BULLETIN OF THE
INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
Volume 26, Number 1, March 1998

ON HILBERT-KUNZ FUNCTION AND REPRESENTATION RING

BY

LI CHIANG (江 立) AND YU CHING HUNG (洪有情)

Abstract. Let p be a prime, $(\mathcal{O}, m)$ a complete local $\mathbb{Z}/(p)$-algebra, and I_n the ideal of $\mathcal{O}$ generated by all a^{p^n} with $a \in m$. By $e_n(\mathcal{O})$ we denote the length of $\mathcal{O}/I_n$. The function $n \mapsto e_n(\mathcal{O})$ is called the Hilbert-Kunz function of $\mathcal{O}$.

In this article, we deduce some multiplication formulae for the representation ring (Cf.§2, §3). By these formulae, we give a new proof of the main theorem in [4]: If $\mathcal{O} = F[|X_1, \ldots, X_t|] /(X_1^{d_1} + \cdots + X_t^{d_t})$ where d_i's are positive integers, then the Hilbert-Kunz function is $n \mapsto cp^{(t-1)n} + \Delta(n)$ where c is rational. For the term Δ, there exist integers ω, l such that $\Delta(n+\omega) = l\Delta(n)$ for $n \gg 0$. We also obtain an explicit algorithm to evaluate c, l, ω and the function Δ for any given prime p and $d_i \geq 1$. By using the representation ring, we can also obtain the Hilbert-Kunz functions of some binomial hypersurfaces. (cf. §6)

1. Introduction. Let p be a prime, $(\mathcal{O}, m)$ a complete local $\mathbb{Z}/(p)$-algebra, and I_n the ideal of $\mathcal{O}$ generated by all a^{p^n} with $a \in m$. By $e_n(\mathcal{O})$ we denote the length of $\mathcal{O}/I_n$. The function $h : n \mapsto e_n(\mathcal{O})$ is called the Hilbert-Kunz function of $\mathcal{O}$.

In [7], Monsky showed that $e_n(\mathcal{O}) = cp^{an} + \Delta_n$ where a is the Krull dimension of $\mathcal{O}$, c a positive real constant, and $\Delta_n = \mathcal{O}(p^{(a-1)n})$. While

$$\mathcal{O} = \mathbb{Z}/(p)[[X_1, X_2, \ldots, X_s]]/(X_1^{d_1} - \prod_{i=2}^{s} X_i^{d_i}),$$

Kunz [6] showed that c is rational and $\Delta_n = \sum_{j=0}^{a-1} \Delta^{(j)}(n) p^{jn}$ with each

Received by the editors October 22, 1996 and in revised form February 27, 1997.
AMS 1991 Subject Classification: 13D40, 13J10.
Key words and phrases: Hilbert-Kunz function, F-object, formal difference.

$\Delta^{(j)}(n)$ eventually periodic.

When

$$\mathcal{O} = \mathbb{Z}/(p)[[X_1, X_2, \ldots, X_t]]/(X_1^{d_1} + X_2^{d_2} + \cdots + X_t^{d_t}) \tag{1}$$

where the d_i's are positive integers, by using representation ring as a tool, Han and Monsky [4] proved the following theorem (Theorem 5.7 in [4]):

Theorem 1.1.

$$e_n(\mathcal{O}) = cp^{(t-1)n} + \Delta(n)$$

where c is a rational number, and there exist positive integer ω and integer $l \geq 0$ such that

$$\Delta(n + \omega) = l\Delta(n)$$

for $n \gg 0$.

Furthermore, the integer l has the following properties:

(1) *For odd p, if $t \geq 3$ then $l \leq p^{\omega(t-3)}$,and if $t < 3$ then $l \leq 1$.*

(2) *If $p = 2$ then $l \leq 1$.*

Han and Monsky deduced some multiplication formulae of the representation ring to prove certain functional equations for $D_F(k_1, \ldots, k_t)$ where $F := \mathbb{Z}/(p)$, and $D_F(k_1, \ldots, k_t)$ is the $\mathbb{Z}/(p)$-dimension of

$$\mathbb{Z}/(p)[[X_1, X_2, \ldots, X_t]]/(X_1^{k_1}, X_w^{k_2}, \ldots, X_t^{k_t}, X_1 + X_2 + \cdots + X_t),$$

and then used the functional equations for $D_F(k_1, \ldots, k_t)$ to describe $e_n(\mathcal{O})$. They also made use of computer to develop computations. But the computations and their proofs are rather complicated.

