. \tag{9}$$

Since the supports of $\omega_{T_i}(\alpha_i^{p^i})$ for $1 \leq i \leq r$ are disjoint, by Theorem 2.6 these Witt vectors can be added coordinatewise: the left side of (9) is the Witt vector with T_i-coordinate $\alpha_i^{p^i}$ and other coordinates equal to 0. Since this sum is in $\mathfrak{m}^2$, its T_i- and T'_i-coordinates are the same by Theorem 4.4. The T'_i-coordinate is 0 for all i, so $\alpha_i^{p^i} = 0$ for all i. Thus every α_i is 0 in k.
Since we have found r linearly independent elements of $\mathfrak{m}/\mathfrak{m}^2$ for any $r \geq 1$, its k-dimension is infinite. Therefore $\mathfrak{m}$ is not finitely generated. □

Remark 4.6. *For an infinite pro-p group G with arbitrarily large pairs of linked normal G-sets, the results of this section go through. For such pro-p groups, $\mathbf{W}_G(k)$ is not Noetherian when k is a field (or ring) of characteristic p.*

5 Reducedness of $\mathbf{W}_G(k)$

Although $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ with $d > 2$ is not a domain and is not Noetherian, this is not a pathological state of affairs among p-adic rings. For instance, the ring $C(\mathbf{Z}_p, \mathbf{Q}_p)$ of continuous functions from $\mathbf{Z}_p$ to $\mathbf{Q}_p$ is not a domain and is not Noetherian. This ring is reduced. So we ask: is $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ reduced? We answer this in the case $d = 2$ and for any p.

To do this, we keep track of a new partial ordering on $\mathcal{F}(G)$. This new partial ordering makes sense with no extra effort for $G = \mathbf{Z}_p^d$ with any $d \geq 1$ so we state it in this generality. Consider the descending subgroup filtration

$$G \supsetneqq pG \supsetneqq p^2G \supsetneqq \cdots \supsetneqq p^nG \supsetneqq p^{n+1}G \supsetneqq \cdots,$$

which leads to the rising family of G-sets

$$0 = G/G < G/pG < G/p^2G < \cdots < G/p^nG < G/p^{n+1}G < \cdots$$

in $\mathcal{F}(G)$.

Definition 5.1. *For $G = \mathbf{Z}_p^d$, the level of $T \in \mathcal{F}(G)$ is the largest $n \geq 0$ such that $T \geq G/p^nG$. We write* $\mathrm{Lev}(T) = n$.

This definition makes sense, since if $T \geq G/p^nG$ then $\#T \geq p^{nd}$, so n is bounded above, and $T \geq 0$ so we have somewhere to begin. To get a feel for this concept, we describe it on coset spaces. Write $T \cong G/H$ for a unique open subgroup H of G. We have $T \geq G/p^nG$ if and only if $H \subset p^nG$. Therefore $\mathrm{Lev}(G/H)$ is the largest $n \geq 0$ such that $H \subset p^nG$. See Figure 3.

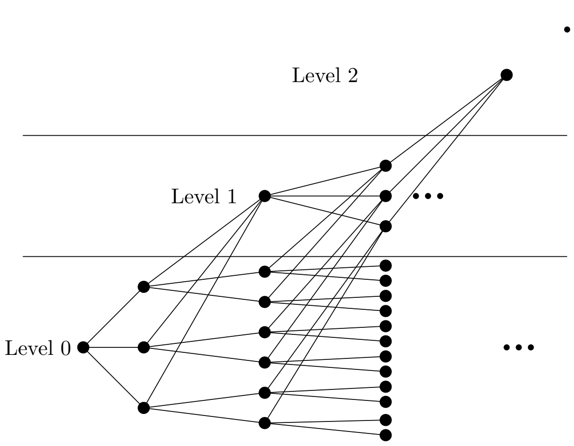

Figure 3: Initial $\mathbf{Z}_2^2$-sets of level $0, 1, 2$.

If $G = \mathbf{Z}_p$ then $\mathrm{Lev}(T)$ and $\#T$ are basically the same concept, since $\#T = p^{\mathrm{Lev}(T)}$. The level is something genuinely new when $G = \mathbf{Z}_p^d$ for $d \geq 2$. In this case neither $\#T$ nor $\mathrm{Lev}(T)$ determines the other; all we can say in general is that $\#T \geq p^{d\mathrm{Lev}(T)}$.

