# THE WITT VECTOR AFFINE RING SCHEME

PAUL PEARSON

Abstract. We describe the ring of Witt vectors as an affine ring scheme, and then describe the objects that corepresent this affine ring scheme together the structure homomorphisms that make it corepresent a ring-valued functor. We call the corepresenting object the co-Witt ring. Further, we describe how to make calculations in the ring of Witt vectors and give some sample calculations.

Contents



*Date*: September 25, 2005, 1:04am.

## 1. Witt polynomials and the Dwork lemma

Fix a prime $p$, and let $\mathbb{Z}_p$ denote the $p$-adic integers. Let $x_0, x_1, \ldots$ be a sequence of indeterminates and let $\mathbb{Z}_p[x_0, x_1, \ldots]$ be the free graded commutative $\mathbb{Z}_p$-algebra on the indeterminates $x_i$. Let

$$w_n(x_0, x_1, \ldots, x_n) = {x_0}^{p^n} + p{x_1}^{p^{n-1}} + \cdots + p^n x_n$$

be the $n$th Witt polynomial. We will sometimes abbreviate polynomials such as these by $w_n$ or $w_n(x)$, where $x$ stands for $(x_0, x_1, \ldots, x_n)$ or $(x_0, x_1, \ldots)$ as appropriate.

An algebra $A$ over $\mathbb{Z}_p$ together with an algebra endomorphism $f : A \to A$ so that $f(x) \equiv x^p \mod p$ is said to have a lift $f$ of the Frobenius $x \mapsto x^p$. For $A = \mathbb{Z}_p[x_0, x_1, \ldots]$, we define the "simple" lift of the Frobenius $\phi : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p[x_0, x_1, \ldots]$ by $\phi(x_n) = {x_n}^p$ for all $n \geq 0$, and we use $\phi$ to denote this lift from now on. Later, we will define the "complicated" lift of the Frobenius $\varphi : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p[x_0, x_1, \ldots]$, and use $\varphi$ to denote it. An unspecified lift of the Frobenius will be denoted $f : A \to A$ throughout the paper.

We now introduce the Dwork lemma, which is our primary tool for constructing morphisms of $\mathbb{Z}_p$-algebras and also Hopf algebras. In particular, we use the Dwork lemma to construct the addition, subtraction, and multiplication in the ring of Witt vectors (or, equivalently, the coaddition, cosubtraction, and comultiplication structure homomorphisms of the co-Witt ring).

1**. Lemma** (Dwork)**.** *Let $A$ be a commutative torsion-free $\mathbb{Z}_p$-algebra. Suppose $A$ has a ring endomorphism $f : A \to A$ so that $f(x) \equiv x^p \mod p$. Then, given a sequence of elements $g_n \in A$, $n \geq 0$, so that*

$$g_n \equiv f(g_{n-1}) \mod p^n,$$

*there are unique elements $q_n \in A$, $n \geq 0$, so that*

$$w_n(q) = w_n(q_0, q_1, \ldots, q_n) = g_n.$$

*Proof.* Make the crucial observation that for any $x$,

$$w_n(x_0, x_1, \ldots, x_n) = w_{n-1}({x_0}^p, {x_1}^p, \ldots, {x_{n-1}}^p) + p^n x_n.$$

Then $q_n$ is determined by

$$p^n q_n = g_n - w_{n-1}({q_0}^p, {q_1}^p, \ldots, {q_{n-1}}^p)$$

whenever the right hand side of this equation is divisible by $p^n$. But, since $f$ is a ring homomorphism

$$\begin{aligned} w_{n-1}({q_0}^p, {q_1}^p, \ldots, {q_{n-1}}^p) &\equiv f(w_n(q_0, q_1, \ldots, q_{n-1})) \mod p^n \\ &= f(g_{n-1}) \\ &\equiv g_n \mod p^n. \end{aligned}$$

□

Using the Dwork lemma, we define a unique $\mathbb{Z}_p$-algebra homomorphism $q : \mathbb{Z}_p[x_0, x_1, \ldots] \to A$ by $x_i \mapsto q_i = q(x_i)$ for $i \geq 0$. Another equivalent way of specifying this homomorphism via Witt polynomials is $w_i(x) \mapsto w_i(q) = g_i$ for $i \geq 0$.

For example, suppose $A = \mathbb{Z}_p[x_0, x_1, \ldots]$ has a lift of the Frobenius and we have a sequence of elements $g_i$ satisfying the hypotheses of the Dwork lemma. Then we may use the Dwork lemma to define a unique $\mathbb{Z}_p$-algebra homomorphism $q : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p[x_0, x_1, \ldots]$ by setting $q(x_i) = q_i$ for all $i \geq 0$.

## 2. The Witt vectors

We describe the Witt vectors as a covariant functor $W(-)$ from the category of commutative $\mathbb{Z}_p$-algebras to the category of commutative rings with unit. This functor is corepresentable, and we describe its corepresenting objects and structure morphisms in the next section.

We construct a covariant ring-valued functor

$$W : (\text{comm.}\mathbb{Z}_p\text{−algebras}) \to (\text{comm.rings})$$
$$R \mapsto W(R) = \mathrm{Hom}_{\mathbb{Z}_p-alg}(\mathbb{Z}_p[x_0, x_1, x_2, \ldots], R)$$

by giving the set $W(R)$ an addition and multiplication that make it into a ring. This ring $W(R)$ is the ring of Witt vectors over $R$.

Let $R$ be a $\mathbb{Z}_p$-algebra. The zero element in $W(R)$ is the algebra homomorphism $e_0 : \mathbb{Z}_p[x_0, x_1, \ldots] \to R$ given by $e_0(x_n) = 0$ for all $n \geq 0$. The unit element in $W(R)$ is the algebra homomorphism $e_1 : \mathbb{Z}_p[x_0, x_1, \ldots] \to R$ given by $e_1(x_0) = 1$ and $e_1(x_n) = 0$ for $n \geq 1$. We will identify an algebra homomorphism $f : \mathbb{Z}_p[x_0, x_1, \ldots] \to R$ in $W(R)$ with the sequence $(f(x_0), f(x_1), \ldots) := (f_0, f_1, \ldots) \in \prod R$ it determines. The zero element in $W(R)$ determines the sequence $(0, 0, 0, \ldots)$ and the unit element determines $(1, 0, 0, 0, \ldots)$.

We use the Dwork lemma to construct unique polynomials $\alpha_n$ that define both the addition in the ring $W(R)$ and the coaddition in the the co-Witt ring.

2**. Corollary.** *There exist unique polynomials*

$$\alpha_n = \alpha_n(x, y) = \alpha_n(x_0, \ldots, x_n, y_0, \ldots, y_n) \in \mathbb{Z}_p[x_0, x_1, \ldots, y_0, y_1, \ldots]$$

*such that*

$$w_n(\alpha_0, \alpha_1, \ldots, \alpha_n) = w_n(x_0, \ldots, x_n) + w_n(y_0, \ldots, y_n).$$

*Proof.* Take $A = \mathbb{Z}_p[x_0, x_1, \ldots, y_0, y_1, \ldots]$, $f = \phi$, $g_n = w_n(x_0, \ldots, x_n) + w_n(y_0, \ldots, y_n)$, and $q_n = \alpha_n$ in the Dwork lemma. □

3**. Definition.** *The sum of two elements $f, g \in W(R)$ is given by*

$$\begin{aligned}(f_0, f_1, \ldots) \underset{W}{+} (g_0, g_1, \ldots) &= (\alpha_0, \alpha_1, \ldots)\\ &= (\alpha_0(f, g), \alpha_1(f, g), \ldots)\\ &= (\alpha_0(f_0, g_0), \alpha_1(f_0, f_1, g_0, g_1), \ldots)\end{aligned}$$

4. *Example.* The polynomials $\alpha_0$ and $\alpha_1$ are easily calculated by hand. For the case $n = 0$,

$$\begin{aligned} w_0(\alpha_0) &= w_0(x_0) + w_0(y_0) \\ \alpha_0 &= x_0 + y_0. \end{aligned}$$

For $n = 1$,

$$\begin{aligned} w_1(\alpha_0, \alpha_1) &= w_1(x_0, x_1) + w_1(y_0, y_1) \\ {\alpha_0}^p + p\alpha_1 &= {x_0}^p + px_1 + {y_0}^p + py_1 \\ (x_0 + y_0)^p + p\alpha_1 &= {x_0}^p + px_1 + {y_0}^p + py_1 \end{aligned}$$

and thus solving for $\alpha_1$ we have

$$\alpha_1 = \alpha_1(x, y) = \alpha_1(x_0, x_1, y_0, y_1) = x_1 + y_1 - \frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i}{x_0}^{p-i}{y_0}^i.$$

The value of $(f_0, f_1, \ldots) \underset{W}{+} (g_0, g_1, \ldots) = (\alpha_0(f_0, g_0), \alpha_1(f_0, f_1, g_0, g_1), \ldots)$ is then found by substituting the values $f_i$ and $g_i$ for $x_i$ and $y_i$, respectively, into the $\alpha_n$ for all $i, n \geq 0$.