In this article, we first deduce four more multiplication formulae (Propositions 3.3-3.6), and then apply these useful formulae to Hilber-Kunz function of (1) and give a new proof of Han-Monsky's theorem (Cf. §5). In addition, we also obtain another explicit algorithm to evaluate c, l and $\Delta(n)$ for any given prime p and $d_i \geq 1$ (Cf. §4). We have a program (Cf.

[1]) written in Maple that can evaluate c, l and the periodic function $\Delta(n)$ for any given prime p and positive integers $d_i \geq 2$.

When $\mathcal{O} = \mathbb{Z}/(p)[X_1, X_2, \ldots, X_s]/I$ where I is a monomial ideal, Conca [2] showed that there exists a polynomial $f(y) \in \mathbb{Z}[y]$ of degree the dimension of $\mathcal{O}$ and leading coefficient the multiplicity of $\mathcal{O}$ such that $e_n(\mathcal{O}) = f(p^n)$ for large n (Cf. Theorem 2.1 in [2]).

If $\mathcal{O} = \mathbb{Z}/(p)[X_1, \ldots, X_s, Y_1, \ldots, Y_t]/I$, where I is a principal ideal generated by a homogeneous form

$$X_1^{d_1} \cdots X_s^{d_s} + Y_1^{e_1} \cdots Y_t^{e_t}, \tag{2}$$

in the same paper [2], Conca use the Groebner basis to show that

$$e_n(\mathcal{O}) = cp^{(s+t-1)n} + c_{s+t-2}(\epsilon)p^{(s+t-2)n} + c_{s+t-3}(\epsilon)p^{(s+t-3)n} + \cdots + c_0(\epsilon)$$

for large n where c is a rational and $c_i(z) \in \mathbb{Q}[z]$ are polynomials, and ϵ is the residue class of p^n modulo the maximum u of $d_1, d_2, \ldots, d_s, e_1, e_2, \ldots, e_t$. Furthermore

$$c = \sum_{i=1}^{s}\sum_{j=1}^{t}(-1)^{i+j}s_i t_j \frac{ij}{(i+j-1)u^{i+j-1}}$$

where s_i and t_j are the i-th and the j-th elementary symmetric polynomials in d_k's and e_k's, respectively (Cf. Theorem 3.1 in [2]).

In this article, we also use the representation ring as a tool to determine the Hilbert-Kunz function of the binomial hypersurface defined by (2), here (2) is not necessarily homogeneous (Cf. §6).

We have the following theorem:

Theorem 1.2. *Let*

$$\mathcal{O} = \mathbb{Z}/(p)[[X_1, \ldots, X_s, Y_1, \ldots, Y_t]]/(X_1^{d_1} \cdots X_s^{d_s} + Y_1^{e_1} \cdots Y_t^{e_t}).$$

Then the Hilbert-Kunz function of $\mathcal{O}$ is

$$n \mapsto cp^{(s+t-1)n} + \Delta_{s+t-2}(n)p^{(s+t-2)n} + \Delta_{s+t-3}(n)p^{(s+t-3)n} + \cdots + \Delta_0(n)$$

where c is a rational and Δ_i are eventually periodic functions. Moreover, if d_1 is the maximum of $d_1, \ldots, d_s$, $e_1, \ldots e_t$, then

$$c := d_1 \prod_{j=2}^{s}(1 - d_j/d_1)\left[1 - \prod_{i=1}^{t}(1 - e_i/d_1)\right] + \sum_{j=2}^{s}\sum_{l=1}^{t}\left[\frac{j(j-1)}{(j+l-1)d_1^{j+l-1}}(-1)^{j+l-1}s_j t_l\right]$$

where s_j and t_l are the j-th and the l-th elementary symmetric polynomials in d_i's and e_i's, respectively.

Basically, Theorem 1.2 is the same as Theorem 3.1 in [2].

2. Preliminary. From now on, F is a field with $\mathrm{char}F = p > 0$. We introduce the F-objects and some of their properties in this section. They play the central role in this article. An F-object M is a finitely generated $F[T]$-module such that $T^i M = 0$ for some positive integer i.