Writing the cyclic decomposition of G/H as $\mathbf{Z}/p^{a_1}\mathbf{Z} \times \mathbf{Z}/p^{a_2}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{a_d}\mathbf{Z}$, its level is $\min\{a_1, a_2, \ldots, a_d\}$. This makes it easy to produce examples.

Example 5.2. *For $a \geq 1$, the G-set $\mathbf{Z}_p^d/(\mathbf{Z}_p \times p^a\mathbf{Z}_p^{d-1})$ of size $p^{a(d-1)}$ has level 0 since $\mathbf{Z}_p \times p^a\mathbf{Z}_p^{d-1}$ is contained in G but not pG. So when $d \geq 2$, arbitrarily large G-sets can have level 0 (but not when $d = 1$).*

Example 5.3. *There are arbitrarily large G-sets of any chosen level n when $d \geq 2$: use $\mathbf{Z}_p^d/(p^n\mathbf{Z}_p \times p^{a+n}\mathbf{Z}_p^{d-1})$ with $a \to \infty$.*

Theorem 5.4. *For $d \geq 2$, each $\mathbf{Z}_p^d$-set of level n is covered by more than one G-set of level n.*

Proof. Let T be a G-set with $\mathrm{Lev}(T) = n$. Pick a $\mathbf{Z}_p$-basis $\{e_1, \ldots, e_d\}$ of $\mathbf{Z}_p^d$ so that $T \cong G/H$ with $H = \mathbf{Z}_p p^{a_1}e_1 + \ldots + \mathbf{Z}_p p^{a_d}e_d$, where $n = a_1 \leq a_2 \leq \ldots \leq a_d$. When $d \geq 3$, $\sum_{i=1}^{d-1}\mathbf{Z}_p p^{a_i}e_i + \mathbf{Z}_p p^{a_d+1}e_d$ and $\sum_{i\neq d-1}\mathbf{Z}_p p^{a_i}e_i + \mathbf{Z}_p p^{a_{d-1}+1}e_{d-1}$ are subgroups of H with index p and they are the stabilizers of two distinct G-sets covering T both with level n. If $d = 2$, on the other hand, $\mathbf{Z}_p p^{a_1}e_1 + \mathbf{Z}_p p^{a_2+1}e_2$ and $\mathbf{Z}_p(p^{a_1+1}e_1 + p^{a_1}e_2) + \mathbf{Z}_p p^{a_2}e_2$ are subgroups of H with index p and they are the stabilizers of two distinct $\mathbf{Z}_p^2$-sets covering T both with level n. □

For any $T \in \mathcal{F}(G)$, $\{U : \#U \leq \#T\}$ and $\{U : U \leq T\}$ are finite (the latter is a subset of the former), but $\{U : \mathrm{Lev}(U) \leq \mathrm{Lev}(T)\}$ is infinite. This is an important distinction to remember.

Remark 5.5. *When $d \geq 2$, any nontrivial cyclic G-set looks like $\mathbf{Z}_p^d/(\mathbf{Z}_p^{d-1} \times p^a\mathbf{Z}_p)$ with $a \geq 1$ after a suitable choice of basis for $\mathbf{Z}_p^d$, and $\mathbf{Z}_p^{d-1} \times p^a\mathbf{Z}_p$ is not contained in $p\mathbf{Z}_p^d$ (this is false for $d = 1$), so all cyclic G-sets have level 0. When $d = 2$, a G-set of level 0 is isomorphic to $\mathbf{Z}_p^2/(\mathbf{Z}_p \times p^a\mathbf{Z}_p)$, so having level 0 and cyclic in $\mathcal{F}(\mathbf{Z}_p^2)$ mean the same thing. For $d \geq 3$, some G-sets of level 0 are not cyclic, such as $\mathbf{Z}_p^d/(\mathbf{Z}_p \times p\mathbf{Z}_p \times p^a\mathbf{Z}_p^{d-2})$ with $a \geq 1$.*

To prove that $\mathbf{W}_{\mathbf{Z}_p^2}(k)$ is reduced when k has characteristic p, we seek the right coordinate to look at in a power of a nonzero Witt vector to know that the power is also not $\mathbf{0}$.