5. *Remark.* The polynomial $\frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i}{x_0}^{p-i}{y_0}^i = \frac{(x+y)^p - x^p - y^p}{p}$ is a homogeneous polynomial of degree $p$.

We use the Dwork lemma again to construct unique polynomials $\iota_n$ that define both the subtraction in the ring $W(R)$ and the cosubtraction in the the co-Witt ring.

6**. Corollary.** *There exist unique polynomials*

$$\iota_n = \iota_n(x, y) = \iota_n(x_0, \ldots, x_n, y_0, \ldots, y_n) \in \mathbb{Z}_p[x_0, x_1, \ldots, y_0, y_1, \ldots]$$

*such that*

$$w_n(\iota_0, \iota_1, \ldots, \iota_n) = w_n(x_0, \ldots, x_n) - w_n(y_0, \ldots, y_n).$$

*Proof.* Take $A = \mathbb{Z}_p[x_0, x_1, \ldots, y_0, y_1, \ldots]$, $f = \phi$, $g_n = w_n(x_0, \ldots, x_n) - w_n(y_0, \ldots, y_n)$, and $q_n = \iota_n$ in the Dwork lemma. $\square$

7**. Definition.** *The difference of two elements $f, g \in W(R)$ is given by*

$$\begin{aligned} (f_0, f_1, \ldots) \underset{W}{-} (g_0, g_1, \ldots) &= (\iota_0, \iota_1, \ldots) \\ &= (\iota_0(f, g), \iota_1(f, g), \ldots) \\ &= (\iota_0(f_0, g_0), \iota_1(f_0, f_1, g_0, g_1), \ldots) \end{aligned}$$

8. *Example.* The polynomials $\iota_0$ and $\iota_1$ are easily calculated by hand. For the case $n = 0$,

$$\begin{aligned} w_0(\iota_0) &= w_0(x_0) - w_0(y_0) \\ \iota_0 &= x_0 - y_0. \end{aligned}$$

For $n = 1$,

$$\begin{aligned} w_1(\iota_0, \iota_1) &= w_1(x_0, x_1) - w_1(y_0, y_1) \\ {\iota_0}^p + p\iota_1 &= {x_0}^p + px_1 - {y_0}^p - py_1 \\ (x_0 - y_0)^p + p\iota_1 &= {x_0}^p + px_1 - {y_0}^p - py_1 \end{aligned}$$

and thus solving for $\iota_1$ we have

$$\iota_1 = \iota_1(x,y) = \iota_1(x_0, x_1, y_0, y_1) = x_1 - y_1 - \frac{1}{p}\sum_{i=1}^{p-1}(-1)^i \binom{p}{i} {x_0}^{p-i}{y_0}^{i}.$$

We use the Dwork lemma once more to construct unique polynomials $\mu_n$ that define both the multiplication in $W(R)$ and the comultiplication in the the co-Witt ring.

9**. Corollary.** *There exist unique polynomials*

$$\mu_n = \mu_n(x,y) = \mu_n(x_0,\dots,x_n,y_0,\dots,y_n) \in \mathbb{Z}_p[x_0,x_1,\dots,y_0,y_1,\dots]$$

*such that*

$$w_n(\mu_0,\mu_1,\dots,\mu_n) = w_n(x_0,\dots,x_n)\,w_n(y_0,\dots,y_n).$$

*Proof.* Take $A = \mathbb{Z}_p[x_0,x_1,\dots,y_0,y_1,\dots]$, $f = \phi$, $g_n = w_n(x_0,\dots,x_n)\cdot w_n(y_0,\dots,y_n)$, and $q_n = \mu_n$ in the Dwork lemma. □

10**. Definition.** *The product of two elements* $f, g \in W(R)$ *is given by*

$$\begin{aligned}(f_0, f_1, \dots) \underset{W}{\times} (g_0, g_1, \dots) &= (\mu_0, \mu_1, \dots)\\ &= (\mu_0(f,g), \mu_1(f,g), \dots)\\ &= (\mu_0(f_0,g_0),\, \mu_1(f_0,f_1,g_0,g_1), \dots)\end{aligned}$$

11. *Example.* The polynomials $\mu_0$ and $\mu_1$ are easily calculated by hand. For the case $n = 0$,

$$\begin{aligned}w_0(\mu_0) &= w_0(x_0)\,w_0(y_0)\\ \mu_0 &= x_0y_0.\end{aligned}$$

For $n = 1$,

$$\begin{aligned}w_1(\mu_0,\mu_1) &= w_1(x_0,x_1)\,w_1(y_0,y_1)\\ {\mu_0}^p + p\mu_1 &= ({x_0}^p + px_1)({y_0}^p + py_1)\\ {x_0}^p{y_0}^p + p\mu_1 &= {x_0}^p{y_0}^p + p{x_0}^p y_1 + px_1{y_0}^p + p^2x_1y_1\end{aligned}$$

and thus solving for $\mu_1$ we have

$$\mu_1 = \mu_1(x,y) = \mu_1(x_0,x_1,y_0,y_1) = {x_0}^p y_1 + x_1{y_0}^p + px_1y_1.$$

## 3. The co-Witt ring

The co-Witt ring is the pair of $\mathbb{Z}_p$-algebras $\mathbb{Z}_p$ and $\mathbb{Z}_p[x_0, x_1, \dots]$ that corepresent the covariant ring-valued functor $W(-)$ on the category of $\mathbb{Z}_p$-algebras. This means that the set $\mathrm{Hom}_{\mathbb{Z}_p-alg}(\mathbb{Z}_p, R) = R$ represents the objects of a ring, and the set $\mathrm{Hom}_{\mathbb{Z}_p-alg}(\mathbb{Z}_p[x_0,x_1,\dots], R) = \prod_{i\geq 0} R$ represents the morphisms of a ring. Put another way, $\mathbb{Z}_p[x_0,x_1,\dots]$ is a coring object in the category of $\mathbb{Z}_p$-algebras. In the language of algebraic geometry, the co-Witt ring corepresents an affine ring scheme. We now describe the structure homomorphisms in the co-Witt ring.

(1) The *coaugmentation* in the co-Witt ring is the $\mathbb{Z}_p$-algebra homomorphism

$$\eta : \mathbb{Z}_p \hookrightarrow \mathbb{Z}_p[x_0, x_1, \ldots]$$

given by the canonical inclusion.

(2) The *cozero* in the co-Witt ring is the $\mathbb{Z}_p$-algebra homomorphism

$$\epsilon_0 : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p$$

given by $\epsilon_0(x_n) = 0$ for all $n \geq 0$.

(3) The *counit* in the co-Witt ring is the $\mathbb{Z}_p$-algebra homomorphism

$$\epsilon_1 : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p$$

given by $\epsilon_1(x_0) = 1$, and $\epsilon_\mu(x_n) = 0$ for all $n \geq 1$.

(4) The *coaddition* in the co-Witt ring is the $\mathbb{Z}_p$-algebra homomorphism

$$\Delta_\alpha : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p[x_0, x_1, \ldots] \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[x_0, x_1, \ldots]$$

given by

$$\begin{aligned} \Delta_\alpha(x_n) &= \alpha_n(x \otimes 1, 1 \otimes x) \\ &= \alpha_n(x_0 \otimes 1, \ldots, x_n \otimes 1, 1 \otimes x_0, \ldots, 1 \otimes x_n). \end{aligned}$$

(5) The *cosubtraction* in the co-Witt ring is the $\mathbb{Z}_p$-algebra homomorphism

$$\Delta_\iota : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p[x_0, x_1, \ldots] \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[x_0, x_1, \ldots]$$

given by

$$\begin{aligned} \Delta_\iota(x_n) &= \iota_n(x \otimes 1, 1 \otimes x) \\ &= \iota_n(x_0 \otimes 1, \ldots, x_n \otimes 1, 1 \otimes x_0, \ldots, 1 \otimes x_n). \end{aligned}$$

(6) The *coaddition inverse* in the co-Witt ring is the $\mathbb{Z}_p$-algebra homomorphism

$$\chi : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p[x_0, x_1, \ldots]$$

given by $\chi(x_n) = \iota_n(0, x) = \iota_n(0, \ldots, 0, x_0, x_1, \ldots, x_n)$.