Let M and N be two F-objects. Then $M \oplus N$ and $M \underset{F}{\otimes} N$ are F-bojects with $T(m \oplus n) := Tm \oplus Tn$ and $T(m \otimes n) := (Tm \otimes n) + (m \otimes T_n)$. We define an equivalence relation on the set of ordered pairs of F-objects $\{(M, N) : M, N$ are F-objects$\}$ as follows:

$$(M_1, N_1) \sim (M_2, N_2) \Longleftrightarrow M_1 \oplus N_2 \text{ is isomorphic to } M_2 \oplus N_1 \text{ as } F[T] - \text{modules.}$$

The equivalence class $[(M, N)]$, denoted by $M - N$, is called the formal difference of M and N. Let Γ be the set of the formal differences of F-objects. On Γ we define two binary operations:

$$(M_1 - N) + (M_2 - N_2) := (M_1 \oplus M_2) - (N_1 \oplus N_2),$$

$$(M_1 - N_1) \cdot (M_2 - N_2) := ((M_1 \underset{F}{\otimes} M_2) \oplus (N_1 \underset{F}{\otimes} N_2)) - ((M_1 \underset{F}{\otimes} N_2) \oplus (N_1 \underset{F}{\otimes} M_2)).$$

The set Γ forms a commutative ring under these two binary operations, which is called the representation ring. Note that we can decompose any

F-object into a direct sum of $F[T]/(T^i)$'s. Let

$$\delta_i := F[T]/(T^i) - 0.$$

Then Γ is a free-$\mathbb{Z}$-module with basis $\{\delta_i\}_{i=1}^{\infty}$. We have a map from the set of F-objects into Γ:

$$\psi : M \mapsto M - 0$$

with $\psi(M \oplus N) = \psi(M) + \psi(N)$ and $\psi(M \otimes N) = \psi(M) \cdot \psi(N)$. Now we consider the Hilbert-Kunz function of

$$R_{d_1,\ldots,d_t} := F[[x_1, x_2, \ldots, x_t]]/(x_1^{d_1} + x_2^{d_2} + \cdots + x_t^{d_t}). \tag{3}$$

For the case of $t = 1$, we define a T-action on $M(n) := F[x]/(x^{p^n})$ by $Tf := x^{d_1} f$. Then $M(n)$ becomes an F-object. It is easy to check that

$$M(n) \simeq [F[T]/(T^a)]^{d-r} \oplus [F[T]/(T^{a+1})]^r$$

where $p^n = da + r$ with $0 \leq r < d$. Then we have

$$\psi(M(n)) = (d - r)\delta_a + r\delta_{a+1}. \tag{4}$$

For $t \geq 2$, let $M_k(n) := F[x_k]/(x_k^{p^n})$, and let the T-action on $M_k(n)$ be $Tf := x_k^{d_k} f$. Then $M(n) := \otimes_{k=1}^{t} M_k(n)$ can be identified with

$$F[x_1, \ldots, x_t]/(x_1^{p^n}, \ldots, x_t^{p^n})$$

where the nilpotent T-action on $F[x_1, \ldots, x_t]/(x_1^{p^n}, \ldots, x_t^{p^n})$ is $Tf := (x_1^{d_1} + \cdots + x_t^{d_t})f$. Denote the Hilbert-Kunz function of $R_{d_1,\ldots,d_t}$ by $H_{(d_1,\ldots,d_t;p)}$. Then $H_{(d_1,\ldots,d_t;p)}(n)$ is just the F-dimension of $M(n)/TM(n)$. As an F-object, $M(n)$ can be decomposed into a direct sum of $F[T]/(T^i)$'s, thus,

$$M(n) \simeq \oplus_i [F[T]/(T^i)]^{\gamma_i}.$$

Then

$$H_{(d_1,\ldots,d_t;p)}(n) = \dim_F M(n)/TM(n) = \sum_i \gamma_i.$$

From Eq(4), we can evaluate $H_{(d_1,\ldots,d_t;p)}(n)$by decomposing

$$\psi(M(n)) = \prod_{k=1}^{t} \psi(M_k(n)) = \prod_{k=1}^{t} [(d_k - r_k)\delta_{a_k} + r_k\delta_{a_k+1}], \tag{5}$$

where $p^n = d_k a_k + r_k$ with $0 \leq r_k < d_k$, into a sum of δ_i's, then counting the number of summands in the decomposition. Thus, we define the map $D_F : \Gamma \mapsto \mathbb{Z}$ as follows:

For any F-objects M and N, if $M \simeq \oplus_i [F[T]/(T^i)]^{a_i}$ and $N \simeq \oplus_i [F[T]/(t^i)]^{b_i}$ then

$$D_F(M - N) := \sum_i (a_i - b_i).$$

It is easy to check that D_F is a $\mathbb{Z}$-homomorphism from Γ to $\mathbb{Z}$. For the detail of this preliminary we refer to [4].

