p-Jets of Finite Algebras, II: p-Typical Witt Rings

Alexandru Buium

Received: January 12, 2012

Communicated by Lars Hesselholt

Abstract. We study the structure of the p-jet spaces of the p-typical Witt rings of the p-adics. We also study the p-jets of the comonad map. These data can be viewed as an arithmetic analogue, for the ring $\mathbb{Z}$, of the Lie groupoid of the line and hence as an infinitesimal version of the Galois group of $\mathbb{Q}$ over "$\mathbb{F}_1$".

2010 Mathematics Subject Classification: 13 K 05
Keywords and Phrases: Witt vectors

1. Introduction

1.1. Motivation. This paper is the second in a series of papers where we investigate p-jet spaces (in the sense of [6]) of finite flat schemes/algebras. The understanding of such p-jet spaces seems to hold the key to a number of central questions about *arithmetic differential equations* [7]. This paper is logically independent of its predecessor [8]. In [8] we dealt with the case of p-divisible groups; in the present paper we investigate the case of algebras of Witt vectors of finite length. Another example of a class of finite algebras whose p-jet spaces are arithmetically significant is that of Hecke algebras; we hope to undertake the study of this example in a subsequent work.
The present paper is partly motivated by the quest for "absolute geometries" (the so-called "geometries over the field with one element, $\mathbb{F}_1$"); cf. [12] for an overview of various approaches and some history. In particular, according to Borger's approach [3], the geometry over $\mathbb{F}_1$ should correspond to λ-*geometry* (i.e. algebraic geometry in which all rings appearing come equipped with a structure of λ-ring in the sense of Grothendieck). For the case of one prime p the "p-adic completion" of λ-geometry is the δ-*geometry* developed by the author [6, 7], where δ is a p-*derivation* (morally a "Fermat quotient operator"). Now Borger established in [3] an elegant categorical framework which predicts what actual objects should correspond to the basic hypothetical constructions over $\mathbb{F}_1$. According to his framework the hypothetical tensor product $\mathbb{Z} \otimes_{\mathbb{F}_1} \mathbb{Z}$

(which was one of the first objects sought in the quest for $\mathbb{F}_1$) should correspond to the big Witt ring $\mathbb{W}(\mathbb{Z})$ of the integers. Then the hypothetical groupoid structure on $\mathbb{Z}\otimes_{\mathbb{F}_1}\mathbb{Z}$ should correspond to the commonad structure $\Delta : \mathbb{W}(\mathbb{Z}) \to \mathbb{W}(\mathbb{W}(\mathbb{Z}))$. The main interest in $\mathbb{Z} \otimes_{\mathbb{F}_1} \mathbb{Z}$ comes from the fact that this tensor product should be viewed as an arithmetic analog of a surface $X \times X$ where X is a curve (algebraic, analytic, C^∞). With this analogy in mind one is immediately tempted to ask for an arithmetic analogue of the Lie groupoid of X, in the sense of Lie and Cartan, and more recently Malgrange [11]. (Recall that, roughly speaking, a point of the Lie groupoid of X is by definition a pair of points of X together with a formal isomorphism between the germs of X at these two points.) Since the Lie groupoid of X is the infinitesimal version of an automorphism group we should view any arithmetic analogue of the Lie groupoid of X as an infinitesimal version of the "Galois group of $\mathbb{Q}/\mathbb{F}_1$". Now the Lie groupoid of X is an open set in the inverse limit, as $n \to \infty$, of the manifolds $J^n(X \times X/X)$ of "n-jets of formal sections, at various points, of the second projection $X \times X \to X$". Since the arithmetic analogue of the second projection $X \times X \to X$ is the structure morphism $Spec\ \mathbb{W}(\mathbb{Z}) \to Spec\ \mathbb{Z}$, one candidate for an arithmetic analogue of the Lie groupoid of X could be the jet spaces (in the sense of [4]) of the Witt ring $\mathbb{W}(\mathbb{Z})$ over $\mathbb{Z}$. We will not recall the definition of these jet spaces here (because we don't need it) but let us note that they are constructed using derivations and knowing them essentially boils down (in this easy case) to knowing the Kähler differentials $\Omega_{\mathbb{W}(\mathbb{Z})/\mathbb{Z}}$. By the way, the module of Kähler differentials $\Omega_{\mathbb{W}(\mathbb{Z})/\mathbb{Z}}$ is also the starting point for the construction of the deRham-Witt complex of $\mathbb{Z}$ [9]. However using Kähler differentials (equivalently usual derivations) arguably looks like "going arithmetic only half way". What we propose in this paper is to "go arithmetic all the way" and consider p-jet spaces (in the sense of [6]) of Witt rings rather than usual jet spaces (in the sense of [4]) of the same Witt rings. The former are an arithmetic analogue of the latter in which usual derivations are replaced by p-derivations.

A few adjustments are in order. First since p-jet spaces are "local at p" we replace the big Witt ring functor $\mathbb{W}(\ \ )$ by the p-typical Witt functor $W(\ \ )$. Also we replace $\mathbb{Z}$ by $\mathbb{Z}_p$ or, more generally, by the Witt ring $R = W(k)$ on a perfect field k of characteristic p. Finally since $W(R)$ is not of finite type over R we replace $W(R)$ by its truncations $W_m(R)$ (where we use the labeling in [1], so $W_m(R) = R^{m+1}$ as sets.) So after all what we are going to study are the p-jet algebras $J^n(W_m(R))$ and the p-jet maps

$$J^n(\Delta) : J^n(W_{m+m'}(R)) \to J^n(W_m(W_{m'}(R)))$$

induced by the comonad maps $\Delta : W_{m+m'}(R) \to W_m(W_{m'}(R))$; cf. the review of J^n and W_m in the next subsection. Since $W_m(R)$ and $W_m(W_{m'}(R))$ are finite flat R-algebras our investigation here is part of the more general effort to study p-jets $J^n(C)$ of finite flat R-algebras C; the case when $Spec\ C$ is a finite flat p-group scheme was addressed in [8].

1.2. Main concepts and results. For $R = W(k)$ the Witt ring on a perfect field k of characteristic $p \neq 2, 3$ we let $\phi = W(\text{Frob})$ be the automorphism of R defined by the p-power Frobenius Frob of k. (The main examples we have in mind are the ring of p-adic integers $\mathbb{Z}_p = W(\mathbb{F}_p)$ and the completion of the maximum unramified extension of $\mathbb{Z}_p$, $\widehat{\mathbb{Z}_p^{ur}} = W(\mathbb{F}_p^a)$; here $\mathbb{F}_p^a$ is the algebraic closure of $\mathbb{F}_p$.) Let $x, x', x'', ..., x^{(n)}, ...$ be families of variables $x = (x_\alpha)_{\alpha \in \Omega}$, $x' = (x'_\alpha)_{\alpha \in \Omega}$, etc., indexed by the same set Ω, and let $\phi : R[x, x', x'', ...] \to R[x, x', x'', ...]$ be the unique endomorphism extending ϕ on R and satisfying $\phi(x_\alpha^{(r)}) = (x_\alpha^{(r)})^p + p x_\alpha^{(r+1)}$ for $r \geq 0$. Following [6] we define the map of sets (referred to as a *p-derivation*) $\delta : R[x, x', x'', ...] \to R[x, x', x'', ...]$ by the formula

$$\delta F = \frac{\phi(F) - F^p}{p}.$$

Then for any R-algebra $C = R[x]/(f)$, where f is a family of polynomials, we define the *p-jet algebras of C*:

$$J^n(C) = \frac{R[x, x', ..., x^{(n)}]}{(f, \delta f, ..., \delta^n f)}, \quad J^\infty(C) = \frac{R[x, x', x'', ...]}{(f, \delta f, \delta^2 f, ...)}.$$

Note that each $J^{n+1}(C)$ has a natural structure of $J^n(C)$-algebra and we have naturally induced set theoretic maps $\delta : J^n(C) \to J^{n+1}(C)$ and $\delta : J^\infty(C) \to J^\infty(C)$. Note also that ϕ on $R[x, x', x'', ...]$ induces ring homomorphisms $\phi : J^n(C) \to J^{n+1}(C)$ and $\phi : J^\infty(C) \to J^\infty(C)$. (For C of finite type over R we also defined in [6] the *p-jet spaces* of *Spec* C as the formal schemes $J^n(\text{Spec } C) := \text{Spf } (J^n(C))\hat{}$ where $\hat{}$ means p-adic completion; these spaces are very useful when one further looks at non-affine schemes but here we will not need to take this step.)

We need one more piece of terminology. First, for any ring B and element $b \in B$ we let $\overline{B} = B/pB$ and we let $\overline{b} \in \overline{B}$ be the image of b. Assume now the finitely generated R-algebra C comes equipped with an R-algebra homomorphism $C \to R$ which we refer to as an *augmentation*. Then there is a unique lift of the augmentation to an R-algebra homomorphism $J^\infty(C) \to R$ that commutes with δ. Composing the latter with the natural homomorphism $J^n(C) \to J^\infty(C)$ and reducing mod p we get an induced homomorphism $\overline{J^n(C)} \to k$. Let P_n be the kernel of the latter. Consider the ring $\overline{J^n(C)}'$ defined (up to isomorphism) by asking that *Spec* $\overline{J^n(C)}'$ be the connected component of *Spec* $\overline{J^n(C)}$ that contains the prime ideal P_n; we refer to $\overline{J^n(C)}'$ as the *identity component* of $\overline{J^n(C)}$. If $\overline{J^n(C)}''$ is "the" ring such that

$$\text{Spec } \overline{J^n(C)}'' \simeq (\text{Spec } \overline{J^n(C)}) \backslash (\text{Spec } \overline{J^n(C)}')$$

then we call $\overline{J^n(C)}''$ the *complement of the identity component* of $\overline{J^n(C)}$. Clearly

$$\overline{J^n(C)} \simeq \overline{J^n(C)}' \times \overline{J^n(C)}''.$$

Let now C be the Witt ring $W_m(R)$, $m \geq 1$. Recall that $W_m(R)$ is the set R^{m+1} equipped with the unique ring structure which makes the *ghost map* $w : R^{m+1} \to R^{m+1}$, $w_i(a_0, ..., a_m) = a_0^{p^i} + pa_1^{p^{i-1}} + ... + p^i a_i$, a ring homomorphism. Let $v_i = (0, ..., 0, 1, 0, ..., 0) \in W_m(R)$, (1 preceded by i zeroes, $i = 1, ..., m$), set $\pi = 1 - \delta v_1 \in J^1(W_m(R))$, and let $\Omega_m = \{1, ..., m\}$. As usual we denote by $\left(\overline{J^n(W_m(R))}\right)_\pi$ the ring of fractions of $\overline{J^n(W_m(R))}$ with denominators powers of π. The ring $W_m(R)$ comes with a natural augmentation $W_m(R) \to R$ given by the first projection. So we may consider the identity component of $\overline{J^n(W_m(R))}$. The following gives a compete description of this component and also shows this component is $\left(\overline{J^n(W_m(R))}\right)_\pi$:

Theorem 1.1. *For $n \geq 2$ the image of π^p in $\overline{J^n(W_m(R))}$ is idempotent and we have an isomorphism*

$$\left(\overline{J^n(W_m(R))}\right)_\pi \simeq \frac{k[x_i^{(r)}; i \in \Omega_m; 0 \leq r \leq n]}{(x_i x_j, (x_i^{(r)})^p; i, j \in \Omega_m, 1 \leq r \leq n-1)}$$

sending each $\overline{\delta^r v_i}$ into the class of the variable $x_i^{(r)}$.

