WITT VECTOR RINGS AND QUOTIENTS OF MONOID ALGEBRAS

Sina Ghassemi-Tabar

Abstract. In a previous paper Cuntz and Deninger introduced the ring $C(R)$ for a perfect $\mathbb{F}_p$-algebra $R$. The ring $C(R)$ is canonically isomorphic to the $p$-typical Witt ring $W(R)$. In fact there exist canonical isomorphisms $\alpha_n : \mathbb{Z}R/I^n \sim \rightarrow W_n(R)$. In this paper we give explicit descriptions of the isomorphisms $\alpha_n$ for $n \geq 2$ if $p \geq n$.

1 Introduction

For a perfect $\mathbb{F}_p$-algebra $R$ consider the monoid algebra $\mathbb{Z}R$ where $R$ is viewed as a monoid under multiplication. In [1] the ring $C(R)$ is constructed as the $I$-adic completion of $\mathbb{Z}R$ where $I$ is the kernel of the natural projection $\pi : \mathbb{Z}R \rightarrow R$. It turns out that $C(R)$ is a strict $p$-ring with $C(R)/pC(R) = R$ and therefore canonically isomorphic to the ring of $p$-typical Witt vectors of $R$. As an immediate consequence we have a unique isomorphism $\alpha_n : \mathbb{Z}R/I^n \sim \rightarrow W_n(R)$ for every $n \geq 2$, c.f. [1] Remark 6 and Corollary 7. In [1] there is an explicit description of the isomorphism $\alpha_2 : \mathbb{Z}R/I^2 \sim \rightarrow W_2(R)$. It was verified by using addition and multiplication on the truncated Witt ring $W_2(R)$ to prove that $\alpha_2$ is a homomorphism and to conclude that it has to be the unique isomorphism.

We choose another approach to calculate the isomorphism $\alpha_n$ by using the inverse map $\beta_n : W_n(R) \sim \rightarrow \mathbb{Z}R/I^n$ given by the formula

$$\beta_n(r_0, r_1, \ldots, r_{n-1}) = \sum_{k=0}^{n-1} p^k [\phi^{-k}(r_k)] \mod I^n \quad (1)$$

where $\phi$ is the Frobenius automorphism on $R$, c.f. [2] Corollary 6.5, [5] §5. For background on the classical theory of Witt vectors see [3], [4]. I would like to thank C. Deninger for suggesting the topic of this note and for helpful discussions.

2 Determination of the isomorphism $\alpha_n$

Let $R$ be a perfect $\mathbb{F}_p$-algebra. Consider the map $\phi : \mathbb{Z}R \rightarrow \mathbb{Z}R, \sum n_r [r] \mapsto \sum n_r [r^p]$. We have $\phi(x) \equiv x^p \mod p \mathbb{Z}R$ for $x \in \mathbb{Z}R$. Therefore we can introduce the “arithmetic derivation”

$$\delta : \mathbb{Z}R \rightarrow \mathbb{Z}R, \quad x \mapsto \frac{1}{p} (\phi(x) - x^p).$$

We mention some immediate facts about $\delta.$
Proposition 1 ([1] page 2). For $x, y, x_1, \ldots, x_n \in \mathbb{Z}R$ we have:

(i) \[ \delta(x + y) = \delta(x) + \delta(y) - \sum_{k=1}^{n-1} \frac{1}{p^k} x^k y^{p-k} \] (2)

(ii) \[ \delta(xy) = \delta(x)\phi(y) + x^p\delta(y) \] (3)

(iii) \[ \delta(x_1 \cdots x_n) = \sum_{k=1}^{n} x_1^p \cdots x_{k-1}^p \delta(x_k)\phi(x_{k+1}) \cdots \phi(x_n) \]

(iv) \[ \delta(x + y) \equiv \delta(x) + \delta(y) \mod I^n \quad \text{if } x \in I^n \text{ or } y \in I^n \] (4)

(v) \[ \delta(I^n) \subset I^{n-1} \quad \text{for } n \geq 1 \] (5)

With these properties we are able to derive equations which will be useful for determining the map $\alpha_n$ above.