3. Multiplication formulae. In this section, we shall give some multiplication formulae in Γ. Throughout this section, q will always denote a power of p. For convenience, we give another basis for the free $\mathbb{Z}$-module Γ (Cf. [4]),

$$\lambda_i = \begin{cases} \delta_1 & \text{if } i = 0 \\ (-1)^i(\delta_{i+1} - \delta_i) & \text{if } i \geq 1. \end{cases}$$

Note that $D_F(\lambda_0) = 1$, $D_F(\lambda_j) = 0$, and $\delta_j = \sum_{i=0}^{j-1}(-1)^i\lambda_i$ for all $j \geq 1$. If $\sum \gamma_j\delta_j = \sum \alpha_j\lambda_j$, we have $\sum \gamma_j = \alpha_0$.

In [4], there are some formulae for the multiplications of δ_i's and λ_j. We list them as follows:

Proposition 3.1 ([4], Lemma 3.3, Theorem 3.4) *For $0 \leq s \leq q$ and $1 \leq i < p$, we have*

$$\delta_{iq}\delta_s = s\delta_{iq}, \tag{6}$$

$$\delta_{iq+1}\delta_s = (s-1)\delta_{iq} + \delta_{iq+s}, \tag{7}$$

$$\delta_{iq-1}\delta_s = (s-1)\delta_{iq} + \delta_{iq-s}, \tag{8}$$

and, for $0 \leq s < q$, *we have*

$$\lambda_{iq}\lambda_s = \lambda_{iq+s}, \tag{9}$$

$$\lambda_{iq-1}\lambda_s = \lambda_{iq-1-s}. \tag{10}$$

By Eq(6) to Eq(10), the following formulae are immediate.

For $s < q$, $i \geq 1$,

$$(-1)^s\lambda_s\delta_{iq} = \delta_{iq}, \tag{11}$$

$$(-1)^{iq}\lambda_{iq}\delta_s + \delta_{iq} = \delta_{iq+s}, \tag{12}$$

$$(-1)^{iq-1}\lambda_{iq-1}\delta_s - \delta_{iq} = -\delta_{iq-s}. \tag{13}$$

Note here that Eq(12) and Eq(13) are valid if $s = q$.

Proposition 3.2 ([4], Theorem 2.5)

$$\lambda_i\lambda_j = \sum_{k=|i-j|}^{\min(i+j,2p-2-i-j)} \lambda_k \tag{14}$$

where $0 \leq i, j < p$.

Lemma 3.1 ([4], Lemma 3.9) *If* $1 \leq j \leq p-2$ *then*

$$\delta_{q+1}\delta_{jq+1} = \delta_{(j+1)q+1} + \delta_{(j-1)q+1} + \delta_{(j+1)q-1} + (q-2)\delta_{jq}. \tag{15}$$

If $1 \leq j \leq p-1$ *then*

$$\delta_{q+1}\delta_{jq} = \delta_{(j+1)q} + \delta_{(j-1)q} + (q-1)\delta_{jq}. \tag{16}$$

Lemma 3.2 ([4], Theorem 3.11) *Suppose* $0 \leq s < q$ *and* $1 \leq i \leq p-2$. *Then*

$$\lambda_q \lambda_{iq+s} = \lambda_{(i+1)q+s} + \lambda_{(i-1)q+s} + \lambda_{(i+1)q-1-s} \tag{17}$$

and

$$\lambda_q \lambda_{(p-1)q} = \lambda_{(p-1)q}. \tag{18}$$

Note that Lemma 3.1 and Lemma 3.2 are also valid while $q = 1$. By Eq(10), we have

$$\lambda_{q-1}^2 = \lambda_0. \tag{19}$$

Let

$$H(i) := \begin{cases} 0 & \text{if } i < 0 \\ 1 & \text{if } i \geq 0. \end{cases}$$

Now we shall prove the following propositions 3.3 – 3.6. They are very useful in evaluating the Hilbert-Kunz functions.

Proposition 3.3 *If* $1 \leq i,\ j \leq p$, *then*

$$\delta_i \delta_j = \delta_{(|i-j|+1)} + \delta_{(|i-j|+3)} + \ldots + \delta_b + (i+j-p)H(i+j-p)\delta_p \tag{20}$$

where $b = \min(i+j-1, 2p-1-i-j)$.