Indeed by the theorem *Spec* $\left(\overline{J^n(W_m(R))}\right)_\pi$ is connected (indeed irreducible) and contains P_n hence $\left(\overline{J^n(W_m(R))}\right)_\pi$ is isomorphic to the identity component of $\overline{J^n(W_m(R))}$. By the way, since $(1-\pi)^p = 1 - \pi^p$ is also idempotent in $\overline{J^n(W_m(R))}$ it follows that $\left(\overline{J^n(W_m(R))}\right)_{1-\pi}$ is isomorphic to the complement of the identity component of $\overline{J^n(W_m(R))}$.

Next let C be one of the iterated Witt rings $W_m(W_{m'}(R))$, $m, m' \geq 1$, (cf. the next section for more details). Set

$$v_{i,i'} = (0, ..., 0, v_{i'}, 0, ..., 0) \in W_m(W_{m'}(R)),$$

with $v_{i'} \in W_{m'}(R)$ preceded by i zeroes in $W_{m'}(R)$ and set

$$\Pi = (1 - \delta v_{1,0})(1 - \delta v_{0,1}) \in J^1(W_m(W_{m'}(R))),$$

$$\Omega_{m,m'} = (\{0, ..., m\} \times \{0, ..., m'\}) \backslash \{(0,0)\}.$$

There is a natural augmentation of $W_m(W_{m'}(R))$ given by composing the two obvious first projections. Then we have the following complete description for the identity component of $\overline{J^n(W_m(W_{m'}(R)))}$.

Theorem 1.2. *For $n \geq 2$ the image of Π^p in $\overline{J^n(W_m(W_{m'}(R)))}$ is idempotent and we have an isomorphism*

$$\left(\overline{J^n(W_m(W_{m'}(R)))}\right)_\Pi \simeq \frac{k[x_{i,i'}^{(r)}; (i,i') \in \Omega_{m,m'}; 0 \leq r \leq n]}{(x_{i,i'} x_{j,j'}, (x_{i,i'}^{(r)})^p; (i,i'), (j,j') \in \Omega_{m,m'}, 1 \leq r \leq n-1)}$$

sending each $\overline{\delta^r v_{i,i'}}$ into the class of the variable $x_{i,i'}^{(r)}$.

Again the theorem shows that

$$\left(\overline{J^n(W_m(W_{m'}(R)))}\right)_{\Pi} \quad \text{and} \quad \left(\overline{J^n(W_m(W_{m'}(R)))}\right)_{1-\Pi}$$

are isomorphic to the identity component, respectively to the complement of the identity component, of $\overline{J^n(W_m(W_{m'}(R)))}$.

Finally we have the following complete description of the reduction mod p of the map induced by the comonad map:

Theorem 1.3. *The map*

$$\overline{J^\infty(\Delta)} : \overline{J^\infty(W_{m+m'}(R))_\pi} \to \overline{J^\infty(W_m(W_{m'}(R)))_\Pi}$$

sends $x_{i''}^{(r)}$ into the class of

$$\sum_{i+i'=i''} x_{i,i'}, \qquad \textit{if} \quad r=0$$

and into the class of

$$\delta^{r-1}\left(\sum_{i+i'=i''} x'_{i,i'}\right), \qquad \textit{if} \quad r \geq 1.$$

Remark 1.4. The above results give a complete description of the identity components of our objects. On the other hand one can ask for a description of the complements of the identity components. Take for instance $\overline{J^n(W_m(R))}$. This is not a group object so the components different from the identity component cannot be expected to necessarily "look like" the identity component. And this is indeed what happens (in spite of the comonad structure floating around): the complement $\left(\overline{J^n(W_m(R))}\right)_{1-\pi}$ of the identity component looks quite differently (more degenerate) than the identity component $\left(\overline{J^n(W_m(R))}\right)_{\pi}$. Indeed the identity component is a polynomial ring in m variables over a local Artin ring (cf. Theorem 1.1) and hence has Krull dimension m; by contrast, for the complement of the identity component, we have:

Theorem 1.5. *For $n \geq 3$ and $m \geq 2$ the ring $\left(\overline{J^n(W_m(R))}\right)_{1-\pi}$ has Krull dimension $\geq 2m-1$.*

Remark 1.6. The simplicity modulo p of all these p-jet rings and maps may be deceptive. The structure of these objects in characteristic zero is actually extremely complicated and, as in [8], the whole point of this paper is to manage the complexity of the situation in such a way that, eventually, mod p, the situation becomes transparent. On a conceptual level the results of this paper are best understood as an attempt to unravel the "differential geometry" of the "automorphisms of $\mathbb{Z}$ over $\mathbb{F}_1$"; cf. the beginning of our Introduction. The objects introduced and studied in the present paper could then be viewed as an "infinitesimal" replacement (at p) for the elusive absolute Galois group of $\mathbb{Q}$ over $\mathbb{F}_1$.

1.3. Plan of the paper. In Section 2 we review (and give some complements to) the basic theory of Witt vectors. Section 3 is devoted to computing $J^n(C)$ for certain finite flat R-algebras C whose structure constants satisfy some simple divisibility/vanishing axioms. These axioms are in particular satisfied in the cases $C = W_m(R)$ and $C = W_m(W_{m'}(R))$. Using this we derive, in Section 4, the main results of this note, stated above.

1.4. Acknowledgment. This material is based upon work supported by the National Science Foundation under Grant No. 0852591, and by IHES, Bures sur Yvette, and MPI, Bonn. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation, IHES, or MPI. Also the author is indebted to James Borger for explaining some of his insights (and also some technical points) about Witt vectors.

2. Witt rings

In this section we review some basic facts about the rings of Witt vectors which we are going to need in the sequel. For most proofs we refer to [9] and [1]. However, for the convenience of the reader, we will provide proofs for the facts for which we could not find an explicit reference. Note that the labeling of Witt rings in [9] and [1] are different (W_m in [9] is W_{m-1} in [1]); we follow here the labeling in [1].

Fix a prime p and m a non-negative integer or ∞. For any ring A we may consider the *ghost maps* $w_i : A^{m+1} \to A$, $0 \leq i \leq m$, $i < \infty$,

$$w_i(a_0, ..., a_m) = a_0^{p^i} + pa_1^{p^{i-1}} + ... + p^i a_i.$$

Then there is a unique functor W_m from the category of rings to itself such that, for any ring A, we have that $W_m(A) = A^{m+1}$ as sets and the *ghost* map $w = (w_0, ..., w_m) : W_m(A) = A^{m+1} \to A^{m+1}$ is a ring homomorphism where the target A^{m+1} is given the product ring structure. We use the convention $\infty + 1 = \infty - 1 = \infty$ and we write $W(A) = W_\infty(A)$. The ghost map $w : W_m(A) \to A^{m+1}$ is an integral ring homomorphism and has a nilpotent kernel if $0 \leq m < \infty$; it is injective if A is p-torsion free and $0 \leq m \leq \infty$. The rings $W_m(A)$ are called the (p-typical) *rings of Witt vectors of length* $m+1$. There are natural additive maps, functorial in A, called *Verschiebung maps* $V : W_{m-1}(A) \to W_m(A)$ defined by

$$V(a_0, a_1, a_2, ...) = (0, a_0, a_1, a_2, ...).$$

Also there are unique ring homomorphisms, functorial in A, called *Frobenius maps*, $F : W_m(A) \to W_{m-1}(A)$, such that $w \circ F = F^w \circ w$ where $F^w : A^{m+1} \to A^m$ is the shift

$$F^w(b_0, b_1, b_2, ...) = (b_1, b_2, ...).$$

(If $pA = 0$ and $m = \infty$ we have $F = W(\text{Frob})$ where $\text{Frob} : A \to A$ is the p-power Frobenius.) For $m < \infty$ one has also ring homomorphisms $\rho : W_m(A) \to$

$W_{m-1}(A)$ defined by

$$\rho(a_0, a_1, ..., a_m) = (a_0, a_1, ..., a_{m-1}).$$

Finally one has the multiplicative map, called the *Teichmüller map*, $[\ ] = [\ ]_m : A \to W_m(A)$,

$$[a] = (a, 0, 0, ...).$$

These maps are related by the following identities:
1) $F(V(u)) = pu$,
2) $uV(u') = V(F(u)u')$,
3) $F([a]) = [a^p]$,
4) If $pA = 0$ then $V(F(u)) = pu$.
It is also convenient to introduce the maps $V^i_m = V^i \circ [\ ]_{m-i} : A \to W_m(A)$, $0 \leq i \leq m < \infty$. Then $V^i_m(a) = (0, ..., 0, a, 0, ..., 0)$ where a is preceded by i zeroes. We have the identities:

$$V^i_m(a) \cdot V^j_m(b) = p^i \cdot V^j_m(a^{p^{j-i}} b), \quad 0 \leq i \leq j \leq m, \tag{2.1}$$

$$w(V^i_m(a)) = (0, ..., 0, p^i a, p^i a^p, p^i a^{p^2}, ...). \tag{2.2}$$

Also, for any $N \in \mathbb{Z}$ we have the following formula for the Teichmüller map [9]:

$$[N]_m = \sum_{t=0}^{m} c_t(N) V^t_m(1)$$

where $c_0(N) = N$ and

$$c_t(N) = \frac{N^{p^t} - N^{p^{t-1}}}{p^t}, \quad t \geq 1.$$

If A is p-torsion free so is $W_m(A)$. Now if A is p-torsion free and $\phi : A \to A$ is a ring homomorphism lifting the p-power Frobenius on A/pA then there is a unique ring homomorphism $\lambda_\phi : A \to W_m(A)$ such that $w_i(\lambda_\phi(a)) = \phi^i(a)$ for all i; if in addition A/pA is perfect then λ_ϕ induces an isomorphism $A/p^{m+1}A \simeq W_m(A/pA)$.

Lemma 2.1. *Let A be a p-torsion free ring equipped with a ring automorphism $\phi : A \to A$ lifting the p-power Frobenius on A/pA. Let $0 \leq m < \infty$ and view $W_m(A)$ as an A-algebra via the homomorphism $\lambda_\phi : A \to W_m(A)$. Set $v_i = V^i_m(1)$, $0 \leq i \leq m$. Then $\{v_i; 0 \leq i \leq m\}$ is an A-basis for $W_m(A)$ and $v_i v_j = p^i v_j$ for $i \leq j$.*

Proof. The case $A = \mathbb{Z}_p$ is in [1]. The general case is similar but for convenience we recall the argument. If $w : W_m(A) \to A^{m+1}$, by (2.2) and by the injectivity of ϕ, we have that $w(v_i)$ are A-linearly independent in A^{m+1} (the latter viewed as an A-algebra via $(1, \phi, ..., \phi^m) : A \to A^{m+1}$). Hence v_i are A-linearly independent. To check that v_i span $W_m(A)$ we proceed by induction on m. For $m = 0$ this is clear. Assume spanning holds for $m - 1$. The kernel of the map $W_m(A) \to W_{m-1}(A)$ is $V^m_m(A) = \{(0, ..., 0, a); a \in A\}$. By induction the images of $v_0, ..., v_{m-1}$ in $W_{m-1}(A)$ generate $W_{m-1}(A)$ so it is enough to show that v_m generates $V_m^m(A)$ as an A-module. This follows from the equality

$$\lambda_\phi(a) \cdot v_m = (0, ..., 0, \phi^m(a)),$$

plus the fact that ϕ is surjective. The last assertion of the Lemma follows from (2.1). $\square$

Lemma 2.2. *With notation as in Lemma* 2.1 *the Frobenius map* $F : W_m(A) \to W_{m-1}(A)$ *is the unique* ϕ*-linear map with* $F(v_i) = p \cdot \rho(v_{i-1})$, $1 \leq i \leq m$, $v_0 = 1$.