(7) The *comultiplication* in the co-Witt ring is the $\mathbb{Z}_p$-algebra homomorphism

$$\Delta_\mu : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p[x_0, x_1, \ldots] \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[x_0, x_1, \ldots]$$

given by

$$\begin{aligned} \Delta_\mu(x_n) &= \mu_n(x \otimes 1, 1 \otimes x) \\ &= \mu_n(x_0 \otimes 1, \ldots, x_n \otimes 1, 1 \otimes x_0, \ldots, 1 \otimes x_n). \end{aligned}$$

## 4. The Witt vectors as a corepresentable functor

As already mentioned, the Witt vectors are a corepresentable, ring-valued functor on the category of $\mathbb{Z}_p$-algebras. The purpose of this section is to explicitly describe how the coaddition, cosubtraction, and comultiplication in the co-Witt ring determine the addition, subtraction, and multiplication in the ring of Witt vectors $W(R)$ for any $\mathbb{Z}_p$-algebra $R$.

Let $R$ be a $\mathbb{Z}_p$-algebra, and let $f, g : \mathbb{Z}_p[x_0, x_1, \ldots] \to R$ be any elements of $W(R) = \mathrm{Hom}_{\mathbb{Z}_p-alg}(\mathbb{Z}_p[x_0, x_1, \ldots], R)$.

12**. Definition.** *The sum of $f$ and $g$ in $W(R)$ is given by the composite*

$$\mathbb{Z}_p[x_0, x_1, \ldots] \xrightarrow{\Delta_\alpha} \mathbb{Z}_p[x_0, x_1, \ldots] \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[x_0, x_1, \ldots] \xrightarrow{f \otimes g} R \underset{\mathbb{Z}_p}{\otimes} R \to R,$$

*where the last map is given by $a \otimes b \mapsto ab$ on tensor monomials. This sum of $f$ and $g$ defined by the composite is equal to $f \underset{W}{+} g$ defined earlier. Similarly, if we replace $\Delta_\alpha$ in the composite above by $\Delta_\iota$ or $\Delta_\mu$, we obtain the difference or product of $f$ and $g$, and they agree with $f \underset{W}{-} g$ or $f \underset{W}{\times} g$, respectively.*

13. *Example.* Suppose $R$ is a $\mathbb{Z}_p$-algebra, and $f, g : \mathbb{Z}_p[x_0, x_1, \ldots] \to R$ are elements of $W(R)$ that determine sequences $(f_0, f_1, \ldots)$ and $(g_0, g_1, \ldots)$ in $\prod R$, respectively. Then the sum of $f$ and $g$ under the composite

$$\mathbb{Z}_p[x_0, x_1, \ldots] \xrightarrow{\Delta_\alpha} \mathbb{Z}_p[x_0, x_1, \ldots] \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p[x_0, x_1, \ldots] \xrightarrow{f \otimes g} R \underset{\mathbb{Z}_p}{\otimes} R \to R,$$

is given by

$$\begin{array}{rcl} x_0 & \mapsto & x_0 \otimes 1 + 1 \otimes x_0 \\ & \mapsto & f_0 \otimes 1 + 1 \otimes g_0 \\ & \mapsto & f_0 + g_0 \end{array}$$

and

$$\begin{array}{rcl} x_1 & \mapsto & x_1 \otimes 1 + 1 \otimes x_1 - \dfrac{1}{p} \displaystyle\sum_{i=1}^{p-1} \binom{p}{i} {x_0}^{p-i} \otimes {x_0}^{i} \\ & \mapsto & f_1 \otimes 1 + 1 \otimes g_1 - \dfrac{1}{p} \displaystyle\sum_{i=1}^{p-1} \binom{p}{i} {f_0}^{p-i} \otimes {g_0}^{i} \\ & \mapsto & f_1 + g_1 - \dfrac{1}{p} \displaystyle\sum_{i=1}^{p-1} \binom{p}{i} {f_0}^{p-i} {g_0}^{i} \end{array}$$

which is $f \underset{W}{+} g$. The difference and product of $f$ and $g$ are easily found mutatis mutandis.

## 5. Additional structure in the co-Witt ring

## 6. The "complicated" lift of the Frobenius on the co-Witt ring

Recall that the "simple" lift $\phi : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p[x_0, x_1, \ldots]$ of the Frobenius is given by $\phi(x_i) = {x_i}^p$ for all $i \geq 0$. We use the Dwork lemma to construct the complicated lift of the Frobenius.

14**. Corollary.** *The complicated lift*

$$\varphi : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p[x_0, x_1, \ldots]$$

*of the Frobenius is the unique $\mathbb{Z}_p$-algebra homomorphism such that $\varphi(w_n(x)) = w_{n+1}(x)$ for all $n \geq 0$.*

*Proof.* Take $A = \mathbb{Z}_p[x_0, x_1, \ldots]$, $f = \phi$, $g_n = w_{n+1}(x_0, \ldots, x_n)$, and $q_n = \varphi_n$ in the Dwork lemma. Notice that $g_n = w_{n+1}$. □

Straightforward computation shows that the values $\varphi(x_n) = q_n = \varphi_n$ are determined by $w_n(q_0, \ldots, q_n) = w_{n+1}(x_0, \ldots, x_{n+1})$. By using the equation $w_n(q_0, \ldots, q_n) = w_{n-1}({q_0}^p, \ldots, {q_{n-1}}^p) + p^n q_n$ we may solve for $q_n = \varphi(x_n)$ recursively.

To show that the complicated lift $\varphi$ of the Frobenius is actually a lift of the Frobenius, we need an analogue of the Dwork lemma with a weaker notion of uniqueness. In particular, we are interested in knowing when two algebra maps are equal when reduced mod $p$.

15**. Lemma.** *Suppose $A$ is a torsion free $\mathbb{Z}_p$-algebra that has a map $f : A \to A$ so that $f(x) \equiv x^p \mod p$. Suppose that there are two sequences of elements in $A$, $g_n$ and $h_n$, such that $f(g_{n-1}) \equiv g_n \mod p^n$ and $f(h_{n-1}) \equiv h_n \mod p^n$. Then by the Dwork lemma there exist unique sequences of elements $q_n$ and $r_n$ in $A$ such that*

$$w_n(q_0, \ldots, q_n) = g_n, \quad \text{and} \quad w_n(r_0, \ldots, r_n) = h_n.$$

*If $g_n \equiv h_n \mod p^{n+1}$ for all $n \geq 0$, then $q_n \equiv r_n \mod p$.*

In other words, this lemma says that if $g_n \equiv h_n \mod p^{n+1}$ for all $n \geq 0$, then the two induced maps of algebras $q : \mathbb{Z}_p[x_0, x_1, \ldots] \to A$ defined by $q(x_n) = q_n$ for all $n \geq 0$, and $r : \mathbb{Z}_p[x_0, x_1, \ldots] \to A$ defined by $r(x_n) = r_n$ for all $n \geq 0$ are equivalent modulo $p$.

*Proof.* Note that if $x \equiv y \mod p^n$, then $x^{p^k} \equiv y^{p^k} \mod p^{n+k}$. Then from the formula

$$p^n q_n = g_n - w_{n-1}({q_0}^p, \ldots, {q_{n-1}}^p)$$

we have $p^n q_n \equiv p^n r_n \mod p^{n+1}$ and the result follows. □

To see that the complicated lift $\varphi$ of the Frobenius actually is a lift of the Frobenius, note that $\varphi(x_n) = q_n$ where

$$\begin{aligned} w_n(q_0, \ldots, q_n) &= w_{n+1}(x_0, \ldots, x_{n+1}) \\ &\equiv w_n({x_0}^p, \ldots, {x_n}^p) \mod p^{n+1}. \end{aligned}$$

So, by Lemma 15 (using the simple lift $\phi$ of the Frobenius) we have $q_n \equiv {x_n}^p \mod p$ and $\varphi(x) \equiv x^p \mod p$.

## 7. The co-Witt ring is a coalgebra over $\mathbb{Z}_p$

We show that the co-Witt ring has at least two different coalgebra structures, one coming from $\Delta_\alpha$ and the other from $\Delta_\mu$.