Lemma 2. For $a, b, c \in \mathbb{Z}R$ we get:

(i) \[ a \equiv b \mod I^n \Rightarrow \delta(a) \equiv \delta(b) \mod I^{n-1} \] (6)

(ii) \[ a \equiv b + c \mod I^n \text{ and } c \in I^{n-1} \Rightarrow \delta(a) \equiv \delta(b) + \delta(c) \mod I^{n-1} \] (7)

(iii) \[ ab \in I^n \Rightarrow \delta(a + b) \equiv \delta(a) + \delta(b) \mod I^n \] (8)

(iv) \[ \delta(p) \equiv 1 \mod I^{p-1} \] (9)

(v) \[ \delta(pa) \equiv \phi(a) \mod I^{p-1} \]

In particular \[ \delta(pa) \equiv \phi(a) \mod I^k \quad \text{for all } 0 < k < p. \] (10)
Proof. (i) For $y \in I^n$ we have by using equations (4) and (5)
\[
a = b + y \Rightarrow \delta(a) = \delta(b + y) \equiv \delta(b) + \delta(y) \mod I^n \equiv \delta(b) \mod I^{n-1}
\]
since $\delta(y) \in I^{n-1}$ and $I^n \subseteq I^{n-1}$.

(ii) For $c \in I^{n-1}$ we have by using equations (4) and (6)
\[
a \equiv b + c \mod I^n \Rightarrow \delta(a) \equiv \delta(b + c) \mod I^{n-1} \equiv \delta(b) + \delta(c) \mod I^{n-1}.
\]

(iii) The assertion follows from equation (2) because for $1 \leq k \leq p - 1$ every binomial coefficient $\binom{p}{k}$ is divisible by $p$.

(iv) \[
\delta(p) = \delta(p \cdot 1) = [1] - p^{p-1}[1] \equiv [1] \mod I^{p-1} \equiv 1 \mod I^{p-1}
\]

(v) \[
\delta(pa) \equiv \delta(p)\phi(a) + p^p \delta(a) \equiv \delta(p)\phi(a) \mod I^{p-1} \equiv \phi(a) \mod I^{p-1}
\]

As already mentioned, our aim is to describe the isomorphisms $\alpha_n : \mathbb{Z}R/I^n \sim \rightarrow W_n(R)$ for $n \in \mathbb{N}$ by explicit formulas. We begin with the case $n = 2$ to clarify the method.

Determining the isomorphism $\alpha_2$

We obtain an explicit formula for the isomorphism $\alpha_2 : \mathbb{Z}R/I^2 \sim \rightarrow W_2(R)$ by using the inverse map $\beta_2$ and the arithmetic derivation $\delta$. Because of formula (1) we know that for every element $x \in \mathbb{Z}R/I^2$ there exist uniquely determined elements $r_0, r_1 \in R$ with
\[
x = \beta_2(r_0, r_1) = [r_0] + p[\phi^{-1}(r_1)] \mod I^2 \quad \text{and} \quad \alpha_2(x) = (r_0, r_1).
\]

Note here that $p \in I$ since $R$ is an $\mathbb{F}_p$-algebra. So by reducing the first equation modulo $I$ we obtain $x \equiv [r_0] \mod I$ in $\mathbb{Z}R$ and therefore $r_0 = \pi(x)$. Substituting $\pi(x)$ for $r_0$ in the above equation, we have the identity
\[
x \equiv \pi(x) + p[\phi^{-1}(r_1)] \mod I^2.
\]