Proof. The equalities $F(v_i) = p \cdot \rho(v_{i-1})$ follow from the identity $FV = p \cdot \mathrm{id}$. We are left to prove that $F \circ \lambda_\phi = \lambda_\phi \circ \phi : A \to W_{m-1}(A)$. It is enough to show that $w \circ F \circ \lambda_\phi = w \circ \lambda_\phi \circ \phi$. This follows from the following computation:

$$\begin{array}{rcl} w \circ F \circ \lambda_\phi & = & F^w \circ w \circ \lambda_\phi \\ & = & F^w \circ (1, \phi, ..., \phi^m) \\ & = & (\phi, ..., \phi^m) \\ & = & (1, ..., \phi^{m-1}) \circ \phi \\ & = & w \circ \lambda_\phi \circ \phi. \end{array}$$

$\square$

Lemma 2.3. *Let A be Noetherian a p-torsion free ring equipped with a ring automorphism $\phi : A \to A$ lifting the p-power Frobenius on A/pA. Let $u : A \to B$ be a p-torsion free A-algebra, let $0 \leq m < \infty$, and view $W_m(B)$ as an A-algebra via the homomorphism $A \xrightarrow{\lambda_\phi} W_m(A) \xrightarrow{W_m(u)} W_m(B)$. If B is a finitely generated A-algebra (respectively a finite A-module) then $W_m(B)$ is also a finitely generated A-algebra (respectively a finite A-module).*

Proof. The ghost map $w : W_m(B) \to B^{m+1}$ is injective and integral. Now if B is a finitely generated A-algebra (respectively a finite A-module) then so is B^{m+1} (with the A-algebra structure given by $(1, \phi, ..., \phi^m) : A \to A^{m+1} \to B^{m+1}$), because ϕ is bijective. In the finite case, by Noetherianity $W_m(B)$ is a finite A-algebra. In the finitely generated case it follows that B^{m+1} is finite over $W_m(B)$ and hence, by the Artin-Tate lemma $W_m(B)$ is a finitely generated A-algebra. $\square$

Next we discuss iterated Witt vectors. One proves (cf. e.g. [9]) that $F : W(A) \to W(A)$ lifts the p-power Frobenius on $W(A)/pW(A)$. So for A p-torsion free, since $W(A)$ is also p-torsion free, we have at our disposal a ring homomorphism $\Delta = \lambda_F : W(A) \to W(W(A))$ which composed with any ghost map $w_i : W(W(A)) \to W(A)$ equals the i-th iterate F^i. Then one trivially checks that the composition

$$W(A) \xrightarrow{\Delta} W(W(A)) \xrightarrow{w} W(A)^\infty \xrightarrow{w^\infty} (A^\infty)^\infty$$

equals the composition

$$W(A) \xrightarrow{w} A^\infty \xrightarrow{\Delta^w} (A^\infty)^\infty,$$

where, if we write the elements of $(A^\infty)^\infty$ as

$$((a_{00},a_{01},a_{02},...),(a_{10},a_{11},a_{12},...),(a_{20},a_{21},a_{22},...),...) = \begin{pmatrix} a_{00} & a_{01} & a_{02} & ... \\ a_{10} & a_{11} & a_{12} & ... \\ a_{20} & a_{21} & a_{22} & ... \\ ... & ... & ... & ... \end{pmatrix}$$

then

$$\Delta^w(a_0,a_1,a_2,...) = \begin{pmatrix} a_0 & a_1 & a_2 & ... \\ a_1 & a_2 & a_3 & ... \\ a_2 & a_3 & a_4 & ... \\ ... & ... & ... & ... \end{pmatrix}. \tag{2.3}$$

Using this plus the injectivity of the map w one immediately checks that if $a_i = 0$ for $i \leq m + m'$ then $\Delta(a_0, a_1, a_2, ...)$ is in the kernel of $W(W(A)) \to W_m(W_{m'}(A))$. So we have induced ring homomorphisms

$$\Delta_{(m,m')} : W_{m+m'}(A) \to W_m(W_{m'}(A)).$$

These homomorphisms (and Δ) were constructed for A p-torsion free but, as usual, one extends this construction uniquely to all rings in a functorial manner. Also one immediately checks (composing with ghost maps) that the following diagram is commutative:

$$\begin{array}{ccc} W(A) & \stackrel{\Delta}{\longrightarrow} & W(W(A)) \\ F \downarrow & & \downarrow F \\ W(A) & \stackrel{\Delta}{\longrightarrow} & W(W(A)) \end{array} \tag{2.4}$$

Lemma 2.4. *Let $R = W(k)$ be the Witt ring on a perfect field of characteristic p and $\phi : R \to R$ the Frobenius. Let $0 \leq m, m' < \infty$. Then:*
1) $W_m(W_{m'}(R))$ is a finite R-algebra, where the structure morphism is given by $R \xrightarrow{\lambda_\phi} W_m(R) \xrightarrow{W_m(\lambda_\phi)} W_m(W_{m'}(R))$.
2) If $W_{m+m'}(R)$ is viewed as an R-algebra via $\lambda_\phi : R \to W_{m+m'}(R)$ then the morphism $\Delta_{(m,m')} : W_{m+m'}(R) \to W_m(W_{m'}(R))$ is an R-algebra homomorphism.

Proof. The first assertion follows from Lemma 2.3. The second assertion follows from the "coassociativity" property in [9], p 15. $\square$

Lemma 2.5. *For any $a \in A$, $s \in \mathbb{Z}_+$, and $0 \leq i \leq m < \infty$ we have the following formula in $W_m(A)$:*

$$V_m^i(p^s a) = \sum_{t=0}^{m-i} c_t(p^s) V_m^{i+t}(a^{p^t}).$$

Proof.

$$\begin{aligned}
V^i_m(p^s a) &= V^i([p^s a]_{m-i}) \\
&= V^i([p^s]_{m-i}[a]_{m-i}) \\
&= V^i(\textstyle\sum_{t=0}^{m-i} c_t(p^s) V^t_{m-i}(1) V^0_{m-i}(a)) \\
&= \textstyle\sum_{t=0}^{m-i} c_t(p^s) V^i(V^t_{m-i}(1) V^0_{m-i}(a))) \\
&= \textstyle\sum_{t=0}^{m-i} c_t(p^s) V^i(V^t_{m-i}(a^{p^t})) \\
&= \textstyle\sum_{t=0}^{m-i} c_t(p^s) V^{i+t}([a^{p^t}]_{m-i-t}) \\
&= \textstyle\sum_{t=0}^{m-i} c_t(p^s) V^{i+t}_m(a^{p^t}).
\end{aligned}$$

□

Lemma 2.6. *Let $R = W(k)$, k a perfect field of characteristic $p \geq 5$, $\phi : R \to R$ the lift of Frobenius on R, $u : R \to A$ a p-torsion free finite R-algebra (e.g. $A = W_{m'}(R)$ for some $0 \leq m' < \infty$), let $0 \leq m < \infty$, and $W_m(A)$ be viewed as an R-algebra via $R \xrightarrow{\lambda_\phi} W_m(R) \xrightarrow{W_m(u)} W_m(A)$. Moreover let $a \in A$, $a^2 = p^\nu a$ (e.g. $a = V^{i'}_{m'}(1)$, in which case $\nu = i'$). Then for any $s \geq 0$ and $0 \leq i \leq m$ we have*

$$V^i_m(p^s a) \in p^s V^i_m(a) + p^{s+1} \sum_{t=0}^{m-i-1} R \cdot V^{i+t+1}_m(a).$$

(For $i = m$ the sum in the right hand side is, by definition, zero.)

Proof. For $0 \leq i \leq m$ onsider the R-modules

$$\begin{aligned}
M^i_m &= \textstyle\sum_{t=0}^{m-i} \sum_{r \geq 0} R \cdot V^{i+t}(p^r a) &\subset\ & W_m(A) \\
N^i_m &= \textstyle\sum_{t=0}^{m-i} R \cdot V^{i+t}(a) &\subset\ & M^i_m.
\end{aligned}$$

Also set $M^i_m = N^i_m = 0$ for $i > m$. Since $W_m(A)$ is a finite R-algebra the modules M^i_m and N^i_m are finitely generated. By Lemma 2.5, for $s \geq 1$ we have

$$\begin{aligned}
V^i_m(p^s a) &= \textstyle\sum_{t=0}^{m-i} c_t(p^s) V^{i+t}_m(a^{p^t}) \\
&= p^s V^i_m(a) + \textstyle\sum_{t=1}^{m-i} c_t(p^s) V^{i+t}_m(p^{(p^t-1)\nu} a) \\
&= p^s V^i_m(a) + \textstyle\sum_{t=1}^{m-i} \sum_{r=0}^{m-i-t} c_t(p^s) c_r(p^{(p^t-1)\nu}) V^{i+t+r}_m(a^{p^r}) \\
&= p^s V^i_m(a) + \textstyle\sum_{t=1}^{m-i} \sum_{r=0}^{m-i-t} c_t(p^s) c_r(p^{(p^t-1)\nu}) V^{i+t+r}_m(p^{(p^r-1)\nu} a) \\
&\in p^s V^i_m(a) + p^{s+1} M^{i+1}_m,
\end{aligned}$$

because for $p \geq 5$, $s \geq 1$, $t \geq 1$, $\nu \geq 1$, $r \geq 0$ we have $p^{s-1}|c_t(p^s)$ and $p^2|c_r(p^{(p^t-1)\nu})$. In particular

$$\begin{aligned} M_m^i &\subset N_m^i + pM_m^i \\ &\subset N_m^i + p(N_m^i + pM_m^i) = N_m^i + p^2 M_m^i \\ &\subset N_m^i + p^2(N_m^i + pM_m^i) = N_m^i + p^3 M_m^i, \quad \text{etc.} \end{aligned}$$

Hence

$$N_m^i \subset M_m^i \subset \bigcap_{r=1}^{\infty} (N_m^i + p^r M_m^i) = N_m^i,$$

because M_m^i is a finitely generated R-module and hence N_m^i is p-adically separated. So $M_m^i = N_m^i$. So for all $s \geq 0$ we have

$$V_m^i(p^s a) \in p^s V_m^i(a) + p^{s+1} N_m^{i+1},$$

which is what we had to prove. $\square$

Lemma 2.7. *Let $R = W(k)$, k a perfect field of characteristic p. For $0 \leq i \leq m < \infty$ and $0 \leq i' \leq m' < \infty$ set*

$$v_{i,i'} = V_m^i(V_{m'}^{i'}(1)) \in W_m(W_{m'}(R)). \tag{2.5}$$

Then the family $\{v_{i,i'}\}$ is R-linearly independent in $W_m(W_{m'}(R))$ where the latter is viewed as an R-algebra via the map

$$R \xrightarrow{\lambda_\phi} W_m(R) \xrightarrow{W_m(\lambda_\phi)} W_m(W_{m'}(R))$$