16**. Definition.** *A coalgebra over $k$ is a triple $(C, \Delta, \epsilon)$ consisting of an $k$-module $C$, a coproduct $\Delta : C \to C \otimes_k C$ and a counit $\epsilon : C \to k$ that satisfies the coassociativity property $(\Delta \otimes 1) \circ \Delta = (1 \otimes \Delta) \circ \Delta$ and the counitary property $(\epsilon \otimes 1) \circ \Delta = R$ and $(1 \otimes \epsilon) \circ \Delta = L$. Here $L$ and $R$ are the canonical isomorphisms $L : C \to C \otimes_k k$ and $R : C \to k \otimes_k C$.*

17. *Example.* On the co-Witt ring, the additive coalgebra over $\mathbb{Z}_p$ is the triple $(\mathbb{Z}_p[x_0, x_1, \ldots], \Delta_\alpha, \epsilon_0)$.

18. *Example.* On the co-Witt ring, the multiplicative coalgebra over $\mathbb{Z}_p$ is the triple $(\mathbb{Z}_p[x_0, x_1, \ldots], \Delta_\mu, \epsilon_1)$.

The coproduct in a coalgebra corepresents a product in a monoid-valued functor. For a coalgebra to induce a group-valued functor requires the existence of a coproduct inverse or conjugation $\chi : C \to C$. In the examples above, the additive coalgebra has a coproduct inverse $\chi : \mathbb{Z}_p[x_0, x_1, \ldots] \to \mathbb{Z}_p[x_0, x_1, \ldots]$ that we called the coaddition inverse. The multiplicative coalgebra, however, does not have a coproduct inverse.

## 8. Important formal properties of the Witt vectors

In lieu of writing this section, I list some helpful references [Rav04, A 2.2.15], [Rav92, p.39-41].

## 9. Calculations in the ring of Witt vectors and the co-Witt ring

**9.1. Addition and coaddition at the prime 2.** The polynomials $\alpha_n$ that define the addition in the ring of Witt vectors are:

$$\begin{array}{rcl}
\alpha_0(x,y) & = & x_0 + y_0 \\
 & \equiv & x_0 + y_0 \mod 2 \\
\alpha_1(x,y) & = & x_1 + y_1 - x_0\, y_0 \\
 & \equiv & x_1 + y_1 + x_0\, y_0 \mod 2 \\
\alpha_2(x,y) & = & x_2 + y_2 - x_1\, y_1 + x_1\, x_0\, y_0 + y_1\, x_0\, y_0 - 2\, x_0^2\, y_0^2 - x_0^3\, y_0 - x_0\, y_0^3 \\
 & \equiv & x_2 + y_2 + x_1\, y_1 + x_1\, x_0\, y_0 + y_1\, x_0\, y_0 + x_0^3\, y_0 + x_0\, y_0^3 \mod 2
\end{array}$$

The values of the coaddition $\Delta_\alpha$ on the generators $x_n$ are:

$$\begin{array}{rcl}
\Delta_\alpha(x_0) & = & x_0 \otimes 1 + 1 \otimes x_0 \\
 & \equiv & x_0 \otimes 1 + 1 \otimes x_0 \mod 2 \\
\Delta_\alpha(x_1) & = & x_1 \otimes 1 + 1 \otimes x_1 - x_0 \otimes x_0 \\
 & \equiv & x_1 \otimes 1 + 1 \otimes x_1 + x_0 \otimes x_0 \mod 2 \\
\Delta_\alpha(x_2) & = & x_2 \otimes 1 + 1 \otimes x_2 - x_1 \otimes x_1 + x_1\, x_0 \otimes x_0 + x_0 \otimes x_1\, x_0 - 2\, x_0^2 \otimes \\
 & & x_0^2 - x_0^3 \otimes x_0 - x_0 \otimes x_0^3 \\
 & \equiv & x_2 \otimes 1 + 1 \otimes x_2 + x_1 \otimes x_1 + x_1\, x_0 \otimes x_0 + x_0 \otimes x_1\, x_0 + x_0^3 \otimes x_0 + x_0 \otimes x_0^3 \\
 & & \mod 2
\end{array}$$

**9.2. Addition and coaddition at the prime 3.** The polynomials $\alpha_n$ that define the addition in the ring of Witt vectors are:

$$\begin{array}{rcl}
\alpha_0(x,y) & = & x_0 + y_0 \\
 & \equiv & x_0 + y_0 \mod 3 \\
\alpha_1(x,y) & = & x_1 + y_1 - x_0^2\, y_0 - x_0\, y_0^2 \\
 & \equiv & x_1 + y_1 + 2\, x_0^2\, y_0 + 2\, x_0\, y_0^2 \mod 3 \\
\alpha_2(x,y) & = & 2\, x_1\, y_1\, x_0^2\, y_0 + 2\, x_1\, y_1\, x_0\, y_0^2 + x_2 + y_2 + x_1^2\, x_0^2\, y_0 + \\
 & & x_1^2\, x_0\, y_0^2 + y_1^2\, x_0^2\, y_0 + y_1^2\, x_0\, y_0^2 - x_1\, x_0^4\, y_0^2 - 2\, x_1\, x_0^3\, y_0^3 - \\
 & & x_1\, x_0^2\, y_0^4 - y_1\, x_0^4\, y_0^2 - 2\, y_1\, x_0^3\, y_0^3 - y_1\, x_0^2\, y_0^4 - x_1^2\, y_1 - \\
 & & x_1\, y_1^2 - 9\, x_0^6\, y_0^3 - 13\, x_0^5\, y_0^4 - 13\, x_0^4\, y_0^5 - 9\, x_0^3\, y_0^6 - \\
 & & x_0^8\, y_0 - 4\, x_0^7\, y_0^2 - 4\, x_0^2\, y_0^7 - x_0\, y_0^8 \\
 & \equiv & 2\, x_1\, y_1\, x_0^2\, y_0 + 2\, x_1\, y_1\, x_0\, y_0^2 + x_2 + y_2 + x_1^2\, x_0^2\, y_0 + \\
 & & x_1^2\, x_0\, y_0^2 + y_1^2\, x_0^2\, y_0 + y_1^2\, x_0\, y_0^2 + 2\, x_1\, x_0^4\, y_0^2 + x_1\, x_0^3\, y_0^3 + \\
 & & 2\, x_1\, x_0^2\, y_0^4 + 2\, y_1\, x_0^4\, y_0^2 + y_1\, x_0^3\, y_0^3 + 2\, y_1\, x_0^2\, y_0^4 + \\
 & & 2\, x_1^2\, y_1 + 2\, x_1\, y_1^2 + 2\, x_0^5\, y_0^4 + 2\, x_0^4\, y_0^5 + 2\, x_0^8\, y_0 + 2\, x_0^7\, y_0^2 + \\
 & & 2\, x_0^2\, y_0^7 + 2\, x_0\, y_0^8 \mod 3
\end{array}$$

The values of the coaddition $\Delta_\alpha$ on the generators $x_n$ are:

$$
\begin{aligned}
\Delta_\alpha(x_0) &= x_0 \otimes 1 + 1 \otimes x_0 \\
&\equiv x_0 \otimes 1 + 1 \otimes x_0 \mod 3 \\
\Delta_\alpha(x_1) &= x_1 \otimes 1 + 1 \otimes x_1 - {x_0}^2 \otimes x_0 - x_0 \otimes {x_0}^2 \\
&\equiv x_1 \otimes 1 + 1 \otimes x_1 + 2\,{x_0}^2 \otimes x_0 + 2\,x_0 \otimes {x_0}^2 \mod 3 \\
\Delta_\alpha(x_2) &= x_2 \otimes 1 + 1 \otimes x_2 - {x_1}^2 \otimes x_1 + {x_1}^2\,{x_0}^2 \otimes x_0 + {x_1}^2\,x_0 \otimes {x_0}^2 - \\
&\quad x_1 \otimes {x_1}^2 + 2\,x_1\,{x_0}^2 \otimes x_1\,x_0 + 2\,x_1\,x_0 \otimes x_1\,{x_0}^2 - x_1\,{x_0}^4 \otimes {x_0}^2 - \\
&\quad 2\,x_1\,{x_0}^3 \otimes {x_0}^3 - x_1\,{x_0}^2 \otimes {x_0}^4 + {x_0}^2 \otimes {x_1}^2\,x_0 + x_0 \otimes {x_1}^2\,{x_0}^2 - \\
&\quad {x_0}^4 \otimes x_1\,{x_0}^2 - 2\,{x_0}^3 \otimes x_1\,{x_0}^3 - {x_0}^2 \otimes x_1\,{x_0}^4 - 9\,{x_0}^6 \otimes {x_0}^3 - \\
&\quad 13\,{x_0}^5 \otimes {x_0}^4 - 13\,{x_0}^4 \otimes {x_0}^5 - 9\,{x_0}^3 \otimes {x_0}^6 - {x_0}^8 \otimes x_0 - 4\,{x_0}^7 \otimes \\
&\quad {x_0}^2 - 4\,{x_0}^2 \otimes {x_0}^7 - x_0 \otimes {x_0}^8 \\
&\equiv x_2 \otimes 1 + 1 \otimes x_2 + 2\,{x_1}^2 \otimes x_1 + {x_1}^2\,{x_0}^2 \otimes x_0 + {x_1}^2\,x_0 \otimes {x_0}^2 + 2\,x_1 \otimes \\
&\quad {x_1}^2 + 2\,x_1\,{x_0}^2 \otimes x_1\,x_0 + 2\,x_1\,x_0 \otimes x_1\,{x_0}^2 + 2\,x_1\,{x_0}^4 \otimes {x_0}^2 + \\
&\quad x_1\,{x_0}^3 \otimes {x_0}^3 + 2\,x_1\,{x_0}^2 \otimes {x_0}^4 + {x_0}^2 \otimes {x_1}^2\,x_0 + x_0 \otimes {x_1}^2\,{x_0}^2 + \\
&\quad 2\,{x_0}^4 \otimes x_1\,{x_0}^2 + {x_0}^3 \otimes x_1\,{x_0}^3 + 2\,{x_0}^2 \otimes x_1\,{x_0}^4 + 2\,{x_0}^5 \otimes {x_0}^4 + \\
&\quad 2\,{x_0}^4 \otimes {x_0}^5 + 2\,{x_0}^8 \otimes x_0 + 2\,{x_0}^7 \otimes {x_0}^2 + 2\,{x_0}^2 \otimes {x_0}^7 + 2\,x_0 \otimes {x_0}^8 \\
&\quad \mod 3
\end{aligned}
$$

9.3. **Addition and coaddition at the prime 5.** The polynomials $\alpha_n$ that define the addition in the ring of Witt vectors are:

$$
\begin{aligned}
\alpha_0(x,y) &= x_0 + y_0 \\
&\equiv x_0 + y_0 \mod 5 \\
\alpha_1(x,y) &= x_1 + y_1 - {x_0}^4\,y_0 - 2\,{x_0}^3\,{y_0}^2 - 2\,{x_0}^2\,{y_0}^3 - x_0\,{y_0}^4 \\
&\equiv x_1 + y_1 + 4\,{x_0}^4\,y_0 + 3\,{x_0}^3\,{y_0}^2 + 3\,{x_0}^2\,{y_0}^3 + 4\,x_0\,{y_0}^4 \mod 5
\end{aligned}
$$

The values of the coaddition $\Delta_\alpha$ on the generators $x_n$ are:

$$
\begin{aligned}
\Delta_\alpha(x_0) &= x_0 \otimes 1 + 1 \otimes x_0 \\
&\equiv x_0 \otimes 1 + 1 \otimes x_0 \mod 5 \\
\Delta_\alpha(x_1) &= x_1 \otimes 1 + 1 \otimes x_1 - {x_0}^4 \otimes x_0 - 2\,{x_0}^3 \otimes {x_0}^2 - 2\,{x_0}^2 \otimes {x_0}^3 - x_0 \otimes {x_0}^4 \\
&\equiv x_1 \otimes 1 + 1 \otimes x_1 + 4\,{x_0}^4 \otimes x_0 + 3\,{x_0}^3 \otimes {x_0}^2 + 3\,{x_0}^2 \otimes {x_0}^3 + 4\,x_0 \otimes {x_0}^4 \\
&\quad \mod 5
\end{aligned}
$$

9.4. **The multiplication and comultiplication at the prime 2.** The polynomials $\mu_n$ that define the multiplication in the ring of Witt vectors are:

$$
\begin{aligned}
\mu_0(x,y) &= x_0 y_0 \\
&\equiv x_0 y_0 \mod 2 \\
\mu_1(x,y) &= {x_0}^2\,y_1 + x_1\,{y_0}^2 + 2\,x_1\,y_1 \\
&\equiv {x_0}^2\,y_1 + x_1\,{y_0}^2 \mod 2 \\
\mu_2(x,y) &= {x_0}^4\,y_2 - {x_1}^2\,{y_1}^2 + 2\,{x_1}^2\,y_2 + x_2\,{y_0}^4 + 2\,x_2\,{y_1}^2 + 4\,x_2\,y_2 - \\
&\quad {x_0}^2\,y_1\,x_1\,{y_0}^2 - 2\,{x_0}^2\,{y_1}^2\,x_1 - 2\,{x_1}^2\,{y_0}^2\,y_1 \\
&\equiv {x_0}^4\,y_2 + {x_1}^2\,{y_1}^2 + x_2\,{y_0}^4 + {x_0}^2\,y_1\,x_1\,{y_0}^2 \mod 2
\end{aligned}
$$

The values of the comultiplication $\Delta_\mu$ on the generators $x_n$ are:

$$
\begin{aligned}
\Delta_\mu(x_0) &= x_0 \otimes x_0 \\
&\equiv x_0 \otimes x_0 \mod 2 \\
\Delta_\mu(x_1) &= x_1 \otimes x_0{}^2 + x_0{}^2 \otimes x_1 + 2\, x_1 \otimes x_1 \\
&\equiv x_1 \otimes x_0{}^2 + x_0{}^2 \otimes x_1 \mod 2 \\
\Delta_\mu(x_2) &= x_2 \otimes x_0{}^4 - x_1{}^2 \otimes x_1{}^2 + 2x_2 \otimes x_1{}^2 + x_0{}^4 \otimes x_2 + 2x_1{}^2 \otimes x_2 + \\
&\quad 4x_2 \otimes x_2 - x_1 x_0{}^2 \otimes x_1 x_0{}^2 - 2x_1{}^2 \otimes x_1 x_0{}^2 - 2x_1 x_0{}^2 \otimes x_1{}^2 \\
&\equiv x_2 \otimes x_0{}^4 + x_1{}^2 \otimes x_1{}^2 + x_0{}^4 \otimes x_2 + x_1\, x_0{}^2 \otimes x_1\, x_0{}^2 \mod 2
\end{aligned}
$$

9.5. **The multiplication and comultiplication at the prime 3.** The polynomials $\mu_n$ that define the multiplication in the ring of Witt vectors are:

$$
\begin{aligned}
\mu_0(x,y) &= x_0 y_0 \\
&\equiv x_0 y_0 \mod 3 \\
\mu_1(x,y) &= x_0{}^3\, y_1 + x_1\, y_0{}^3 + 3\, x_1\, y_1 \\
&\equiv x_0{}^3\, y_1 + x_1\, y_0{}^3 \mod 3 \\
\mu_2(x,y) &= x_0{}^9\, y_2 - 8\, x_1{}^3\, y_1{}^3 + 3\, x_1{}^3\, y_2 + x_2\, y_0{}^9 + 3\, x_2\, y_1{}^3 + \\
&\quad 9\, x_2\, y_2 - x_0{}^6\, y_1{}^2\, x_1\, y_0{}^3 - 3\, x_0{}^6\, y_1{}^3\, x_1 - x_0{}^3\, y_1\, x_1{}^2\, y_0{}^6 - \\
&\quad 6\, x_0{}^3\, y_1{}^2\, x_1{}^2\, y_0{}^3 - 9\, x_0{}^3\, y_1{}^3\, x_1{}^2 - 3\, x_1{}^3\, y_0{}^6\, y_1 - 9\, x_1{}^3\, y_0{}^3\, y_1{}^2 \\
&\equiv x_0{}^9\, y_2 + x_1{}^3\, y_1{}^3 + x_2\, y_0{}^9 + 2\, x_0{}^6\, y_1{}^2\, x_1\, y_0{}^3 + 2\, x_0{}^3\, y_1\, x_1{}^2\, y_0{}^6 \\
&\quad \mod 3
\end{aligned}
$$