Say $\mathbf{x} \in \mathbf{W}_G(k)$ and $\mathbf{x} \neq \mathbf{0}$. It is natural to consider how $\mathbf{x}$ sits in the descending ideal filtration $\{I_{p^n}\}$: there is some I_{p^n} for which $\mathbf{x} \in I_{p^n}$ and n is as large as possible, so $x_T = 0$ for $\#T < p^n$ and some x_T is nonzero where $\#T = p^n$. In this case it is not hard to check that $\mathbf{x}^2 \in I_{p^{2n}}$ (Corollary 2.15), and we can anticipate (if $\mathbf{W}_G(k)$ is reduced) that $\mathbf{x}^2$ has a nonzero coordinate at some G-set of size p^{2n}. Which one? We need a way to predict a nonzero coordinate in $\mathbf{x}^2$ when $\mathbf{x} \neq \mathbf{0}$.

Lemma 5.6. *Let $G = \mathbf{Z}_p^d$. If $U \leq T$ in $\mathcal{F}(G)$ then $\mathrm{Lev}(U) \leq \mathrm{Lev}(T)$.*

Proof. Let $n = \mathrm{Lev}(U)$, so $U \geq G/p^nG$. Since $T \geq U$, we have $T \geq G/p^nG$, so $\mathrm{Lev}(T) \geq n$. □

Note that if $U < T$ and $d \geq 2$ it need not follow that $\mathrm{Lev}(U) < \mathrm{Lev}(T)$: we might have $\mathrm{Lev}(U) = \mathrm{Lev}(T)$. For example, if $U = G/H$ and $T = G/K$ where $H = p\mathbf{Z}_p^d = p\mathbf{Z}_p^{d-1} \times p\mathbf{Z}_p$ and $K = p\mathbf{Z}_p^{d-1} \times p^2\mathbf{Z}_p$ then $K \subset H$ so $U < T$ and $\mathrm{Lev}(U) = \mathrm{Lev}(T) = 1$.

Lemma 5.7. *Let $G = \mathbf{Z}_p^d$ and $T \in \mathcal{F}(G)$ have level n. Write $T \cong G/H$ with $H \subset p^n\mathbf{Z}_p^d$ and $H \not\subset p^{n+1}\mathbf{Z}_p^d$ so $H = p^n\widehat{H}$ for a unique open subgroup $\widehat{H}$ of $\mathbf{Z}_p^d$. Set $\widehat{T} = G/\widehat{H}$. Then $\widehat{T}$ has level* 0. *Moreover, if $U \in \mathcal{F}(G)$ and* $\mathrm{Lev}(U) = n$ *then $U \leq T$ if and only if $\widehat{U} \leq \widehat{T}$.*

Proof. By choosing a suitable basis of $\mathbf{Z}_p^d$, we may assume $H = p^{a_1}\mathbf{Z}_p \times \ldots \times p^{a_d}\mathbf{Z}_p$. The statement that T has level n means $n = \min\{a_1, \ldots, a_d\}$, so $H = p^n(p^{b_1}\mathbf{Z}_p \times \ldots \times p^{b_d}\mathbf{Z}_p)$ with some $b_i = 0$. Then $\widehat{H} = p^{b_1}\mathbf{Z}_p \times \ldots \times p^{b_d}\mathbf{Z}_p$ and $\widehat{T}$ has level 0.
To prove the second claim, write $U \cong G/K$ and $K = p^n\widehat{K}$. We have $U \leq T$ if and only if $H \subset K$ and $\widehat{U} \leq \widehat{T}$ if and only if $\widehat{H} \subset \widehat{K}$. The conditions $H \subset K$ and $\widehat{H} \subset \widehat{K}$ are the same. □

Lemma 5.8. *For $G = \mathbf{Z}_p^d$ with $d \geq 2$ and $T \in \mathcal{F}(G)$, set $\#T = p^n$. For each $m \geq n$, there exist T' such that $\#T' = p^m$, $T \leq T'$ and* $\mathrm{Lev}(T) = \mathrm{Lev}(T')$.