Proof. First it is trivial to check that the composition

$$R \xrightarrow{\lambda_\phi} W(R) \xrightarrow{W(\lambda_\phi)} W(W(R)) \xrightarrow{w} W(R)^\infty \xrightarrow{w^\infty} (R^\infty)^\infty \tag{2.6}$$

is given by

$$a \mapsto \begin{pmatrix} a & \phi(a) & \phi^2(a) & ... \\ \phi(a) & \phi^2(a) & \phi^3(a) & \\ \phi^2(a) & \phi^3(a) & \phi^4(a) & ... \\ ... & ... & ... & ... \end{pmatrix}.$$

Next note that the images of $w^\infty(w(v_{i,i'}))$ in $(R^{m'+1})^{m+1}$ are R-linearly independent (where $(R^{m'+1})^{m+1}$ is an R-algebra via the map (2.6)); indeed the matrix

$$w^\infty(w(v_{i,i'})) = \begin{pmatrix} 0 & ... & 0 & 0 & 0 & ... \\ ... & ... & ... & ... & ... & ... \\ 0 & ... & 0 & 0 & 0 & ... \\ 0 & ... & 0 & p^{i+i'} & p^{i+i'} & ... \\ 0 & ... & 0 & p^{i+i'p} & p^{i+i'p} & ... \\ 0 & ... & 0 & p^{i+i'p^2} & p^{i+i'p^2} & ... \\ ... & ... & ... & ... & ... & ... \end{pmatrix} \tag{2.7}$$

with the first i rows and i' columns zero. The assertion of the Lemma now follows. $\square$

Lemma 2.8. *Let $R = W(k)$, k a perfect field of characteristic $p \geq 5$. For $0 \leq i \leq m < \infty$ and $0 \leq i' \leq m' < \infty$ let $v_{i,i'}$ be as in (2.5). Then for $0 \leq i \leq j \leq m$, $i', j' \in \{0, ..., m'\}$, and $1 \leq t \leq m - j$ there exist unique elements $c_{ii'jj't} \in R$ such that the following equalities hold in $W_m(W_{m'}(R))$:*

$$v_{i,i'} \cdot v_{j,j'} = \begin{cases} p^{i+i'p^{j-i}} v_{j,j'} + p^{i+i'p^{j-i}+1} \sum_{t=1}^{m-j} c_{ii'jj't} \cdot v_{j+t,j'}, & i' \leq j' \\ \\ p^{i+i'(p^{j-i}-1)+j'} v_{j,i'} + p^{i+i'(p^{j-i}-1)+j'+1} \sum_{t=1}^{m-j} c_{ii'jj't} \cdot v_{j+t,i'}, & i' \geq j' \end{cases}$$

Proof. Uniqueness of the c's follows from Lemma 2.7. Let us prove the existence of the c's. We have

$$\begin{aligned} v_{i,i'} \cdot v_{j,j'} &= p^i V_m^j (V_{m'}^{i'}(1)^{p^{j-i}} V_{m'}^{j'}(1)) \\ &= p^i V_m^j (p^{(p^{j-i}-1)i'} V_{m'}^{i'}(1) V_{m'}^{j'}(1)). \end{aligned}$$

The latter equals $p^i V_m^j (p^{i'p^{j-i}} V_{m'}^{j'}(1))$ if $i' \leq j'$ and $p^i V_m^j (p^{i'(p^{j-i}-1)+j'} V_{m'}^{i'}(1))$ if $i' \geq j'$. We conclude by Lemma 2.6. $\square$

Lemma 2.9. *Let $R = W(k)$, k a perfect field of characteristic $p \geq 5$, let $m, m' < \infty$, and view $W_m(W_{m'}(R)$ as an R-algebra via the homomorphism $W_m(\lambda_\phi) \circ \lambda_\phi : R \to W_m(R) \to W_m(W_{m'}(R))$. Then $\{v_{i,i'}; 0 \leq i \leq m, 0 \leq i' \leq m'\}$ is an R-basis for $W_m(W_{m'}(R))$.*

Proof. Linear independence was proved in Lemma 2.7. To prove generation we fix m', set $A = W_{m'}(R)$, and proceed by induction on m. The case $m = 0$ is Lemma 2.1. For the induction step we need to show that the kernel of the map $W_m(A) \to W_{m-1}(A)$ (which equals $V^m(A) = \{(0, ..., 0, a); a \in A\}$) is generated as an R-module by $v_{m,j'}$. By Lemma 2.1 the R-module A is generated by the $v_{j'}$'s and note that $v_{m,j'} = V^m(v_{j'})$. So to conclude it is enough to show that the map $V^m : A_{\phi^m} \to V^m(A)$ is an isomorphism of R-modules where A_{ϕ^m} is A viewed as an R-module via the map $R \xrightarrow{\phi^m} R \xrightarrow{\lambda_\phi} A$. The map $V^m : A_{\phi^m} \to V^m(A)$ is clearly a bijection. So we are reduced to check that $V^m : A_{\phi^m} \to W_m(A)$ is an R-module homomorphism. It is enough to check that the composition $w \circ V^m : A_{\phi^m} \to W_m(A) \to A^{m+1}$ (which by the way is given by $a \mapsto (0, ..., 0, p^m a)$), is an R-module homomorphism where A^{m+1} is an R-algebra via the map $(\lambda_\phi)^{m+1} \circ (1, \phi, ..., \phi^m) : R \to R^{m+1} \to A^{m+1}$. This is however trivial to check. $\square$

Lemma 2.10. *With notation as in Lemmas 2.1 and 2.9 the comultiplication $\Delta = \Delta_{(m,m')} : W_{m+m'}(R) \to W_m(W_{m'}(R))$ is given by*

$$\Delta v_{i''} = \sum_{i,i'} a_{i,i',i''} v_{i,i'}, \quad 0 \leq i'' \leq m + m', \tag{2.8}$$

where $a_{i,i',i''} \in \mathbb{Z}$. Moreover we have the following relations:
1) $a_{i,i',i''} = 0$ for $i + i' < i''$,

2) $a_{i,i',i''} = 1$ *for* $i + i' = i''$,
3) $a_{i,0,i''} = 0$ *for* $i > i''$,
4) $a_{i,i',i''} = 0$ *for* $i' > i''$,
5) $a_{i,i',i''} \in p\mathbb{Z}$ *for* $i + i' > i''$,
6) For $i + i' \geq i'' + 1$, *and* $i, i' \geq 1$,

$$a_{i,i',i''} = -\sum_{j=i''-i'}^{i-1} a_{j,i',i''} p^{j+i'p^{i-j}-i-i'}. \tag{2.9}$$

Note that the relations above allow one to recurrently determine all the coefficients $a_{i,i',i''}$.

Proof of Lemma 2.10. Let $K = Frac(R)$ and let $M(i'')$ be the linear subspace of the space of all $(m+1)\times(m'+1)$-matrices $(K^{m'+1})^{m+1}$ consisting of all matrices $(r_{i,i'})$ with $r_{i,i'} = 0$ for $i + i' < i''$. Since the elements $w^\infty(w(v_{i,i'})) \in M(i'')$ for $i + i' \geq i''$ and since these elements are K-linearly independent it follows that these elements form a basis of $M(i'')$. By (2.2) and (2.3) we have that

$$w^\infty(w(\Delta(v_{i''}))) = \left(\begin{array}{ccccccc} 0 & ... & 0 & 0 & p^{i''} & p^{i''} & ... \\ 0 & ... & 0 & p^{i''} & p^{i''} & p^{i''} & ... \\ 0 & ... & p^{i''} & p^{i''} & p^{i''} & p^{i''} & ... \\ ... & ... & ... & ... & ... & ... & ... \end{array} \right)$$

with i'' zeros on the first line. So $w^\infty(w(\Delta(v_{i''})))$ belongs to $M(i'')$, hence we get an equality as in (2.8) with $a_{i,i',i''} \in K$ and relation 1) holding. Since $v_{i,i'}$ form a basis of $W_m(W_{m'}(R))$ we get that $a_{i,i',i''} \in R$. Picking out the (i,i')-entry in (2.8) and using (2.7) we get the relation

$$p^{i''} = \sum_{j+j' \geq i'', j \leq i, j' \leq i'} a_{j,j',i''} p^{j+j'p^{i-j}}. \tag{2.10}$$

Relations 2) follows immediately. Relation 3) follows by induction. To prove relation 6) subtract the equality (2.10) with i' replaced by $i'-1$ from the equality (2.10) and divide by $p^{i+i'}$. Relation 4) for $i = 0$ follows by induction from (2.10). Relation 4) for arbitrary i follows by induction from 6). Relations 1), 2), and 6) imply relation 5) by induction. By 1), 2), and 5) we have $a_{i,i',i''} \in \mathbb{Z}$ for all i, i', i''. □

Remark 2.11. It is easy to see directly from the definitions that for any $\mathbb{Z}_p$-algebra C we have an isomorphism of $\mathbb{Q}_p$-algebras

$$J^n(C) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq (C \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\otimes(n+1)}$$

which for any $c \in C$ sends $c^{\phi^s} := \phi^s(c)$ into $1 \otimes ... \otimes 1 \otimes c \otimes 1 \otimes ... \otimes 1$ (c on position s with positions labled from 0 to n). Hence we have $\mathbb{Q}_p$-algebra isomorphisms

$$
\begin{array}{rcl}
J^n(W_m(\mathbb{Z}_p)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p & \simeq & (W_m(\mathbb{Z}_p) \otimes \mathbb{Q}_p)^{\otimes(n+1)} \\
 & \simeq & (\prod^{m+1} \mathbb{Q}_p)^{\otimes(n+1)} \\
 & \simeq & \prod^{(m+1)^{n+1}} \mathbb{Q}_p
\end{array}
\tag{2.11}
$$

where $\prod^N$ means N-fold product in the category of rings. If we set $v_0 = 1$ and $v_{m+1} = 0$ then the isomorphism $W_m(\mathbb{Z}_p) \otimes \mathbb{Q}_p \simeq \prod^{m+1} \mathbb{Q}_p$ is defined by the family of orthogonal idempotents

$$\frac{v_j}{p^j} - \frac{v_{j+1}}{p^{j+1}} \in W_m(\mathbb{Z}_p) \otimes \mathbb{Q}_p, \quad 0 \leq j \leq m.$$

Hence the isomorphism (2.11) is defined by the family of orthogonal idempotents

$$\prod_{s=0}^{n} \left(\frac{v_{j_s}}{p^{j_s}} - \frac{v_{j_s+1}}{p^{j_s+1}} \right)^{\phi^s} \in J^n(W_m(\mathbb{Z}_p)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \quad j_0, ..., j_n \in \{0, ..., m\}. \tag{2.12}$$