The values of the comultiplication $\Delta_\mu$ on the generators $x_n$ are:

$$
\begin{aligned}
\Delta_\mu(x_0) &= x_0 \otimes x_0 \\
&\equiv x_0 \otimes x_0 \mod 3 \\
\Delta_\mu(x_1) &= x_1 \otimes x_0{}^3 + x_0{}^3 \otimes x_1 + 3\, x_1 \otimes x_1 \\
&\equiv x_1 \otimes x_0{}^3 + x_0{}^3 \otimes x_1 \mod 3 \\
\Delta_\mu(x_2) &= x_2 \otimes x_0{}^9 - 8\, x_1{}^3 \otimes x_1{}^3 + 3\, x_2 \otimes x_1{}^3 + x_0{}^9 \otimes x_2 + 3\, x_1{}^3 \otimes \\
&\quad x_2 + 9\, x_2 \otimes x_2 - x_1{}^2\, x_0{}^3 \otimes x_1\, x_0{}^6 - 3\, x_1{}^3 \otimes x_1\, x_0{}^6 - x_1\, x_0{}^6 \otimes \\
&\quad x_1{}^2\, x_0{}^3 - 6\, x_1{}^2\, x_0{}^3 \otimes x_1{}^2\, x_0{}^3 - 9\, x_1{}^3 \otimes x_1{}^2\, x_0{}^3 - 3\, x_1\, x_0{}^6 \otimes \\
&\quad x_1{}^3 - 9\, x_1{}^2\, x_0{}^3 \otimes x_1{}^3 \\
&\equiv x_2 \otimes x_0{}^9 + x_1{}^3 \otimes x_1{}^3 + x_0{}^9 \otimes x_2 + 2\, x_1{}^2\, x_0{}^3 \otimes x_0{}^6\, x_1 + 2\, x_0{}^6\, x_1 \otimes \\
&\quad x_1{}^2\, x_0{}^3 \mod 3
\end{aligned}
$$

9.6. **The multiplication and comultiplication at the prime 5.** The polynomials $\mu_n$ that define the multiplication in the ring of Witt vectors are:

$$
\begin{aligned}
\mu_0(x,y) &= x_0 y_0 \\
&\equiv x_0 y_0 \mod 5 \\
\mu_1(x,y) &= x_0{}^5\, y_1 + x_1\, y_0{}^5 + 5\, x_1\, y_1 \\
&\equiv x_0{}^5\, y_1 + x_1\, y_0{}^5 \mod 5 \\
\mu_2(x,y) &= -624\, x_1{}^5\, y_1{}^5 - x_0{}^{20}\, y_1{}^4\, x_1\, y_0{}^5 - 2\, x_0{}^{15}\, y_1{}^3\, x_1{}^2\, y_0{}^{10} - \\
&\quad 20\, x_0{}^{15}\, y_1{}^4\, x_1{}^2\, y_0{}^5 - 2\, x_0{}^{10}\, y_1{}^2\, x_1{}^3\, y_0{}^{15} - \\
&\quad 30\, x_0{}^{10}\, y_1{}^3\, x_1{}^3\, y_0{}^{10} - 150\, x_0{}^{10}\, y_1{}^4\, x_1{}^3\, y_0{}^5 - \\
&\quad 20\, x_0{}^5\, y_1{}^2\, x_1{}^4\, y_0{}^{15} - 150\, x_0{}^5\, y_1{}^3\, x_1{}^4\, y_0{}^{10} - \\
&\quad 500\, x_0{}^5\, y_1{}^4\, x_1{}^4\, y_0{}^5 - x_0{}^5\, y_1\, x_1{}^4\, y_0{}^{20} - 5\, x_0{}^{20}\, y_1{}^5\, x_1 - \\
&\quad 50\, x_0{}^{15}\, y_1{}^5\, x_1{}^2 - 250\, x_0{}^{10}\, y_1{}^5\, x_1{}^3 - 625\, x_0{}^5\, y_1{}^5\, x_1{}^4 - \\
&\quad 5\, x_1{}^5\, y_0{}^{20}\, y_1 - 50\, x_1{}^5\, y_0{}^{15}\, y_1{}^2 - 250\, x_1{}^5\, y_0{}^{10}\, y_1{}^3 - \\
&\quad 625\, x_1{}^5\, y_0{}^5\, y_1{}^4 + x_0{}^{25}\, y_2 + 5\, x_1{}^5\, y_2 + x_2\, y_0{}^{25} + 5\, x_2\, y_1{}^5 + \\
&\quad 25\, x_2\, y_2 \\
&\equiv x_1{}^5\, y_1{}^5 + 4\, x_0{}^{20}\, y_1{}^4\, x_1\, y_0{}^5 + 3\, x_0{}^{15}\, y_1{}^3\, x_1{}^2\, y_0{}^{10} + \\
&\quad 3\, x_0{}^{10}\, y_1{}^2\, x_1{}^3\, y_0{}^{15} + 4\, x_0{}^5\, y_1\, x_1{}^4\, y_0{}^{20} + x_0{}^{25}\, y_2 + x_2\, y_0{}^{25} \\
&\quad \mod 5
\end{aligned}
$$

The values of the comultiplication $\Delta_\mu$ on the generators $x_n$ are:

$$
\begin{aligned}
\Delta_\mu(x_0) &= x_0 \otimes x_0 \\
&\equiv x_0 \otimes x_0 \mod 5 \\
\Delta_\mu(x_1) &= x_1 \otimes x_0{}^5 + x_0{}^5 \otimes x_1 + 5\, x_1 \otimes x_1 \\
&\equiv x_1 \otimes x_0{}^5 + x_0{}^5 \otimes x_1 \mod 5 \\
\Delta_\mu(x_2) &= 25\, x_2 \otimes x_2 - 624\, x_1{}^5 \otimes x_1{}^5 + 5\, x_1{}^5 \otimes x_2 + x_2 \otimes x_0{}^{25} + \\
&\quad x_0{}^{25} \otimes x_2 + 5\, x_2 \otimes x_1{}^5 - x_0{}^{20}\, x_1 \otimes x_1{}^4\, x_0{}^5 - 20\, x_0{}^{15}\, x_1{}^2 \otimes \\
&\quad x_1{}^4\, x_0{}^5 - 500\, x_1{}^4\, x_0{}^5 \otimes x_1{}^4\, x_0{}^5 - x_1{}^4\, x_0{}^5 \otimes x_0{}^{20}\, x_1 - 5\, x_1{}^5 \otimes \\
&\quad x_0{}^{20}\, x_1 - 50\, x_1{}^5 \otimes x_0{}^{15}\, x_1{}^2 - 2\, x_0{}^{10}\, x_1{}^3 \otimes x_0{}^{15}\, x_1{}^2 - 2\, x_0{}^{15}\, x_1{}^2 \otimes \\
&\quad x_0{}^{10}\, x_1{}^3 - 20\, x_1{}^4\, x_0{}^5 \otimes x_0{}^{15}\, x_1{}^2 - 625\, x_1{}^4\, x_0{}^5 \otimes x_1{}^5 - \\
&\quad 50\, x_0{}^{15}\, x_1{}^2 \otimes x_1{}^5 - 5\, x_0{}^{20}\, x_1 \otimes x_1{}^5 - 250\, x_0{}^{10}\, x_1{}^3 \otimes x_1{}^5 - \\
&\quad 250\, x_1{}^5 \otimes x_0{}^{10}\, x_1{}^3 - 30\, x_0{}^{10}\, x_1{}^3 \otimes x_0{}^{10}\, x_1{}^3 - 150\, x_1{}^4\, x_0{}^5 \otimes \\
&\quad x_0{}^{10}\, x_1{}^3 - 625\, x_1{}^5 \otimes x_1{}^4\, x_0{}^5 - 150\, x_0{}^{10}\, x_1{}^3 \otimes x_1{}^4\, x_0{}^5 \\
&\equiv 4\, x_0{}^{20}\, x_1 \otimes x_1{}^4\, x_0{}^5 + 4\, x_1{}^4\, x_0{}^5 \otimes x_0{}^{20}\, x_1 + 3\, x_0{}^{10}\, x_1{}^3 \otimes \\
&\quad x_1{}^2\, x_0{}^{15} + 3\, x_1{}^2\, x_0{}^{15} \otimes x_0{}^{10}\, x_1{}^3 + x_0{}^{25} \otimes x_2 + x_1{}^5 \otimes x_1{}^5 + x_2 \otimes x_0{}^{25} \\
&\quad \mod 5
\end{aligned}
$$

9.7. **The "complicated" lift of the Frobenius at the prime 2.** Some values of the complicated lift of the Frobenius at the prime 2 are:

$$
\begin{aligned}
\varphi(x_0) &= x_0{}^2 + 2\, x_1 \\
&\equiv x_0{}^2 \mod 2 \\
\varphi(x_1) &= -x_1{}^2 + 2\, x_2 - 2\, x_1\, x_0{}^2 \\
&\equiv x_1{}^2 \mod 2 \\
\varphi(x_2) &= -4\, x_1{}^4 - x_2{}^2 + 2\, x_3 - 2\, x_0{}^6\, x_1 - 8\, x_0{}^4\, x_1{}^2 - 10\, x_0{}^2\, x_1{}^3 + \\
&\quad 2\, x_1{}^2\, x_2 + 4\, x_2\, x_1\, x_0{}^2 \\
&\equiv x_2{}^2 \mod 2
\end{aligned}
$$