Proof. Write $T = G/H$. Choose a $\mathbf{Z}_p$-basis $\{e_1, e_2, \ldots, e_d\}$ of $\mathbf{Z}_p^d$ such that $H = \sum_{i=1}^d \mathbf{Z}_p p^{a_i} e_i$. Without loss of generality, assume $a_1 \leq a_2 \leq \ldots \leq a_d$ and set $K = \sum_{i=1}^{d-1} \mathbf{Z}_p p^{a_i} e_i + \mathbf{Z}_p p^{a_d+m-n} e_d$. Then $K \subset H$ and $[H : K] = p^{m-n}$ so G/K is a cover of G/H. Since $a_1 \leq a_2 \leq \ldots \leq a_d$ and $d \geq 2$, $\min\{a_1, a_2, \ldots, a_d\} = \min\{a_1, a_2, \ldots, a_d + m - n\}$, so $\mathrm{Lev}(G/K) = \mathrm{Lev}(G/H)$. □

Consider Figure 3. The two horizontal lines divide the diagram into regions of $\mathbf{Z}_2^2$-sets with the same level. Lemma 5.8 just says that these levels go infinitely far out in the frame.
Returning to the assumption $G = \mathbf{Z}_p^2$ we have the following lemma.

Lemma 5.9. *When $G = \mathbf{Z}_p^2$ and T and T' in $\mathcal{F}(G)$ satisfy $T \leq T'$ and* $\mathrm{Lev}(T) = \mathrm{Lev}(T')$,

$$\{U \in \mathcal{F}(G) : U \leq T' \textit{ and } \mathrm{Lev}(U) = \mathrm{Lev}(T) \textit{ and } \#U = \#T\} = \{T\}.$$

Proof. The set of G-sets of level zero is a tree (see Remark 2.1), so the property is obviously true when $\mathrm{Lev}(T) = \mathrm{Lev}(T') = 0$. Using Lemma 5.7 one has the result for any level. □

Lemma 5.10. *Let $G = \mathbf{Z}_p^2$, A be a nonzero commutative ring, and choose any nonzero $\mathbf{a} \in W_G(A)$. There is $T_0 \in \mathcal{F}(G)$ such that $a_{T_0} \neq 0$ and $a_U = 0$ under either of the following conditions:*

- $\mathrm{Lev}(U) < \mathrm{Lev}(T_0)$,
- $\mathrm{Lev}(U) = \mathrm{Lev}(T_0)$ *and* $\#U < \#T_0$,

Proof. Given $\mathbf{a} \neq \mathbf{0}$ in $\mathbf{W}_G(A)$, among $\{T : a_T \neq 0\}$ first select all T with minimal level, and then among the T of that minimal level, choose one T of minimal size. Call that T_0.
If $\mathrm{Lev}(U) < \mathrm{Lev}(T_0)$ then $a_U = 0$ since T_0 is a nonzero coordinate with minimal level. If $\mathrm{Lev}(U) = \mathrm{Lev}(T_0)$ and $\#U < \#T_0$ then $a_U = 0$ since otherwise T_0 is not a nonzero coordinate of minimal size among nonzero coordinates of minimal level. □

Remark 5.11. *Lemma 5.10 is expressed in a form convenient for the applications we have in mind, but it's not a result about nonzero Witt vectors so much as a property of $\mathcal{F}(G)$: for any nonempty subset $\mathcal{S}$ of $\mathcal{F}(G)$, there is a $T_0 \in \mathcal{S}$ such that $U \notin \mathcal{S}$ if* $\mathrm{Lev}(U) < \mathrm{Lev}(T_0)$, *or if* $\mathrm{Lev}(U) = \mathrm{Lev}(T_0)$ *and* $\#U < \#T_0$.

Remark 5.12. *In our application of Lemma 5.10 it is important to note the order in which the concepts are minimized. Here we are first choosing nonzero G-sets of minimal level, then among those we choose one of minimal size. These two minimizations do not commute. Figure 4 depicts a nonzero element of $\mathbf{W}_{\mathbf{Z}_2^2}(k)$, where all coordinates are zero except for the circled ones which are non-zero. The T coordinate is the one of minimal size first and then level, whereas the U coordinate is the one of minimal level first and then size.*