In particular the whole complexity of $J^n(W_m(\mathbb{Z}_p))$ disappears after tensorization with $\mathbb{Q}_p$ and hence it is an "integral" phenomenon. On the other hand, by the above, the $\mathbb{Z}_p$-algebra

$$J^n(W_m(\mathbb{Z}_p))/\text{torsion}$$

is a free $\mathbb{Z}_p$-module of rank $(m+1)^{n+1}$ that retains most (but not all) of the complexity of $J^n(W_m(\mathbb{Z}_p))$. For instance if one considers the surjection

$$\overline{J^n(W_m(\mathbb{Z}_p))} \to \overline{J^n(W_m(\mathbb{Z}_p))/\text{torsion}} \tag{2.13}$$

then the target of this surjection is an $\mathbb{F}_p$-vector space of dimension $(m+1)^{n+1}$ whereas the source of this surjection is, by Theorem 1.1, an infinite dimensional $\mathbb{F}_p$-vector space; in fact this source, $\overline{J^n(W_m(\mathbb{Z}_p))}$, is a product of two algebras: the identity component of $\overline{J^n(W_m(\mathbb{Z}_p))}$ and the complement of the identity component. By Theorem 1.1, the identity component is a polynomial algebra in

$$\delta^n v_1, ..., \delta^n v_m \in \overline{J^n(W_m(\mathbb{Z}_p))}$$

over an Artin local subring of $\overline{J^n(W_m(\mathbb{Z}_p))}$ whose dimension as an $\mathbb{F}_p$-vector space is $2p^{n-1}m^n$. Indeed one can take as an $\mathbb{F}_p$-vector space basis for this Artin ring the elements

$$v_{j_0}^{e_0}(\delta v_{j_1})^{e_1} ... (\delta^{n-1} v_{j_{n-1}})^{e_{n-1}} \in \overline{J^n(W_m(\mathbb{Z}_p))}, \tag{2.14}$$

$$e_0 \in \{0, 1\}, \quad e_1, ..., e_{n-1} \in \{0, ..., p-1\}.$$

It is interesting to compare the two families (2.12) and (2.14).

Remark 2.12. We end by discussing the link between p-jets and Witt vectors. The discussion that follows will be helpful to set up notation for later and to put things into the right perspective. However, the adjunction properties that will be explained below have, by themselves, very little impact on the unraveling of the structure of p-jet spaces.

The following concept was introduced independently by Joyal [10] and the author [6]. A p-derivation from a ring A into an A-algebra B is a map of sets $\delta : A \to B$ such that the map $A \to W_1(B)$, $a \mapsto (a, \delta a)$ is a ring homomorphism. (Here we identify a with $a \cdot 1_B$.) A δ-ring is a ring A equipped with a p-derivation $A \to A$. The category of δ-rings is the category whose objects are the δ-rings and whose morphisms are the ring homomorphisms that commute with δ. By definition a p-derivation $\delta : A \to B$ satisfies

$$\begin{array}{rcl} \delta(x+y) & = & \delta x + \delta y + C_p(x,y) \\ \delta(xy) & = & x^p \delta y + y^p \delta x + p \delta x \delta y, \end{array}$$

where C_p is the polynomial:

$$C_p(X,Y) = p^{-1}(X^p + Y^p - (X+Y)^p) \in \mathbb{Z}[X,Y].$$

If δ is as above then $\phi : A \to B$, $\phi(x) = x^p + p\delta x$, is a ring homomorphism. Note that $\delta(xy) = x^p \delta y + \phi(y)\delta x = y^p \delta x + \phi(x) \delta y$. Also δ and ϕ commute. If A is p-torsion free then δ is, of course, uniquely determined by ϕ; also

$$\delta(x_1 + ... + x_m) = \delta x_1 + ... + \delta x_m + C_{mp}(x_1, ..., x_m), \tag{2.15}$$

where

$$C_{mp}(X_1, ..., X_m) := p^{-1}(\sum_{i=1}^m X_i^p - (\sum_{i=1}^m X_i)^p) \in \mathbb{Z}[X_1, ..., X_m].$$

Note that for any ring A the ring $W(A)$ has a structure of δ-ring which functorial in A; it is given by the composition $W(A) \xrightarrow{\Delta} W(W(A)) \to W_1(W(A))$. According to a result of Joyal [10] (which will not be needed in the sequel) for any ring A and any δ-ring B we have

$$Hom_{\text{rings}}(B^!, A) \simeq Hom_{\delta-\text{rings}}(B, W(A)),$$

where ! is the forgetful functor from δ-rings to rings. More generally if R is a δ-ring by a δ-ring over R we shall mean a δ-ring equipped with a δ-ring homomorphism from R into it. Similarly a ring over R will mean an R-algebra. Then the above adjunction property implies that for any δ-ring B over R and any ring A over R,

$$Hom_{\text{rings}/R}(B^!, A) \simeq Hom_{\delta-\text{rings}/R}(B, W(A)),$$

where $W(A)$ is an R-algebra via $R \to W(R) \to W(A)$. Let now $R = W(k)$ with k a perfect field of characteristic p. Recall that for any R-algebra we defined in the Introduction R-algebras $J^n(C)$ and $J^\infty(C)$. The set theoretic maps $\delta : J^n(C) \to J^{n+1}(C)$ and $\delta : J^\infty(C) \to J^\infty(C)$ constructed in the Introduction are then p-derivations and we have the following adjunction property: for any δ-ring D over R and any ring C over R we have

$$Hom_{\text{rings}/R}(C, D^!) \simeq Hom_{\delta-\text{rings}/R}(J^\infty(C), D).$$

Putting together the two adjunction properties above we get

$$Hom_{\text{rings}/R}(J^\infty(C)^!, A) \simeq Hom_{\delta-\text{rings}/R}(J^\infty(C), W(A)) \simeq Hom_{\text{rings}/R}(C, W(A)^!)$$

for any rings A and C over R.

It is sometimes useful to use a universality property that is more refined than that of J^∞. To that purpose let us define a *prolongation sequence* to be a sequence

$$B^0 \xrightarrow{\varphi_0} B^1 \xrightarrow{\varphi_1} B^2 \xrightarrow{\varphi_2} ...$$

of ring homomorphisms which is equipped with p-derivations

$$B^0 \xrightarrow{\delta} B^1 \xrightarrow{\delta} B^2 \xrightarrow{\delta} ...$$

such that $\varphi_n \circ \delta = \delta \circ \varphi_{n-1}$ for all n. We denote by B^* a prolongation sequence as above. A morphism of prolongation sequences $B^* = (B^n)$ and $C^* = (C^n)$ is by definition a sequence of morphisms $B^n \to C^n$ that commute, in the obvious sense, with the φs and the δs. Clearly, for any ring C, $J^*(C) := (J^n(C))$ is naturally a prolongation sequence. Moreover, for any prolongation sequence $D^* = (D^n)$ and any ring C we have

$$Hom_{\text{rings}}(C, D^0) \simeq Hom_{\text{prol.seq.}}(J^*(C), D^*).$$

Finally consider the prolongation sequence $R^* = (R^n)$ where all R^n are $R = W(k)$, k a perfect field of characteristic p, and all φ are the identity. By a prolongation sequence over R we understand a morphism of prolongation sequences $R^* \to B^*$; we have a natural notion of morphism of prolongation sequences over R^*. Clearly, for any ring C over R, $J^*(C) := (J^n(C))$ is naturally a prolongation sequence over R. Moreover, for any prolongation sequence $D^* = (D^n)$ over R and any ring C over R we have

$$Hom_{\text{rings}/R}(C, D^0) \simeq Hom_{\text{prol.seq.}/R}(J^*(C), D^*).$$

Note that for any ring A over R the morphisms $\Delta : W_m(A) \to W_1(W_{m-1}(A))$ induce p-derivations $\delta : W_m(A) \to W_{m-1}(A)$ which, for each N, fit into a prolongation sequence

$$W_N(A) \stackrel{\delta}{\to} W_{N-1}(A) \stackrel{\delta}{\to} ... \stackrel{\delta}{\to} W_0(A) = A \to 0 \to 0 \to ...$$

This is a prolongation sequence over R because of the ϕ-linearity of $F : W_m(R) \to W_{m-1}(R)$ and hence of $F : W_m(A) \to W_{m-1}(A)$; cf. Lemma 2.2. So by the universality property for prolongation sequences we have a natural (compatible) family of R-homomorphisms:

$$s : J^n(W_N(A)) \to W_{N-n}(A) \tag{2.16}$$

for $0 \leq n \leq N$. Note that for any R-algebra A the p-derivation $\delta : W_m(A) \to W_{m-1}(A)$ sends v_i into

$$\delta v_i = \rho(v_{i-1}) - p^{i(p-1)-1}\rho(v_i) \tag{2.17}$$

for $i = 1, ..., m$, where $v_0 = 1$. Indeed it is enough to show this for $A = R$ in which case this follows from Lemmas 2.1 and 2.2. Finally note that by the commutativity of (2.4) if m' is fixed and m varies the morphisms $\Delta : W_{m+m'}(R) \to W_m(W_{m'}(R))$ fit into a morphism of prolongation sequences. This induces commutative diagrams

$$\begin{array}{ccc} J^n(W_{m+m'}(R)) & \stackrel{J^n(\Delta)}{\longrightarrow} & J^n(W_m(W_{m'}(R))) \\ s\downarrow & & \downarrow s \\ W_{m+m'-n}(R) & \stackrel{\Delta}{\longrightarrow} & W_{m-n}(W_{m'}(R)) \end{array} \tag{2.18}$$

Remark 2.13. If the upper row of the diagram 2.18, for m, m', n variable, is viewed as the "Lie groupoid of the integers" (i.e. an arithmetic analogue, for the integers, of the Lie groupoid of the line) then one is tempted to view the bottom row of the above diagram as an analogue of a "subgroupoid" of that "Lie groupoid". However this candidate for a "subgroupoid" is contained in the "complement of the identity component" of the "Lie groupoid of integers"; cf. Remark 4.7.

3. p-jets and p-triangular bases

Let R be any ring, and let C be a commutative unital R-algebra, equipped with an R-algebra homomorphism $C \to R$. Let C^+ be the kernel of this homomorphism and assume C^+ is a free R-module of finite rank. Let $\{v_\alpha; \alpha \in \Omega\}$ be an R-basis of C^+ where Ω is a finite set equipped with a total order $\leq$. Write

$$v_\alpha \cdot v_\beta = \sum_{\gamma\in\Omega} c_{\alpha\beta\gamma} v_\gamma$$

for $\alpha \leq \beta$, where $c_{\alpha\beta\gamma} \in R$. Let x be a collection of variables x_α indexed by $\alpha \in \Omega$ and

$$Q_{\alpha\beta} = x_\alpha x_\beta - \sum_{\gamma\in\Omega} c_{\alpha\beta\gamma} x_\gamma \in R[x].$$

Lemma 3.1. *The R-algebra map*

$$R[x]/(Q_{\alpha\beta}; \alpha \leq \beta) \to C$$

sending $x_\alpha \mapsto v_\alpha$ is an isomorphism.