Proof. If $i+j \leq p$, the proposition is just Theorem 2.15 of [4]. Suppose $i+j > p$. Then by Eq(6), Eq(8) and Eq(19),

$$\begin{aligned} &\delta_i \delta_j \\ =&\lambda_{p-1}^2 \delta_i \delta_j \\ =&(\delta_p - \delta_{p-1})\delta_i(\delta_p - \delta_{p-1})\delta_j \\ =&(\delta_{p-i} - \delta_p)(\delta_{p-j} - \delta_p) \\ =&\delta_{p-i}\delta_{p-j} + (i+j-p)\delta_p. \end{aligned}$$

Since $(p-i)+(p-j) \leq p$, using Theorem 2.15 of [4] again to the product $\delta_{p-i}\delta_{p-j}$, we complete the proof.

Proposition 3.4 *If* $1 \leq i,\ j \leq p$ *and* $\delta_i \delta_j = \sum_{k=1}^{p} \gamma_k \delta_k$ *then* $\delta_{iq}\delta_{jq} = q \sum_{k=1}^{p} \gamma_k \delta_{kq}$ *for all* $q = 1, p, p^2, \ldots$

Proof. We take $i \geq j$ and use induction on j. For $j = 0$ and $j = 1$, the proposition is true by Eq(6). For $2 \leq j \leq p$, by Eq(16), we have

$$\delta_{jq} = \delta_{q+1}\delta_{(j-1)q} - (q-1)\delta_{(j-1)q} - \delta_{(j-2)q}$$

for $q = 1, p, p^2, \ldots$. By inductive hypothesis, we suppose that

$$\delta_{iq}\delta_{(j-1)q} = q\sum_k \gamma'_k \delta_{kq}$$

and

$$\delta_{iq}\delta_{(j-2)q} = q\sum_k \gamma''_k \delta_{kq}.$$

Using Lemma 3.1, we then have

$$\begin{aligned}
&\delta_{iq}\delta_{jq} \\
=&\delta_{iq}\delta_{(j-1)q}\delta_{q+1} - (q-1)\delta_{iq}\delta_{(j-1)q} - \delta_{iq}\delta_{(j-2)q} \\
=&q\delta_{q+1}\sum_{k=1}^{p}\gamma'_k\delta_{kq} - q(q-1)\sum_{k=1}^{p}\gamma'_k\delta_{kq} - \delta_{iq}\delta_{(j-2)q} \\
=&q(q+1)\gamma'_p\delta_{pq} + q\sum_{k=1}^{p-1}\gamma'_k(\delta_{(k+1)q} + \delta_{(k-1)q} + (q-1)\delta_{kq}) \\
&- q(q-1)\sum_{k=1}^{p}\gamma'_k\delta_{kq} - \delta_{iq}\delta_{(j-2)q} \\
=&2q\gamma'_p\delta_{pq} + q\sum_{k=1}^{p-1}\gamma'_k(\delta_{(k+1)q} + \delta_{(k-1)q}) - q\sum_k \gamma''_k\delta_{kq} \\
=&q\left[2\gamma'_p\delta_{pq} + \sum_{k=1}^{p-1}\gamma'_k(\delta_{(k+1)q} + \delta_{(k-1)q}) - \sum_k \gamma''_k\delta_{kq}\right].
\end{aligned}$$

Now by inductive hypothesis the coefficients γ'_k's and γ''_k's are invariant while q varies in $\{1, p, p^2, \ldots\}$, i.e. the recursive formula list here is valid for all $q = p^n$ including $q = 1$.

Corollary 1.

(21) $\delta_{iq}\delta_{jq} = q(\delta_{(|i-j|+1)q} + \delta_{(|i-j|+3)q} + \cdots + \delta_{bq} + (i+j-p)H(i+j-p)\delta_{pq})$.

Proposition 3.5 *For $0 \le i \le p-1$ and $1 \le j \le p$, we have*

$$(22)\quad (-1)^{iq}\lambda_{iq}\delta_{jq} = H(j-i)\delta_{|i-j|q} - \delta_{(|i-j|+1)q} + \cdots \pm \delta_{cq} + H(i+j-p)\delta_{pq}$$

where $c := \min(i+j, 2p-1-i-j)$.