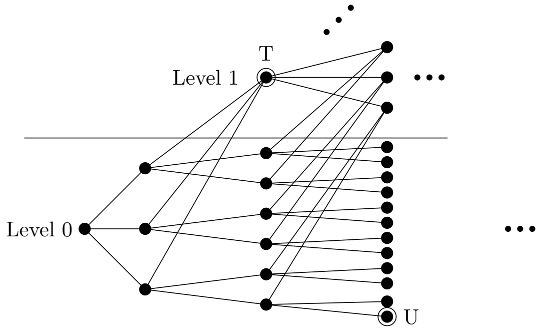

Figure 4: Nonzero element in $\mathbf{W}_{\mathbf{Z}_2^2}$

Now we will use the concept of level to prove something about multiplication in $\mathbf{W}_G(k)$. The end of the next lemma identifies a formula for a specific coordinate in the product of two Witt vectors if all the "smaller" coordinates are 0. It is analogous to something simple when $G = \mathbf{Z}_p$: if $\mathbf{a} = p^n(a_0 + p\mathbf{a}')$ and $\mathbf{b} = p^n(b_0 + p\mathbf{b}')$ then $\mathbf{ab} = p^{2n}(a_0b_0 + p\mathbf{c})$. (It is not assumed that a_0 and b_0 are nonzero.) There is a similar formula even if the p-powers in $\mathbf{a}$ and $\mathbf{b}$ are not equal, but for $G = \mathbf{Z}_p^d$ with $d \geq 2$ we don't have a formula that broad. It seems to be the price we pay for $\mathbf{W}_G(k)$ not being a domain.

Lemma 5.13. *Let G be an abelian pro-p group and A be a ring of characteristic p. Let $V \in \mathcal{F}(G)$ with $\#V \leq p^{m+n}$ for positive integers m and n. Consider Witt vectors $\mathbf{a}$ and $\mathbf{b}$ in $\mathbf{W}_G(A)$ such that $a_U = 0$ for all $U < V$ such that $\#U < p^m$ and $b_U = 0$ for all $U < V$ such that $\#U < p^n$. Set $\mathbf{c} = \mathbf{ab}$. Then $c_V = 0$.*

Proof. This will follow from functoriality by proving the following mod p congruence for particular Witt vectors over the ring $R = \mathbf{Z}[\underline{X}, \underline{Y}]$. Define $\mathbf{x}, \mathbf{y} \in \mathbf{W}_G(R)$ by

$$x_T = \begin{cases} 0, & \#T < p^m \text{ and } T < V, \\ X_T, & \text{otherwise,} \end{cases} \quad \text{and } y_T = \begin{cases} 0, & \#T < p^n \text{ and } T < V, \\ Y_T, & \text{otherwise.} \end{cases}$$

Set $\mathbf{z} = \mathbf{xy}$. We will show that

$$T \leq V \Longrightarrow z_T \equiv 0 \bmod pR. \tag{10}$$

Returning to the proof of (10), we argue by induction on $\#T$. If $\#T = 1$ then $T = 0$ and $z_0 = x_0 y_0 = 0$. Let $p^r \leq p^{m+n}$ with $r \geq 1$ and assume by induction that for all $U < V$ such that $\#U < p^r$, $z_U \equiv 0 \bmod pR$. Pick $T \leq V$ with $\#T = p^r$. Since the T-th Witt polynomial is a multiplicative function $W_T \colon \mathbf{W}_G(R) \to R$, $W_T(\mathbf{z}) = W_T(\mathbf{x})W_T(\mathbf{y})$:

$$\sum_{U \leq T} \varphi_T(U) z_U^{\#T/\#U} = \sum_{T_1, T_2 \leq T} \varphi_T(T_1)\varphi_T(T_2) x_{T_1}^{\#T/\#T_1} y_{T_2}^{\#T/\#T_2}.$$

Solving this equation for z_T in $\mathbf{Q}[\underline{X}, \underline{Y}]$,

$$z_T = \sum_{T_1, T_2 \leq T} \frac{\varphi_T(T_1)\varphi_T(T_2)}{\varphi_T(T)} x_{T_1}^{\#T/\#T_1} y_{T_2}^{\#T/\#T_2} - \sum_{U < T} \frac{\varphi_T(U)}{\varphi_T(T)} z_U^{\#T/\#U}. \tag{11}$$