9.8. **The "complicated" lift of the Frobenius at the prime 3.** Some values of the complicated lift of the Frobenius at the prime 3 are:

$$
\begin{aligned}
\varphi(x_0) &= x_0^3 + 3\,x_1 \\
&\equiv x_0^3 \mod 3 \\
\varphi(x_1) &= -8\,x_1^3 + 3\,x_2 - 3\,x_0^6\,x_1 - 9\,x_1^2\,x_0^3 \\
&\equiv x_1^3 \mod 3 \\
\varphi(x_2) &= -2016\,x_1^9 - 8\,x_2^3 + 3\,x_3 - 387\,x_1^4\,x_2\,x_0^6 - 432\,x_1^5\,x_2\,x_0^3 + \\
&\quad 27\,x_2^2\,x_0^6\,x_1 + 81\,x_2^2\,x_1^2\,x_0^3 - 27\,x_2\,x_0^{12}\,x_1^2 - \\
&\quad 162\,x_2\,x_0^9\,x_1^3 - 192\,x_1^6\,x_2 + 72\,x_1^3\,x_2^2 - 3\,x_0^{24}\,x_1 - \\
&\quad 36\,x_0^{21}\,x_1^2 - 243\,x_0^{18}\,x_1^3 - 1053\,x_0^{15}\,x_1^4 - 3087\,x_0^{12}\,x_1^5 - \\
&\quad 6129\,x_0^9\,x_1^6 - 7908\,x_0^6\,x_1^7 - 5985\,x_0^3\,x_1^8 \\
&\equiv x_2^3 \mod 3
\end{aligned}
$$

9.9. **The "complicated" lift of the Frobenius at the prime 5.** Some values of the complicated lift of the Frobenius at the prime 5 are:

$$
\begin{aligned}
\varphi(x_0) &= x_0^5 + 5\,x_1 \\
&\equiv x_0^5 \mod 5 \\
\varphi(x_1) &= -624\,x_1^5 + 5\,x_2 - 5\,x_0^{20}\,x_1 - 50\,x_1^2\,x_0^{15} - 250\,x_0^{10}\,x_1^3 - \\
&\quad 625\,x_1^4\,x_0^5 \\
&\equiv x_1^5 \mod 5
\end{aligned}
$$