Proof. Indeed the source is generated as an R-module by 1 and the classes of x_α so the algebra map above is injective (because 1 and the v_α's are linearly independent) and surjective (because 1 and the v_α's generate C). □

Definition 3.2. Let C and C^+ be as above and let p be a prime. Let us say that v_α is a *p-triangular basis* of C^+ if for all $\alpha \leq \beta$ and all γ the structure constants $c_{\alpha\beta\gamma}$ satisfy the following conditions:
1) $c_{\alpha\beta\gamma} = 0$ for $\gamma < \alpha$;
2) $c_{\alpha\beta\gamma} \equiv 0 \mod p^2$ for $\gamma \neq \beta$;
3) $c_{\alpha\beta\beta} \equiv p\epsilon_{\alpha\beta} \mod p^2$ where $\epsilon_{\alpha\beta} \in \{0, 1\}$.

For the rest of this section, we assume that C^+ possesses a p-triangular basis v_α, $\alpha \in \Omega$. We also assume $R = W(k)$ for k a perfect field of characteristic $p \geq 3$.
Let $A = R\{x\} = R[x, x', x'', ...]$ and $A^n = R[x, x', ..., x^{(n)}]$. We start by recalling some filtrations from [8]. Let

$$A^{\{n\}} = A^n + pA^{n+1} + p^2 A^{n+2} + ... \subset A.$$

Also let

$$I = (x, x', x'', ...) \subset A.$$

Consider the ideal $I^{[p]} \subset A$ generated by all elements of the form pf and f^p where $f \in I$; equivalently $I^{[p]} \subset A$ is the ideal generated by all elements of the form $px_\alpha^{(j)}$ and $(x_\alpha^{(j)})^p$ where $\alpha \in \Omega$, $j \geq 0$. It is trivial to check (cf. [8]) that

$$\delta(A^{\{n\}}) \subset A^{\{n+1\}}, \quad \phi(A^{\{n\}}) \subset A^{\{n\}}, \quad \delta(I^{[p]}) \subset I^{[p]}. \tag{3.1}$$

$$\delta(p^{i+1} A^{\{n\}}) \subset p^i A^{\{n\}}, \quad \delta(p^{i+1} I) \subset p^i I. \tag{3.2}$$

For any set S let us denote by $[S]$ an arbitrary element of S. In particular for our algebra C and the V-basis v_α of C^+,

$$Q_{\alpha\beta} = x_\alpha x_\beta - p\epsilon_{\alpha\beta} x_\beta + p^2[A^0 \cap I]$$

and $Q_{\alpha\beta}$ depends only on the variables x_γ with $\gamma \geq \alpha$.
Finally let $\mathcal{Q}^{(n)} \subset A^n$ be the ideal generated by

$$\{\delta^r Q_{\alpha\beta}; \alpha \leq \beta, 0 \leq r \leq n\}.$$

Note that if $F, G \in A^n$ and $F \equiv G \bmod \mathcal{Q}^{(n-1)} A^n$ then $\delta F \equiv \delta G \bmod \mathcal{Q}^{(n)} A^{n+1}$.
Here is our main computation in characteristic zero.

Theorem 3.3. *Assume C^+ has a p-triangular basis and let $Q_{\alpha\beta}$ and $\mathcal{Q}^{(n)} \subset A^n$ be as above. Then for $n \geq 1$ and $\alpha \leq \beta$ we have the congruences*

$$\delta^n Q_{\alpha\beta} \equiv F_{\alpha\beta n} \mod \mathcal{Q}^{(n-1)} A^n$$

in the ring A^n where

$$F_{\alpha\beta n} = \begin{cases} px'_\alpha x'_\beta - p\epsilon_{\alpha\beta} x'_\beta + p[A^{\{0\}} \cap I], & n = 1 \\ \\ (x'_\alpha)^p \phi(x'_\beta) + (x'_\beta)^p \phi(x'_\alpha) - (x'_\alpha x'_\beta)^p - \epsilon_{\alpha\beta}\phi(x'_\beta) + [A^{\{0\}} \cap I^{[p]}], & n = 2 \\ \\ (x'_\alpha)^{p^{n-1}} \phi(x_\beta^{(n-1)}) + (x'_\beta)^{p^{n-1}} \phi(x_\alpha^{(n-1)}) - \epsilon_{\alpha\beta}\phi(x_\beta^{(n-1)}) \\ \qquad +[A^{\{n-2\}} \cap I^{[p]}], & n \geq 3, \end{cases}$$

and $F_{\alpha\beta n}$ only depends on the variables indexed by $\gamma \geq \alpha$.

Proof. Note that $x_\alpha^s \equiv p^2[I] \bmod \mathcal{Q}^{(0)}$ for $s \geq 3$. We get the following congruences mod $\mathcal{Q}^{(0)}A^1$:

$$\begin{aligned}
\delta Q_{\alpha\beta} &= \delta(x_\alpha x_\beta) - \delta(\epsilon_{\alpha\beta} p x_\beta) + \delta(p^2[A^{\{0\}} \cap I]) + p[A^{\{0\}} \cap I] \\
&= x_\alpha^p x'_\beta + x_\beta^p x'_\alpha + p x'_\alpha x'_\beta - \epsilon_{\alpha\beta} x_\beta^p \delta p - \epsilon_{\alpha\beta} p x'_\beta + p[A^{\{0\}} \cap I] \\
&\equiv p^2[A^{\{1\}} \cap I] + p x'_\alpha x'_\beta - p\epsilon_{\alpha\beta} x'_\beta + p[A^{\{0\}} \cap I] \\
&= p x'_\alpha x'_\beta - p\epsilon_{\alpha\beta} x'_\beta + p[A^{\{0\}} \cap I].
\end{aligned}$$

Using the fact that $\delta p \equiv 1 \bmod p$ we get the following congruences mod $\mathcal{Q}^{(1)}A^2$:

$$\begin{aligned}
\delta^2 Q_{\alpha\beta} &\equiv \delta(p x'_\alpha x'_\beta) - \delta(p\epsilon_{\alpha\beta} x'_\beta) + \delta(p[A^{\{0\}} \cap I]) \\
&\quad + C_{3p}(p x'_\alpha x'_\beta, -p\epsilon_{\alpha\beta} x'_\beta, [A^{\{0\}} \cap I^{[p]}]) \\
&\equiv (x'_\alpha x'_\beta)^p (\delta p) + p\delta(x'_\alpha x'_\beta) - \delta(p\epsilon_{\alpha\beta})(x'_\beta)^p - p\epsilon_{\alpha\beta} x''_\beta + [A^{\{0\}} \cap I^{[p]}] \\
&\equiv (x'_\alpha x'_\beta)^p + p((x'_\alpha)^p x''_\beta + (x'_\beta)^p x''_\alpha + p[A^2 \cap I]) \\
&\quad - \epsilon_{\alpha\beta}\phi(x'_\beta) + [A^{\{0\}} \cap I^{[p]}] \\
&= (x'_\alpha)^p \phi(x'_\beta) + (x'_\beta)^p \phi(x'_\alpha) - (x'_\alpha x'_\beta)^p - \epsilon_{\alpha\beta}\phi(x'_\beta) + [A^{\{0\}} \cap I^{[p]}].
\end{aligned}$$

Using the fact that the 5 terms above are in $A^{\{1\}} \cap I^{[p]}$, the fact that $\phi\delta = \delta\phi$, and the fact that $\delta((x'_i)^p), \delta((x'_i)^p(x'_j)^p) \in pA^2 \cap I^{[p]} \subset A^{\{1\}} \cap I^{[p]}$ we get the following congruence mod $\mathcal{Q}^{(2)}A^3$:

$$\begin{aligned}
\delta^3 Q_{\alpha\beta} &\equiv \delta((x'_\alpha)^p \phi(x'_\beta)) + \delta((x'_\beta)^p \phi(x'_\alpha)) - \delta((x'_\alpha x'_\beta)^p) \\
&\quad - \delta(\epsilon_{\alpha\beta}\phi(x'_\beta)) + \delta([A^{\{0\}} \cap I^{[p]}]) + C_{5p}([A^{\{1\}} \cap I^{[p]}], ..., [A^{\{1\}} \cap I^{[p]}]) \\
&\equiv \delta((x'_\alpha)^p \phi(x'_\beta)) + \delta((x'_\beta)^p \phi(x'_\alpha)) - \delta(\epsilon_{\alpha\beta}\phi(x'_\beta)) + [A^{\{1\}} \cap I^{[p]}] \\
&\equiv (x'_\alpha)^{p^2} \delta(\phi(x'_\beta)) + \phi^2(x'_\beta)\delta((x'_\alpha)^p) + (x'_\beta)^{p^2} \delta(\phi(x'_\alpha)) \\
&\quad + \phi^2(x'_\alpha)\delta((x'_\beta)^p) - \epsilon_{\alpha\beta}\delta(\phi(x'_\beta)) + [A^{\{1\}} \cap I^{[p]}] \\
&\equiv (x'_\alpha)^{p^2} \phi(x''_\beta) + (x'_\beta)^{p^2} \phi(x''_\alpha) - \epsilon_{\alpha\beta}\phi(x''_\beta) + [A^{\{1\}} \cap I^{[p]}].
\end{aligned}$$

Finally using the same kind of computation as for $\delta^3 Q_{\alpha\beta}$ one proves by induction on n that for $n \geq 3$ we have the following congruence mod $\mathcal{Q}^{(n-1)}A^n$:

$$\delta^n Q_{\alpha\beta} \equiv (x'_\alpha)^{p^{n-1}} \phi(x_\beta^{(n-1)}) + (x'_\beta)^{p^{n-1}} \phi(x_\alpha^{(n-1)}) - \epsilon_{\alpha\beta}\phi(x_\beta^{(n-1)}) + [A^{\{n-2\}} \cap I^{[p]}].$$

The fact that $F_{\alpha\beta n}$ only depends on the variables indexed by $\gamma \geq \alpha$ follows simply from the fact that for any pair $\alpha \leq \beta$ we can make the computations above in the rings with variables indexed by indices $\gamma \geq \alpha$. $\square$

Let $\overline{B} = B/pB$ for any ring B; also for $b \in B$ let $\overline{b} \in \overline{B}$ be the class of b. Set $k = R/pR$. Then the ideal $\overline{I^{[p]}}$ in $\overline{A} = k[x, x', x'', ...]$ is generated by the set $\{(x_\alpha^{(r)})^p; r \geq 0, \alpha \in \Omega\}$ and it is trivial to see that we have an equality of ideals

$$\overline{A^{\{n-2\}} \cap I^{[p]}} = \overline{A^{n-2}} \cap \overline{I^{[p]}} = ((x_\alpha^{(r)})^p; 0 \leq r \leq n-2, \alpha \in \Omega)$$

in the ring

$$\overline{A^{n-2}} = k[x, x', ..., x^{(n-2)}].$$

Set $F_{\alpha\beta 0} = Q_{\alpha\beta}$. We get the following:

COROLLARY 3.4.