Since $z_U \in pR$ for $U < T$, the second term in (11) is 0 mod pR by Lemma 2.11. In the first term in (11), if $T_1 = V$ then $T_1 = T = V$ and $\varphi_T(T_1)\varphi_T(T_2)/\varphi_T(T) \equiv \varphi_T(T_2) \equiv 0 \bmod pR$ by Lemma 2.10 provided $T_2 \neq 0$, while if $T_2 = 0$ then $y_{T_2} = 0$. A similar argument holds if $T_2 = V$ so we can assume $T_1 < V$ and $T_2 < V$. If either $\#T_1 < p^m$ or $\#T_2 < p^n$ then $x_{T_1} = 0$ or $y_{T_2} = 0$ respectively. The remaining terms in the first sum in (11) have $T_1 < V$ with $\#T_1 \geq p^m$ and $T_2 < V$ with $\#T_2 \geq p^n$. In this case $\#T_1 \#T_2 \geq p^{m+n} > p^r = \#T$. Since G is abelian, $\varphi_T(U) = \#U$ and so the coefficient in the first sum in (11) is an integral multiple of p. Thus $z_T \equiv 0 \bmod pR$. □

Remark 5.14. *The only place where G being abelian played a role in the proof of Lemma 5.13 was at the last step calculating the p-divisibility of the coefficients* *in the first sum in (11). For general pro-p groups, this ratio need not even be integral, however the conclusion of Lemma 5.13 holds true not just for abelian pro-p groups, but any pro-p which satisfies*

$$\frac{\varphi_T(T_1)\varphi_T(T_2)}{\varphi_T(T)} \in p\mathbf{Z}$$

for any $T, T_1, T_2 \in \mathcal{F}(G)$.

Lemma 5.15. *For $G = \mathbf{Z}_p^2$ and k a field of characteristic p. Let $\mathbf{a}$ and $\mathbf{b}$ be in $\mathbf{W}_G(k)$ such that there is a $T_0 \in \mathcal{F}(G)$ with $a_U = b_U = 0$ if $\mathrm{Lev}(U) < \mathrm{Lev}(T_0)$, or if $\mathrm{Lev}(U) = \mathrm{Lev}(T_0)$ and $\#U < \#T_0$. Set $\#T_0 = p^n$. For any $T \in \mathcal{F}(G)$ with size p^{2n} such that $T_0 \leq T$ and $\mathrm{Lev}(T_0) = \mathrm{Lev}(T)$, the product $\mathbf{ab}$ has T-coordinate $(a_{T_0}b_{T_0})^{p^n}$.*

Proof. Let $R = \mathbf{Z}[\underline{X}, \underline{Y}]$. Define $\mathbf{x}, \mathbf{y}$ in $\mathbf{W}_G(R)$ by

$$x_U = \begin{cases} 0 & \text{if } \mathrm{Lev}(U) < \mathrm{Lev}(T_0), \\ 0 & \text{if } \mathrm{Lev}(U) = \mathrm{Lev}(T_0) \text{ and } \#U < p^n, \\ X_U & \text{otherwise,} \end{cases}$$

and

$$y_U = \begin{cases} 0 & \text{if } \mathrm{Lev}(U) < \mathrm{Lev}(T_0), \\ 0 & \text{if } \mathrm{Lev}(U) = \mathrm{Lev}(T_0) \text{ and } \#U < p^n, \\ Y_U & \text{otherwise.} \end{cases}$$

and set $\mathbf{z} = \mathbf{xy}$. For any G-set T of size p^{2n} with $T_0 \leq T$ and $\mathrm{Lev}(T_0) = \mathrm{Lev}(T)$ we will show $z_T \equiv (X_{T_0}Y_{T_0})^{p^n} \bmod pR$. By functoriality the lemma would then follow.

For any G-set T, $W_T(\mathbf{z}) = W_T(\mathbf{x})W_T(\mathbf{y})$:

$$\sum_{U \leq T} \#U z_U^{\#T/\#U} = \left(\sum_{U \leq T} \#U x_U^{\#T/\#U}\right)\left(\sum_{U \leq T} \#U y_U^{\#T/\#U}\right). \tag{12}$$

By Lemma 5.8 we can choose $T \geq T_0$ such that $\#T = p^{2n}$ and $\mathrm{Lev}(T) = \mathrm{Lev}(T_0)$. First we look at the left side of (12). Let $V < T$, so $\#V < p^{2n}$. By Lemma 5.6 $\mathrm{Lev}(V) \leq \mathrm{Lev}(T) = \mathrm{Lev}(T_0)$. So either $\mathrm{Lev}(V) < \mathrm{Lev}(T)$ or $\mathrm{Lev}(V) = \mathrm{Lev}(T)$. For all $U < V$ with $\#U < p^n$, both x_U and y_U are zero by hypothesis. The proof of Lemma 5.13 tells us that $z_V \equiv 0 \bmod pR$ when $V < T$ and $\#V < p^{2n}$. So $\#V z_V^{\#T/\#V} \equiv 0 \bmod p^{2n+1}R$ for $V < T$ and $\#V < p^{2n}$, so the left side of (12) is $p^{2n}z_T \bmod p^{2n+1}R$.