## 10. Maple source code

```
> # Reference: "Hopf Rings, Dieudonn\' e Modules, and
  # $E_*(\Omega^2 S^3)$" by Paul Goerss (see references)
> restart: interface(labelling=false);
> # Define the tensor product.
> # Remark: to get the "define" command to work
> # correctly, you may need to download the
> # package for Maple called "Bigebra"
> with(Bigebra):
> define(`&o`,flat,multilinear);
>
> # Define operations for multiplication of tensors
> PTM:=proc(R,S)
  # "Pure tensor" (tensor monomial) multiplication

  # convert R,S to lists of the form [c,[a,b]] that represent
  # c*(a \otimes b)
  # or more generally [c,[a_1,a_2,...,a_n]]
  # represents c*(a_1 \otimes ... \otimes a_n)
  local A,B:
  if type(R,`*`) then
```

```
    A:=[mul(op(i,R),i=1..nops(R)-1),[op([op(R)][nops(R)])]]
  else A:=[1,[op(R)]] fi;
  if type(S,`*`) then
    B:=[mul(op(i,S),i=1..nops(S)-1),[op([op(S)][nops(S)])]]
  else B:=[1,[op(S)]] fi;

  RETURN(A[1]*B[1]*`&o`(seq(A[2,i]*B[2,i],i=1..nops(A[2]))));
  end:
>
> `&*`:=proc(R,S)
  # Multiplies sums of "pure tensors".
  local M,r,s;
  if type(R,`+`) then r:=nops(R) else r:=1 fi; #print(r);
  if type(S,`+`) then s:=nops(S) else s:=1 fi; #print(s);
  if (r=1 and s=1) then
     RETURN(PTM(R,S));

   elif r=1 then
     M:=matrix(r,s,(i,j)->PTM(R,op(j,S)));

   elif s=1 then
     M:=matrix(r,s,(i,j)->PTM(op(i,R),S));

   else
     M:=matrix(r,s,(i,j)->PTM(op(i,R),op(j,S)));
  fi;
  RETURN(add(add(M[i,j],i=1..r),j=1..s))
  end:
>
> `&^`:=proc(a,p)
  # An exponentiation for sums of "pure tensors".
  if type(a,complexcons) then RETURN(a^p);
  elif p=0 then RETURN(1);
  elif p=1 then RETURN(a);
  else RETURN(`&*`(a,`&^`(a,p-1))); fi;
  end:
>
> # Define w(p,n,x) = w_n(x) at the prime p;
  # this is defined on p.5 of Goerss's paper
> w:=(p,n,x)->expand(add(p^i*x[i]^(p^(n-i)),i=0..n));
>
> w(p,0,x);
> w(p,1,x);
> w(p,2,x);
>
```

```
> # Define the unique polynomials a(p,n,x,y) = a_n(x,y)
  # at the prime p that define the addition in the ring
  # of Witt vectors.  The polynomials a_n satisfy
  # w_n(a_0,a_1,...,a_n) = w_n(x_0,...,x_n) + w_n(y_0,...,y_n),
  # and they induce the comultiplication
  # \Delta_a : x_n \mapsto a_n(x \otimes 1, 1 \otimes x).
  # This is from Corollary 1.3 in Goerss's paper
> a:=(p,n,x,y)->simplify(expand((w(p,n,x)+w(p,n,y)
  -add(p^(n-i)*a(p,n-i,x,y)^(p^i),i=1..n))/p^n));
>
> a(2,0,x,y);
> a(2,1,x,y);
> a(2,2,x,y);
>
> a(3,0,x,y);
> a(3,1,x,y);
> a(3,2,x,y);
>
> a(5,0,x,y);
> a(5,1,x,y);
> a(5,2,x,y):
>
> amodp:=(p,n,x,y)->simplify(expand((w(p,n,x)+w(p,n,y)
  -add(p^(n-i)*a(p,n-i,x,y)^(p^i),i=1..n))/p^n)) mod p;
>
> amodp(2,0,x,y);
> amodp(2,1,x,y);
> amodp(2,2,x,y);
>
> amodp(3,0,x,y);
> amodp(3,1,x,y);
> amodp(3,2,x,y);
>
> amodp(5,0,x,y);
> amodp(5,1,x,y);
> amodp(5,2,x,y):
>

> # CPA (CoProduct inducing Addition) define the coproduct
  # that induces addition in the Witt vectors; this map CPA
  # is the diagonal map \Delta of equation 1.2 in Goerss's
  # paper; this is just the tensor product version of
  # a_n(x,y) = a(p,n,x,y).
  # CPA(p,n,x) = \Delta(x_n) = a_n(x \otimes 1, 1 \otimes x)
```

```
  # where (x \otimes 1) = (x_0 \otimes 1, x_2 \otimes 1, ...)
>
> # Define the Witt polynomial w_left(p,n,x) = w_n(x \otimes 1)
> w_left:=(p,n,x)->expand(add(&o(p^i*x[i]^(p^(n-i)),1),i=0..n));
> w_left(p,0,x);
> w_left(p,1,x);
> w_left(p,2,x);
>
> # Define the Witt polynomial w_right(p,n,x) = w_n(1 \otimes x)
> w_right:=(p,n,x)->expand(add(&o(1,p^i*x[i]^(p^(n-i))),i=0..n));
> w_right(p,0,x);
> w_right(p,1,x);
> w_right(p,2,x);
>
> CPA:=(p,n,x)->
  if n=0 then &o(x[0],1)+&o(1,x[0]) elif n > 0 then
  expand((w_left(p,n,x)+w_right(p,n,x)
  -add(p^(n-i)*CPA(p,n-i,x)&^(p^i),i=1..n))/p^n) end if:
>
> CPA(2,0,x);
> CPA(2,1,x);
> CPA(2,2,x);
>
> CPA(3,0,x);
> CPA(3,1,x);
> CPA(3,2,x);
>
> CPA(5,0,x);
> CPA(5,1,x);
> CPA(5,2,x);
>
> # Define a mod p version of the coproduct that induces
  # addition.  This map defines the Hopf group (algebra)
  # H(n) defined just above Lemma 4.1 in Goerss's paper.
  # H(n) is a projective generator in \script{HA}.
  # CPAmodp(p,n,x) = \Delta(x_n) mod p
  # = a_n(x \otimes 1, 1 \otimes x) mod p
> CPAmodp:=(p,n,x)->
  if n=0 then &o(x[0],1)+&o(1,x[0]) elif n > 0 then
  expand((w_left(p,n,x)+w_right(p,n,x)
  -add(p^(n-i)*CPAmodp(p,n-i,x)&^(p^i),i=1..n))/p^n)
  mod p end if:
>
> CPAmodp(2,0,x);
> CPAmodp(2,1,x);
```

```
> CPAmodp(2,2,x);
>
> CPAmodp(3,0,x);
> CPAmodp(3,1,x);
> CPAmodp(3,2,x);
>
> CPAmodp(5,0,x);
> CPAmodp(5,1,x);
> CPAmodp(5,2,x);

> # Define the unique polynomials m(p,n,x,y) = m_n(x,y)
  # at the prime p that define multiplication in the ring
  # of Witt vectors.  These polynomials m_n satisfy the
  # equations
  # w_n(m_0,...,m_n) = w_n(x_0,...,x_n)*w_n(y_0,...,y_n).
  # They are used to define the comultiplication
  # \Delta_m: x_n \mapsto m_n(x \otimes 1, 1 \otimes x)
  # which induces multiplication in the Witt vector ring scheme.
>
> w_list:=(p,n,L)->add(p^i*(L[i+1])^(p^(n-i)),i=0..n);
> # p is the prime, n+1 is the number of variables,
  # and L is the list of variables
>
> m:=(p,n,x,y)->
  if n=0 then RETURN(x[0]*y[0]);
  else RETURN( expand(w_list(p,n,[seq(x[i],i=0..n)])
  *w_list(p,n,[seq(y[i],i=0..n)])
  - expand(w_list(p,n-1,[seq((m(p,i,x,y))^p,i=0..n-1)])) )/(p^n) );
  fi:
>
> m(2,0,x,y);
> m(2,1,x,y);
> m(2,2,x,y);
>
> m(3,0,x,y);
> m(3,1,x,y);
> m(3,2,x,y);
>
> m(5,0,x,y);
> m(5,1,x,y);
> m(5,2,x,y);
>
> mmodp:=(p,n,x,y)->
> if n=0 then RETURN(x[0]*y[0]);
  else RETURN( (expand(w_list(p,n,[seq(x[i],i=0..n)])
```

```
  *w_list(p,n,[seq(y[i],i=0..n)])
  - expand(w_list(p,n-1,[seq((m(p,i,x,y))^p,i=0..n-1)]))
  )/(p^n)) mod p );
  fi:
>
> mmodp(2,0,x,y);
> mmodp(2,1,x,y);
> mmodp(2,2,x,y);
>
> mmodp(3,0,x,y);
> mmodp(3,1,x,y);
> mmodp(3,2,x,y);
>
> mmodp(5,0,x,y);
> mmodp(5,1,x,y);
> mmodp(5,2,x,y);
>

> # CPM (CoProduct inducing Multiplication) the coproduct
  # map that induces multiplication in the ring of Witt
  # vectors; this map is given in Remark 1.5.3 of Goerss's paper
> # CPM(p,n,x) = w_n(x \otimes 1) w_n(1 \otimes x)
> w_tensor:=(p,n,L)->add(p^i*(L[i+1])&^(p^(n-i)),i=0..n);
> CPM:=(p,n,x)->
  if n=0 then RETURN(&o(x[0],x[0]));
  else RETURN( expand( &*(w_left(p,n,x),w_right(p,n,x))
  - expand(w_tensor(p,n-1,[seq((CPM(p,i,x))&^p,i=0..n-1)])))/(p^n) );
  fi:
>
> CPM(2,0,x);
> CPM(2,1,x);
> CPM(2,2,x);
>
> CPM(3,0,x);
> CPM(3,1,x);
> CPM(3,2,x);
>
> CPM(5,0,x);
> CPM(5,1,x);
> CPM(5,2,x);
>
> # Define a mod p version of the coproduct that induces
  # multiplication; I'm not sure that this is a structure map for H(n)...
> CPMmodp:=(p,n,x)->
  if n=0 then RETURN(&o(x[0],x[0]));
```

```
  else RETURN( expand( &*(w_left(p,n,x),w_right(p,n,x))
  - expand(w_tensor(p,n-1,[seq((CPM(p,i,x))&^p,i=0..n-1)])))/(p^n) mod p);
  fi:
>
> CPMmodp(2,0,x);
> CPMmodp(2,1,x);
> CPMmodp(2,2,x);
>
> CPMmodp(3,0,x);
> CPMmodp(3,1,x);
> CPMmodp(3,2,x);
>
> CPMmodp(5,0,x);
> CPMmodp(5,1,x);
> CPMmodp(5,2,x);

> # The value of the Frobenius on x_n is q_n.  We calculate
  # the values of the Frobenius \varphi : CW(\infty) \to
  # CW(\infty) = \Z_p[x_0,x_1,\ldots] on the elements x_n,
  # as given by \varphi(x_n) = q_n where the q_i are the
  # unique polynomials that satisfy w_n(q_0,\ldots,q_n)
  # = w_{n+1}(x_0,\ldots,x_{n+1}) by Goerss's paper p.8
>
> w_list(p,1,[seq(x[i],i=0..1)]);
> # so q_0 = q_0(x[0],x[1]) = x[0]^p + p*x[1] ;
  # note that q_0 is a function of two variables!
>
> # \varphi(x_n) = q_n = q(p,n) = q_n(x_0,x_1,...,x_{n+1}) below
> q:=(p,n)->
  if n=0 then RETURN(x[0]^p+p*x[1]);
  else RETURN( (w_list(p,n+1,[seq(x[i],i=0..n+1)])
  - expand(w_list(p,n-1,[seq((q(p,i))^p,i=0..n-1)])) )/(p^n) );
  fi:
> q(2,0); q(2,0) mod 2;
> q(2,1); q(2,1) mod 2;
> q(2,2); q(2,2) mod 2;
> q(3,0); q(3,0) mod 3;
> q(3,1); q(3,1) mod 3;
> q(3,2); q(3,2) mod 3;
> q(5,0); q(5,0) mod 5;
> q(5,1); q(5,1) mod 5;
> q(5,2); q(5,2) mod 5;
```

## References


[Dem72] Michel Demazure, *Lectures on p-divisible groups*, Springer-Verlag, Berlin, 1972, Lecture Notes in Mathematics, Vol. 302. MR MR0344261 (49 #9000)

[Dem86] ______, *Lectures on p-divisible groups*, Lecture Notes in Mathematics, vol. 302, Springer-Verlag, Berlin, 1986, Reprint of the 1972 original. MR **MR883960 (88a:**14049)

[Fri03] Eric M. Friedlander, *Lectures on the cohomology of finite group schemes*, Rational representations, the Steenrod algebra and functor homology, Panor. Synthèses, vol. 16, Soc. Math. France, Paris, 2003, pp. 27–53. MR MR2117527

[Goe99] Paul G. Goerss, *Hopf rings, Dieudonné modules, and $E_*\Omega^2S^3$*, Homotopy invariant algebraic structures (Baltimore, MD, 1998), Contemp. Math., vol. 239, Amer. Math. Soc., Providence, RI, 1999, pp. 115–174. MR **MR1718079 (2000j:**57078)

[Rav86] Douglas C. Ravenel, *Complex cobordism and stable homotopy groups of spheres*, Pure and Applied Mathematics, vol. 121, Academic Press Inc., Orlando, FL, 1986. MR **MR860042 (87j:**55003)

[Rav92] ______, *Nilpotence and periodicity in stable homotopy theory*, Annals of Mathematics Studies, vol. 128, Princeton University Press, Princeton, NJ, 1992, Appendix C by Jeff Smith. MR **MR1192553 (94b:**55015)

[Rav04] *Complex cobordism and stable homotopy groups of spheres*, 2 ed., AMS Chelsea Publishing, 2004, http://www.math.rochester.edu/people/faculty/drav/mu.html.

[Rez] Charles Rezk, *Supplementary notes for math 512 (version 0.17)*, http://www.math.uiuc.edu/~rezk/512-spr2001-notes.dvi.