$$\overline{F_{\alpha\beta n}} = \begin{cases} x_\alpha x_\beta, & n = 0 \\ 0, & n = 1 \\ (x'_\alpha x'_\beta)^p - \epsilon_{\alpha\beta}(x'_\beta)^p + \overline{G}_{\alpha\beta 2}, & n = 2 \\ (x'_\alpha)^{p^{n-1}}(x_\beta^{(n-1)})^p + (x'_\beta)^{p^{n-1}}(x_\alpha^{(n-1)})^p - \epsilon_{\alpha\beta}(x_\beta^{(n-1)})^p + \overline{G}_{\alpha\beta n}, & n \geq 3, \end{cases}$$

for $\alpha \leq \beta$, where

$$\overline{G}_{\alpha\beta n} \in ((x_\gamma^{(r)})^p; \gamma \geq \alpha, 0 \leq r \leq n-2) \subset k[x_\gamma, ..., x_\gamma^{(n-2)}; \gamma \geq \alpha].$$

COROLLARY 3.5. *The ideal $\mathcal{Q}^{(n)} \subset A^n$ is generated by the set*

$$\{F_{\alpha\beta r};\ \alpha \leq \beta,\ 0 \leq r \leq n\}.$$

In particular:

$$J^n(C) = A^n/(F_{\alpha\beta r};\ \alpha \leq \beta,\ 0 \leq r \leq n),$$
$$\overline{J^n(C)} = \overline{A^n}/(\overline{F_{\alpha\beta r}};\ \alpha \leq \beta,\ 0 \leq r \leq n).$$

Since

$$\overline{\mathcal{Q}^{(n)}} \subset (x_\alpha x_\beta, (x_\alpha^{(r)})^p; \alpha, \beta \in \Omega, 1 \leq r \leq n-1) \subset \overline{A^n}$$

we get

COROLLARY 3.6. *There is a natural surjection*

$$\overline{J^n(C)} \to \frac{\overline{A^n}}{(x_\alpha x_\beta, (x_\alpha^{(r)})^p; \alpha, \beta \in \Omega, 1 \leq r \leq n-1)}. \tag{3.3}$$

In some important cases the above surjection is close to an isomorphism as we shall see next.

DEFINITION 3.7. Assume C^+ has a p-triangular basis v_α, $\alpha \in \Omega$. Let

$$\{\gamma \in \Omega; \epsilon_{\gamma\gamma} = 1\} = \{\gamma_1, ..., \gamma_N\}, \quad \gamma_1 < ... < \gamma_N.$$

We say that v_α is a *non-degenerate* p-triangular basis if min $\Omega = \gamma_1$ and $\epsilon_{\gamma_i\gamma} = 1$ for all $i = 1, ..., N$ and all $\gamma_i \leq \gamma < \gamma_{i+1}$. (Here and later we discard the condition $\gamma < \gamma_{i+1}$ if $i = N$.)

Remark 3.8. Let m be a non-negative integer. Let $\Omega = \Omega_m = \{1, ..., m\}$ be equipped with the usual total order and consider the R-algebra $C = W_m(R)$, the ghost homomorphism $w_0 : W_m(R) \to R$, and its kernel $W_m(R)^+$. Then by Lemma 2.1 $v_1, ..., v_m$ is a non-degenerate p-triangular basis of $W_m(R)^+$; indeed $\{i \in \Omega_m; \epsilon_{ii} = 1\} = \{1\}$ and $\epsilon_{1j} = 1$ for $j = 1, ..., m$.

Remark 3.9. Let m, m' be non-negative integers. Consider the set

$$\Omega := \Omega_{m,m'} = \{(i, i') \in \mathbb{Z} \times \mathbb{Z}; 0 \leq i \leq m,\ 0 \leq i' \leq m'\} \backslash \{(0, 0)\},$$

ordered by the lexicographic order: $(i, i) \leq (j, j')$ if either $i < j$ or $i = j$, $i' \leq j'$. Consider the R-algebra $W_m(W_{m'}(R))$ $(p \geq 5)$ and the composition of ghost maps $w_0 \circ w_0 : W_m(W_{m'}(R)) \to R$ with kernel $W_m(W_{m'}(R))^+$. Consider the R-basis $v_{(i,i')} = v_{i,i'}$ of $W_m(W_{m'}(R))^+$ where $(i, i') \in \Omega_{m,m'}$; cf Lemma 2.9. Then $v_{i,i'}$ is a non-degenerate p-triangular basis by Lemma 2.8; note that for $m, m' \geq 1$

$$\{(i, i') \in \Omega_{m,m'};\ \epsilon_{(i,i')(i,i')} = 1\} = \{(0, 1), (1, 0)\}.$$

Going back to our general C, viewed with augmentation $C \to C/C^+ = R$, the following is a computation of the identity component of $\overline{J^n(C)}$ in the presence of non-degenerate p-triangular bases.
With notation as in Definition 3.7 we have

Theorem 3.10. *Assume C^+ has a non-degenerate p-triangular basis v_α and set*

$$\pi = \prod_{i=1}^{N} (\delta v_{\gamma_i} - 1) \in J^1(C).$$

Then the image of π^p in $\overline{J^2(C)}$ is idempotent and for all $n \geq 2$ we have a natural isomorphism

$$\overline{J^n(C)}_\pi \simeq \frac{\overline{A^n}}{(x_\alpha x_\beta, (x_\alpha^{(r)})^p; \alpha, \beta \in \Omega, 1 \leq r \leq n-1)} \tag{3.4}$$

sending the class of $\delta^r v_\alpha$ into the class of $x_\alpha^{(r)}$ for all $r \geq 0$ and all α.

By the theorem it follows that $\overline{J^n(C)}_\pi$, respectively $\overline{J^n(C)}_{1-\pi}$, are isomorphic to the identity component, respectively to the complement of the identity component, of $\overline{J^n(C)}$.

Proof of Theorem 3.10. Since the map (3.3) sends π into the class of the polynomial $\Phi = \prod_{i=1}^N (x'_{\gamma_i} - 1)$ (which is an invertible element) we get a surjective map from the left hand side of (3.4) to the right hand side of (3.4). In order to prove that the latter map is an isomorphism it is enough to show that the inclusion of ideals

$$\left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi \subset (x_\alpha x_\beta, (x_\alpha^{(r)})^p; \alpha, \beta \in \Omega, 1 \leq r \leq n-1)_\Phi$$

in the ring $(\overline{A^n})_\Phi$ is an equality. Clearly $x_\alpha x_\beta \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi$. Next we show that for all $i = 1, ..., N$, all $\gamma_i \leq \gamma < \gamma_{i+1}$, and all $1 \leq r \leq n-1$ we have

$(x_\gamma^{(r)})^p \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi$. We proceed by induction on $N-i \geq 0$. The proof of the case $N-i=0$ is similar to the proof of the induction step so we skip it. For the induction step assume the assertion is true for $i+1, i+2, ..., N$, for some index $1 \leq i < N$, and let us prove it for i. We proceed by induction on $r \geq 1$. To check the base case $r=1$ note that for all $\gamma \in \Omega_i$ we have

$$\overline{F_{\gamma_i\gamma 2}} = (x'_{\gamma_i}-1)^p(x'_\gamma)^p + \overline{G}_{\gamma_i\gamma 2} \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi.$$

Since $\overline{G}_{\gamma_i\gamma 2} \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi$ we get $(x'_\gamma)^p \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi$. Now let $3 \leq s \leq n$ and assume that for all $1 \leq r \leq s-2$ and all $\gamma \in \Omega_i$ we have $(x_\gamma^{(r)})^p \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi$; we want to show that $(x_\gamma^{(s-1)})^p \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi$. Note that

$$\overline{F_{\gamma_i\gamma s}} = (x'_{\gamma_i})^{p^{s-1}}(x_\gamma^{(s-1)})^p + (x'_\gamma)^{p^{s-1}}(x_{\gamma_i}^{(s-1)})^p - (x_\gamma^{(s-1)})^p + \overline{G}_{\gamma_i\gamma s} \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi.$$

Recall that $\overline{G}_{\gamma_i\gamma s}$ is in the ideal generated by $(x_\mu^{(r)})^p$ with $\mu \geq \gamma_i$ and $0 \leq r \leq s-2$. By the induction hypotheses (and the fact that $x_\alpha^p \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi$) we have that

$$(x'_{\gamma_i})^{p^{s-1}}, (x'_\gamma)^{p^{s-1}}, \overline{G}_{\gamma_i\gamma s} \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi.$$

It follows that $(x_\gamma^{(s-1)})^p \in \left(\overline{\mathcal{Q}^{(n)}}\right)_\Phi$ which ends the induction on r and hence the induction on i as well. To conclude the proof of the Theorem note that

$$\overline{F}_{\gamma_i\gamma_i 2} - \overline{G}_{\gamma_i\gamma_i 2} = (x'_{\gamma_i})^{2p} - (x'_{\gamma_i})^p \in \overline{\mathcal{Q}^{(2)}}$$

so the image of $(\delta v_{\gamma_i})^p$ in $\overline{J^2(C)}$ is idempotent hence so is the image of π^p. $\square$

Finally we need the following

Lemma 3.11. *For $U_1, U_2 \in I \cap A^0$ and $n \geq 0$ we have*

$$\delta^n(U_1 + pU_2) = \delta^n U_1 + [I^{[p]} \cap A^{\{n\}}].$$

Proof. We proceed by induction on n. The case $n=0$ is tautological. For the induction step,

$$\begin{aligned}
\delta^{n+1}(U_1+pU_2) &= \delta^{n+1}U_1 + \delta([I^{[p]} \cap A^{\{n\}}]) \\
&\quad + C_p(\delta^n U_1, [I^{[p]} \cap A^{\{n\}}]) \\
&= \delta^{n+1}U_1 + [I^{[p]} \cap A^{\{n+1\}}]
\end{aligned}$$

which ends the proof. $\square$

Corollary 3.12. *Assume the notation in Theorem 3.10 and let $u_1, u_2 \in C^+$. Then for any $i = 0, ..., n-1$ we have*

$$\overline{\delta^i(u_1 + pu_2)} = \overline{\delta^i(u_1)}$$

in the ring $\overline{J^n(C)}_\pi$. *In particular for all* $u_1, ..., u_s, u \in C^+$ *we have*

$$\overline{\delta(\sum_{t=1}^{s} u_t + pu)} = \sum_{t=1}^{s} \overline{\delta(u_t)}.$$

Proof. Let u_1, u_2 be the classes of polynomials $U_1, U_2 \in \overline{I \cap A^0}$. Then the first assertion follows from Lemma 3.11 because, for $i \leq n-1$, $\overline{I^{[p]} \cap A^{\{i\}}}$ is contained in the denominator of the fraction in Equation 3.4. The second assertion follows from the fact that the difference between $\delta(\sum_{t=1}^{s} u_t)$ and $\sum_{t=1}^{s} \delta(u_i)$ is in the square of the ideal C^+ and hence its reduction mod p s zero. □

4. Applications to p-jets of Witt rings

In this section we continue to write $R = W(k)$ for k a perfect field of characteristic $p \geq 5$. In view of Remark 3.8 the results in the previous section apply to the algebra $C = W_m(R)$ equipped with the homomorphism $w_0 : W_m(R) \to R$ and with the non-degenerate p-triangular basis $v_1, ..., v_m$ indexed by $\Omega_m = \{1, ..., m\}$. For $m = 1$ we have:

Corollary 4.1.

$$\overline{J^n(W_1(R))} = \begin{cases} \frac{k[x,x']}{(x^2)}, & n = 1 \\ \frac{k[x,x',x'']}{(x^2,((x')^2-x')^p)}, & n = 2 \\ \frac{k[x,x',...,x^{(n)}]}{(x^2,((x')^2-x')^p,(2x'-1)^{p^{r-1}}(x^{(r-1)})^p+\overline{G}_{11r};3\leq r\leq n)}, & n \geq 3, \end{cases}$$

where $\overline{G}_{11r} \in ((x^{(s)})^p; 0 \leq s \leq r-2) \subset k[x, ..., x^{(r-2)}]$. *In particular, since* $2x' - 1$ *is invertible in the ring* $k[x']/(((x')^2 - x')^p)$, *the ring* $\overline{J^n(W_1(R))}$ *is a polynomial ring in* m *variables* $x_1^{(n)}, ..., x_m^{(n)}$ *over an Artin ring. This Artin ring is a free module of rank* p^{n-1} *over the ring* $\overline{W_1(R)} = k[x]/(x^2)$. *Moreover the ring* $\overline{J^\infty(W_1(R))}$ *is a flat integral extension of* $\overline{W_1(R)}$.