Now we turn to the right side of (12). If $U \leq T$ then $\mathrm{Lev}(U) \leq \mathrm{Lev}(T)$ (Lemma 5.6) and since $\mathrm{Lev}(T) = \mathrm{Lev}(T_0)$ our hypotheses tells us $x_U = 0$ and $y_U = 0$ if $\mathrm{Lev}(U) < \mathrm{Lev}(T)$, or if $\mathrm{Lev}(U) = \mathrm{Lev}(T)$ and $\#U < p^n$. So the only U-terms in each sum on the right side of (12) that are not automatically 0 have $\mathrm{Lev}(U) = \mathrm{Lev}(T)$ and $\#U \geq p^n$.

Dropping the terms in (12) where $x_U = 0$ and $y_U = 0$ and reducing modulo $p^{2n+1}R$, one has that $p^{2n}z_T$ is equivalent to

$$\left(\sum_{\substack{U \leq T \\ \mathrm{Lev}(U)=\mathrm{Lev}(T) \\ \#U \geq p^n}} \#U X_U^{\#T/\#U} \right) \left(\sum_{\substack{U \leq T \\ \mathrm{Lev}(U)=\mathrm{Lev}(T) \\ \#U \geq p^n}} \#U Y_U^{\#T/\#U} \right) \bmod p^{2n+1}R.$$

Each summand has a coefficient divisible at least by p^n, so any product of a term from each sum is divisible by p^{2n}. A term divisible by p^{n+1} in one sum has a product with any term in the other sum that is 0 mod $p^{2n+1}R$, so

$$p^{2n}z_T \equiv \left(\sum_{\substack{U \leq T \\ \mathrm{Lev}(U)=\mathrm{Lev}(T) \\ \#U = p^n}} p^n X_U^{p^n} \right) \left(\sum_{\substack{U \leq T \\ \mathrm{Lev}(U)=\mathrm{Lev}(T) \\ \#U = p^n}} p^n Y_U^{p^n} \right) \bmod p^{2n+1}R.$$

Dividing through by p^{2n} and using additivity of the pth power map in R/pR,

$$z_T \equiv \left(\sum_{\substack{U \leq T \\ \mathrm{Lev}(U)=\mathrm{Lev}(T) \\ \#U = p^n}} X_U \cdot \sum_{\substack{U \leq T \\ \mathrm{Lev}(U)=\mathrm{Lev}(T) \\ \#U = p^n}} Y_U \right)^{p^n} \bmod pR. \tag{13}$$

What are the U lying below T in $\mathcal{F}(G)$ with the same level as T and of size p^n? One example is $U = T_0$. By Lemma 5.9 this is the only example, so $z_T \equiv (X_{T_0}Y_{T_0})^{p^n} \bmod pR$. The argument did not depend on the choice of T and so holds for any T with $T \geq T_0$, $\#T = p^{2n}$, and $\mathrm{Lev}(T) = \mathrm{Lev}(T_0)$. □

We will only apply Lemma 5.15 when the two Witt vectors are equal, i.e., to the square of a nonzero element of $\mathbf{W}_G(k)$.

Remark 5.16. *Most of the proof of Lemma 5.15 goes through for $G = \mathbf{Z}_p^d$ for $d \geq 3$ and not just $d = 2$. In fact (13) is true for $G = \mathbf{Z}_p^d$ for $d \geq 2$ and it was only at the last step where we used the fact that $d = 2$, which hinged on Lemma 5.9. Lemma 5.9 is not true for $G = \mathbf{Z}_p^d$ with $d \geq 3$ since the level 0 part of $\mathcal{F}(\mathbf{Z}_p^d)$ is not a tree. This is well-known after one realizes the level 0 part of $\mathcal{F}(\mathbf{Z}_p^d)$ is in order bijection with the $\mathbf{Z}_p$-lattices in $\mathbf{Q}_p^d$ up to scaling (see Remark 2.1), which forms the Bruhat-Tits building for $\mathrm{SL}_d(\mathbf{Q}_p)$ which is not a tree for $d \geq 3$ (see [Bro08, pg. 137].) More concretely, when $d \geq 3$, $\mathbf{Z}_p^d/(\mathbf{Z}_p \times p\mathbf{Z}_p \times p^a\mathbf{Z}_p^{p-2})$ with $a \geq 1$ is not a cyclic group and so its strict downset is not a chain.*