The remaining component $r_1$ can now be determined by applying $\delta$. We define $a$ to be $a := \phi^{-1}(r_1)$. By applying $\delta$ to the second term on the right-hand side we have
\[
\delta(p[a]) = \frac{1}{p}(\phi(p[a]) - (p[a])^p) = \frac{1}{p}(p[a^p] - p^p[a^p]) = [a^p] - p^{p-1}[a]^p.
\]
Since \( p - 1 \geq 1 \) and \( \delta([\cdot]) = 0 \) we obtain the following congruence:

\[
\delta(x) \equiv \delta([\pi(x)]) + \delta(p[a]) \mod I \equiv \delta(p[a]) \mod I \equiv [a^p] \mod I \equiv [r_1] \mod I
\]

So for any element \( y \in I \) satisfying \( \delta(x) = [r_1] + y \) we obtain

\[
\pi(\delta(x)) = \pi([r_1] + y) = \pi([r_1]) + \pi(y) = \pi([r_1]) = r_1
\]

since \( I \) is the kernel of the natural projection \( \pi \). In conclusion, the isomorphism \( \alpha_2 \) is given by the formula

\[
\alpha_2(x) = (\pi(x), \pi(\delta(x))). \quad (11)
\]

As mentioned earlier, [1] Proposition 8 uses a different approach to obtain this formula.

**Determining the isomorphism \( \alpha_3 \)**

As already described we have

\[
x \equiv [r_0] + p[\phi^{-1}(r_1)] + p^2[\phi^{-2}(r_2)] \mod I^3
\]

with uniquely determined elements \( r_0, r_1, r_2 \in R \). By reducing modulo \( I^2 \) we obtain analogue results as above for \( r_0 \) and \( r_1 \). So we can focus on calculating the component \( r_2 \). Therefore we apply \( \delta \) two times. Using equation (7) leads to the congruences

\[
\begin{align*}
\delta(x - [r_0]) & \equiv [r_1] - p^{p-1}[r_1] + p[\phi^{-1}(r_2)] - p^{2p-1}[\phi^{-1}(r_2)] \mod I^2 \\
2p - 1 & > 2 \Rightarrow \delta(x - [r_0]) \equiv [r_1] - p^{p-1}[r_1] + p[\phi^{-1}(r_2)] \mod I^2 \\
\end{align*}
\]

At this point we have two different cases depending on the prime number \( p \).

1. case: \( p \geq 3 \)

In this case it applies that \( p^{p-1} \in I^2 \) and we obtain from (\*\*) the congruence

\[
\delta(x - [r_0]) - [r_1] \equiv p[\phi^{-1}(r_2)] \mod I^2.
\]

Applying \( \delta \) once again and using equation (6) we have

\[
\begin{align*}
\delta(\delta(x - [r_0]) - [r_1]) & \equiv \delta(\delta(p^{-1}(r_2))) \mod I \\
\Rightarrow & \delta(\delta(x - [r_0]) - [r_1]) \equiv [r_2] - p^{p-1}[r_2] \mod I \\
\Rightarrow & \delta(\delta(x - [r_0]) - [r_1]) \equiv [r_2] \mod I
\end{align*}
\]

which means that

\[
r_2 = \pi(\delta(\delta(x - [r_0]) - [r_1])).
\]
2. case: $p = 2$

From (*) we obtain
\[
\delta(x - [r_0]) + [r_1] \equiv 2[\phi^{-1}(r_2)] \mod I^2
\]
(6) \Rightarrow \delta(x - [r_0]) + [r_1] \equiv [r_2] - 2[r_2] \mod I
\[
p = 2 \in I \Rightarrow \delta(x - [r_0]) + [r_1] \equiv [r_2] \mod I.
\]
So we have
\[
r_2 = \pi(\delta(x - [r_0]) + [r_1]).
\]
For all prime numbers $p$ the third component is given by
\[
r_2 = \pi(\delta(x - [r_0]) + (-1)^p[r_1])
\]
and the isomorphism $\alpha_3$ is determined by
\[
\alpha_3(x) = (\pi(x), \pi(\delta(x)), \pi(\delta(x - [\pi(x)]) + (-1)^p[\pi(\delta(x))])).
\]
(12)
The same method can be used to determine the isomorphism $\alpha_4$ for all prime numbers $p$. Already in this case the formulas for the small primes $p = 2$ and $p = 3$ are quite complicated. For general $n \geq 2$ we therefore concentrate on the primes $p \geq n$. Here is the main result:

**Theorem 3.** For $n \geq 2$ and $p \geq n$ the $\nu$-th Witt vector component $r_\nu$ of an element $x \in \mathbb{Z}R/I^n$ under the isomorphism $\alpha_n: \mathbb{Z}R/I^n \rightarrow W_n(R) = R^n$ is recursively given by
\[
r_\nu = \pi(\delta(x - [r_0]) - [r_1] - \cdots - [r_{\nu-1}]) \quad \text{for } \nu = 1, \ldots, n-1
\]
with the 0-th component being $r_0 = \pi(x)$.

**Proof.** By formula (1) the elements $r_0, \ldots, r_{n-1} \in R$ are uniquely determined by the formula
\[
x \equiv \sum_{k=0}^{n-1} p^k[\phi^{-k}(r_k)] \mod I^n \quad \left( \in \mathbb{Z}R/I^n \right).
\]
To calculate the components, we proceed inductively. In the following we use equations (6) and (10) to calculate the $\nu$-th component $r_\nu$ for $\nu = 0, \ldots, n-1$. By reducing modulo $I^{\nu+1}$ we obtain
\[
x \equiv \sum_{k=0}^{\nu} p^k[\phi^{-k}(r_k)] \mod I^{\nu+1}.
\]
For $\nu = 0$ we are done by applying $\pi$. Otherwise we continue as follows:

**Step 1:** By subtracting the first term on the right-hand side we have
\[
x - [r_0] \equiv \sum_{k=1}^{\nu} p^k[\phi^{-k}(r_k)] \mod I^{\nu+1}.
\]
Step 2: We now use equation (6) to obtain

\[ \delta(x - [r_0]) \equiv \delta(\sum_{k=1}^{\nu} p^k[\phi^{-k}(r_k)]) \mod I^\nu \equiv \delta(p\left( \sum_{k=1}^{\nu} p^{k-1}[\phi^{-k}(r_k)] \right)) \mod I^\nu. \]

Step 3: Because of our assumption \( p \geq n \) we can use equation (10) to obtain

\[
\begin{align*}
\delta(x - [r_0]) &\equiv \phi(\sum_{k=1}^{\nu} p^{k-1}[\phi^{-k}(r_k)]) \mod I^\nu \\
&\equiv \sum_{k=1}^{\nu} p^{k-1}[\phi^{-(k-1)}(r_k)] \mod I^\nu \\
&\equiv \sum_{k=0}^{\nu-1} p^{k}[\phi^{-k}(r_{k+1})] \mod I^\nu.
\end{align*}
\]

By repeating these three steps \((\nu - 1)\)-times we finally have

\[ [r_{n-1}] \mod I \equiv \delta(\cdots \delta(x - [r_0]) - [r_1]) \cdots - [r_{n-2}]). \]

This implies the assertion by using the natural projection \( \pi \) and \( I = \ker(\pi). \)

Remark 4. Comparing Theorem 3 for \( n = 2 \) and formula (11) we get

\[ \pi(\delta(x)) = \pi(\delta(x - [\pi(x)])). \]

This can also be seen directly.

References

[1] J. Cuntz and C. Deninger. An alternative to Witt vectors. *Münster Journal of Mathematics*, 2013. arXiv:1311.2774.

[2] J. Cuntz and C. Deninger. Witt Vector Rings and the Relative de Rham Witt Complex. 2014. arXiv:1410.5249.

[3] M. Hazewinkel. *Witt Vectors, Part 1*. 2007. arXiv:0804.3888.

[4] J. Rabinoff. The Theory of Witt Vectors. 2014. arXiv:1409.7445.

[5] J.-P. Serre. *Local fields*, volume 67 of Graduate Texts in Mathematics. Springer-Verlag, 1979. Translated from the French by Marvin Jay Greenberg.