Set $\pi = 1 - \delta v_1$. For $m \geq 1$ and $n \geq 2$ we have a splitting

$$\overline{J^n(W_m(R))} = \left(\overline{J^n(W_m(R))}\right)_\pi \times \left(\overline{J^n(W_m(R))}\right)_{1-\pi}.$$

For the identity component we have the following direct consequence of Theorem 3.10:

Corollary 4.2. *For* $n \geq 2$

$$\left(\overline{J^n(W_m(R))}\right)_\pi \simeq \frac{k[x_i^{(r)}; i \in \Omega_m, 0 \leq r \leq n]}{(x_i x_j, (x_i^{(r)})^p; i, j \in \Omega_m, 1 \leq r \leq n-1)}.$$

In particular the above ring is a polynomial ring in m *variables* $x_1^{(n)}, ..., x_m^{(n)}$ *over a local Artin ring. This local Artin ring is a free module of rank* $p^{m(n-1)}$

over $\overline{W_m(R)}$. Moreover the ring

$$\left(\overline{J^{\infty}(W_m(R))}\right)_{\pi} = \frac{k[x_i^{(r)}; i \in \Omega_m, r \geq 0]}{(x_i x_j, (x_i^{(r)})^p; i, j \in \Omega_m, r \geq 1)}$$

is local and is a flat integral extension of $\overline{W_m(R)}$.

On the other hand the canonical lifts $J^n(W_m(R)) \to R$ of $w_1, ..., w_m$ send $\delta v_1 \mapsto \delta p \in R^{\times}$ so they factor through $J^n(W_m(R))_{1-\pi} \to R$. In particular the complement of the identity component, $\left(\overline{J^n(W_m(R))}\right)_{1-\pi}$, is non-zero. Moreover for $m \geq 2$ this ring is, in some sense, more "degenerate" than the identity component. Indeed this ring is trivially seen to be the quotient of $(\overline{A^n})_{x_1'}$ by the ideal generated by the following elements:
1) $x_i x_j,\ \ 1 \leq i \leq j \leq m$,
2) $(x_1')^p - 1$,
3) $(x_i')^p (x_j')^p,\ 2 \leq i \leq j \leq m$,
4) $(x_1^{(r-1)})^p + \overline{G}_{11r},\ 3 \leq r \leq n$,
5) $\overline{G}_{1jr},\ 2 \leq j \leq m,\ 3 \leq r \leq n$,
6) $\overline{G}_{ijr},\ 2 \leq i \leq j \leq m,\ 3 \leq r \leq n$.
Since the variables $x_2^{(n-1)}, ..., x_m^{(n-1)}, x_1^{(n)}, ..., x_m^{(n)}$ do not appear in any of the above generators, and since, as we saw, the ring $\left(\overline{J^n(W_m(R))}\right)_{1-\pi}$ is non-zero we get:

COROLLARY 4.3. *For $n \geq 3$ and $m \geq 2$ the ring $\left(\overline{J^n(W_m(R))}\right)_{1-\pi}$ is isomorphic to a polynomial ring in $2m-1$ variables $x_2^{(n-1)}, ..., x_m^{(n-1)}, x_1^{(n)}, ..., x_m^{(n)}$ over some non-zero ring.*

Assume from now on $p \geq 5$. In a similar way, in view of Remark 3.9, the results in the previous section apply to the R-algebra $C = W_m(W_{m'}(R))$, $1 \leq m, m' < \infty$, equipped with the homomorphism $w_0 \circ w_0 : W_m(W_{m'}(R)) \to R$ and with the non-degenerate p-triangular basis $v_{i,i'}$ indexed by $\Omega = \Omega_{m,m'}$ in loc. cit. In particular if $\Pi = (1 - \delta v_{0,1})(1 - \delta v_{1,0})$ we have a splitting

$$\overline{J^n(W_m(W_{m'}(R)))} = \left(\overline{J^n(W_m(W_{m'}(R)))}\right)_{\Pi} \times \left(\overline{J^n(W_m(W_{m'}(R)))}\right)_{1-\Pi}.$$

For the identity component we have the following direct consequence of Theorem 3.10:

COROLLARY 4.4. *For $n \geq 2$ we have*

$$\left(\overline{J^n(W_m(W_{m'}(R)))}\right)_{\Pi} \simeq \frac{k[x_{ii'}^{(r)}; (i, i') \in \Omega, 0 \leq r \leq n]}{(x_{ii'} x_{jj'}, (x_{ii'}^{(r)})^p; (i, i'), (j, j') \in \Omega, 1 \leq r \leq n-1)}.$$

Next consider the comultipication R-algebra map

$$\Delta : W_{m+m'}(R) \to W_m(W_{m'}(R))$$

and the induced R-algebra maps

$$J^n(\Delta) : J^n(W_{m+m'}(R)) \to J^n(W_m(W_{m'}(R))). \tag{4.1}$$

Lemma 4.5. *For $n \geq 2$ the above R-algebra map induces an R-algebra map*

$$\overline{J^n(\Delta)} : \overline{J^n(W_{m+m'}(R))}_\pi \to \overline{J^n(W_m(W_{m'}(R)))}_\Pi.$$

Proof. It is enough to show that $J^n(\Delta)$ in (4.1) sends $\pi = 1 - \delta v_1$ into an invertible element of $\overline{J^n(W_m(W_{m'}(R)))}_\Pi$. But by Lemmas 2.10 and 3.12 we have the following congruences mod p:

$$J^n(\Delta)(1 - \delta v_1) = 1 - \delta(\Delta v_1) \equiv 1 - \delta v_{1,0} - \delta v_{0,1} \equiv \Pi - (\delta v_{1,0})(\delta v_{0,1})$$

and we conclude by the fact that the image of $(\delta v_{1,0})(\delta v_{0,1})$ in $\overline{J^1(W_m(W_{m'}(R))}$ is nilpotent; cf. Corollary 4.4. □

By the identifications in Lemmas 4.2 and 4.4 we get that the R-algebra map in Lemma 4.5 induces an R-algebra map

$$\overline{J^\infty(\Delta)} : \frac{k[x_i^{(r)}; i \in \Omega_{m+m'}, r \geq 0]}{(x_i x_j, (x_i^{(r)})^p; r \geq 1)} \to \frac{k[x_{ii'}^{(r)}; (i, i') \in \Omega_{m,m'}, r \geq 0]}{(x_{ii'} x_{jj'}, (x_{ii'}^{(r)})^p; r \geq 1)}. \tag{4.2}$$

Corollary 4.6. *For $1 \leq i'' \leq m + m'$ we have that $\overline{J^\infty(\Delta)}$ sends the class of $x_{i''}^{(r)}$ into the class of*

$$\sum_{i+i'=i''} x_{i,i'}, \quad \textit{if} \quad r = 0$$

and into the class of

$$\delta^{r-1}\left(\sum_{i+i'=i''} x'_{i,i'}\right), \quad \textit{if} \quad r \geq 1.$$

Proof. By Corollary 3.12 and Lemma 2.10 $\overline{J^\infty(\Delta)}$ sends the class of $x_{i''}^{(r)}$ into the class of

$$\delta^r\left(\sum_{i+i'=i''} x_{i,i'}\right)$$

if $r \geq 0$. It is then enough to prove that

$$\delta^r\left(\sum_{i+i'=i''} x_{i,i'}\right) = \delta^{r-1}\left(\sum_{i+i'=i''} x'_{i,i'}\right) + (I^2 \cap A^0)A + I^{[p]}$$

for $r \geq 1$ in $A = R[x, x', x'', ...]$, where I^2 denotes as usual the square of the ideal I. The later follows by induction using the fact that

$$\delta((I^2 \cap A^0)A) \subset (I^2 \cap A^0)A + I^{[p]}.$$

□

Remark 4.7. It would be interesting to have an explicit understanding of the homomorphisms $s : J^n(W_m(R)) \to W_{m-n}(R)$ in (2.16), or at least of their reduction mod p. This involves understanding the iterates of formula 4.2. Note however that by formula 4.2 it follows that

$$s(\pi) = 1 - (1 - p^{p-2}\rho(v_1)) \in pW_{m-1}(R).$$

In other words for $n \geq 2$

$$\overline{s} : \overline{J^n(W_m(R))} \to \overline{W_{m-n}(R)}$$

factors through the *complement of the identity component* !

$$\overline{J^n(W_m(R))}_{1-\pi} \to \overline{W_{m-n}(R)}$$

rather than through the identity component $\overline{J^n(W_m(R))}_{\pi}$; this makes the problem more subtle.

REFERENCES

1. Borger, J., *The basic geometry of Witt vectors, I: The affine case*, Algebra and Number Theory 5 (2011), no. 2, pp 231-285.
2. Borger, J., *The basic geometry of Witt vectors, II: Spaces*, Mathematische Annalen 351 (2011), no. 4, pp 877-933.
3. Borger, J.: *Λ-rings and the field with one element*, arXiv:0906.3146v1
4. A.Buium, *Intersections in jet spaces and a conjecture of S.Lang*, Annals of Math. 136 (1992) 557-567.
5. A. Buium, *Differential algebra and diophantine geometry*, Hermann, 1994.
6. Buium, A: *Differential characters of Abelian varieties over p-adic fields*, Invent. Math. 122 (1995), 2, pp. 309-340.
7. Buium, A.: *Arithmetic Differential Equations*, Math. Surveys and Monographs 118, AMS, 2005.
8. Buium, A., *p-jets of finite algebras, I: p-divisible groups*, Documenta Math. 18, (2013), 943-969.
9. L. Hesselholt, *The big de Rham Witt complex*, arXiv:1006.3125.
10. Joyal, A., *δ-anneaux et vecteurs de Witt*, C. R. Acad. Sci. Canada VII, 3 (1985), 177-182.
11. Malgrange, B.: *Le groupoïde de Galois d'un feuilletage*, Monographie 28 Vol 2, L'enseignement Mathématique (2001).
12. Manin, Yu. I.: *Cyclotomy and analytic geometry over* $\mathbb{F}_1$, arXiv:0809.1564.

Alexandru Buium
Department of Mathematics
and Statistics
University of New Mexico
Albuquerque
NM 87131
USA
buium@math.unm.edu