Theorem 5.17. *For any field k of characteristic p, the ring $\mathbf{W}_G(k)$ is reduced for $G = \mathbf{Z}_p^2$.*

Proof. Let $\mathbf{v}$ be nonzero in $\mathbf{W}_G(k)$. If $v_0 \neq 0$ then $\mathbf{v} \in \mathbf{W}_G(k)^\times$ by Theorem 2.16. Otherwise $\mathbf{v} \in \mathfrak{m}$ and it suffices to show for all $n \in \mathbf{Z}^+$ that $\mathbf{v}^{2^n}$ is nonzero. Thus it suffices to show if $\mathbf{v} \in \mathfrak{m}$ and $\mathbf{v} \neq \mathbf{0}$ then $\mathbf{v}^2 \neq \mathbf{0}$. By Lemma 5.10 there is a $T_0 \in \mathcal{F}(G)$ such that v_{T_0} is nonzero but v_U is zero for all $U \in \mathcal{F}(G)$ where $\mathrm{Lev}(U) < \mathrm{Lev}(T_0)$ or where $\mathrm{Lev}(U) = \mathrm{Lev}(T_0)$ and $\#U < \#T_0$. Lemma 5.15 with $\mathbf{a} = \mathbf{b} = \mathbf{v}$ tells us that $\mathbf{v}^2$ has a coordinate equal to $v_{T_0}^{2\#T_0} \neq 0$, so $\mathbf{v}^2 \neq \mathbf{0}$. □

Acknowledgments

The author is forever indebted to Keith Conrad and would also like to thank Sarah Glaz, Álvaro Lozano-Robledo, Jeremy Teitelbaum, Anurag Singh, Jesse Elliott, and Karl Schwede for their readings and enlightening discussions as well as the reviewer and to Lars Hesselholt for his guidance.

References

[Bru05] M. Brun, *Witt vectors and Tambara functors*, Adv. Math., 193, 2, (2005), 233–256.

[Bru07] M. Brun, *Witt vectors and equivariant ring spectra applied to cobordism*, Proc. London Math. Soc., 94, (2007), 351–385.

[Bro08] K. S. Brown, *Buildings*, Springer, New York, 2008.

[DS88] A. Dress, C. Siebeneicher, *The Burnside ring of profinite groups and the Witt vector construction*, Adv. Math., 70, (1988), 87–132.

[Gra93] J. Graham, *Generalized Witt vectors*, Adv. Math., 99, (1993), 248–263.

[Ell06] J. Elliott, *Constructing Witt–Burnside rings*, Adv. Math., 203, (2006), 319–363.

[Oh07] Y. Oh, *q-deformation of Witt-Burnside rings*, Math. Z., 257, (2007), 151–191.

[Oh09] Y. Oh, *Decomposition of the Witt-Burnside ring and Burnside ring of an abelian profinite group*, Adv. Math., 222, 2, (2009), 485–526.

[Oh12] Y. Oh, *Classification and decomposition of the Witt-Burnside ring and Burnside ring of a profinite group*, Proc. London Math. Soc., 3, 104, (2012), 649–689.

[Ser79] J.-P. Serre, *Local Fields*, Springer, New York, 1979.

[Ser77] J.-P. Serre, *Trees*, Springer, New York, 1977.

[Str] N. P. Strickland, *Tambara functors*, arXiv:1205.251.

[Wit36] E. Witt, *Zyklische Körper und Algebren der Characteristik p vom Grad p^n*, J. Reine Angew. Math., 176, (1936), 126–140.

Lance Edward Miller
University of Arkansas
Department of Mathematical Sciences
301 SCEN
Fayetteville, AR
72701.
lmiller@math.utah.edu