Proof. We do this by induction on i. The case of $i = 0$ is clear. For $i = 1$, by Eq(16), we have

$$\delta_{q+1}\delta_{jq} = \delta_{(j+1)q} + \delta_{(j-1)q} + (q-1)\delta_{jq} = \delta_{(j+1)q} - \delta_{jq} + \delta_{(j-1)q} + q\delta_{jq}.$$

By Eq(6)

$$\delta_{q+1}\delta_{jq} - q\delta_{jq} = (\delta_{q+1} - \delta_q)\delta_{jq}.$$

Then

$$(-1)^q\lambda_q\delta_{jq} = \delta_{(j+1)q} - \delta_{jq} + \delta_{(j-1)q}.$$

For $i \ge 2$, by Eq(15) and Eq(16)

$$\begin{aligned}&\delta_{q+1}(\delta_{(i-1)q+1} - \delta_{(i-1)q})\\ =&\delta_{iq+1} - \delta_{iq} + \delta_{(i-2)q+1} - \delta_{(i-2)q} + \delta_{(i-1)q+q-1} - \delta_{(i-1)q}.\end{aligned}$$

We can write

$$\begin{aligned}&(-1)^{iq}\lambda_{iq}\\ =&\delta_{iq+1} - \delta_{iq}\\ =&\delta_{q+1}(\delta_{(i-1)q+1} - \delta_{(i-1)q}) - \delta_{(i-2)q+1} + \delta_{(i-2)q} - \delta_{(i-1)q+q-1} + \delta_{(i-1)q}\\ =&\delta_{q+1}(-1)^{(i-1)q}\lambda_{(i-1)q} - (-1)^{(i-2)q}\lambda_{(i-2)q}\\ &- [\delta_{q-1}\delta_{(i-1)q+1} - (q-2)\delta_{(i-1)q}] + \delta_{(i-1)q}\\ =&\delta_{q+1}(-1)^{(i-1)q}\lambda_{(i-1)q} - (-1)^{(i-2)q}\lambda_{(i-2)q}\\ &- \delta_{q-1}\delta_{(i-1)q+1} + (q-1)\delta_{(i-1)q}.\end{aligned}$$

Then we have

$$\begin{aligned}&(-1)^{iq}\lambda_{iq}\delta_{jq}\\ =&[\delta_{q+1}(-1)^{(i-1)q}\lambda_{(i-1)q} - (-1)^{(i-2)q}\lambda_{(i-2)q}\\ &- \delta_{q-1}\delta_{(i-1)q+1} + (q-1)\delta_{(i-1)q}]\delta_{jq}\end{aligned}$$

$$
\begin{aligned}
&=\delta_{q+1}(-1)^{(i-1)q}\lambda_{(i-1)q}\delta_{jq} - (-1)^{(i-2)q}\lambda_{(i-2)q}\delta_{jq} \\
&\quad - (q-1)\delta_{(i-1)q+1}\delta_{jq} + (q-1)\delta_{(i-1)q}\delta_{jq} \\
&=\delta_{q+1}(-1)^{(i-1)q}\lambda_{(i-1)q}\delta_{jq} - (-1)^{(i-2)q}\lambda_{(i-2)q}\delta_{jq} \\
&\quad - \delta_q(-1)^{(i-1)q}\lambda_{(i-1)q}\delta_{jq} + (-1)^{(i-1)q}\lambda_{(i-1)q}\delta_{jq} \\
&= -(-1)^{(i-2)q}\lambda_{(i-2)q}\delta_{jq} + (-1)^q\lambda_q(-1)^{(i-1)q}\lambda_{(i-1)q}\delta_{jq} \\
&\quad + (-1)^{(i-1)q}\lambda_{(i-1)q}\delta_{jq}.
\end{aligned}
$$

By inductive hypothesis, we may take

$$(-1)^{(i-2)q}\lambda_{(i-2)q}\delta_{jq} = \sum_{k=1}^{p}\zeta'_k\delta_{kq},$$

$$(-1)^{(i-1)q}\lambda_{(i-1)q}\delta_{jq} = \sum_{k=1}^{p}\zeta''_k\delta_{kq}$$

where ζ'_k's and ζ''_k's are constant integers while q varies in $\{1, p, p^2, \ldots\}$. Then

$$(-1)^{iq}\lambda_{iq}\delta_{jq} = \sum_{k=1}^{p}\zeta_k\delta_{kq}$$

where ζ_k's are also constant integers while q varies in $\{1, p, p^2, \ldots\}$. Thus if we can prove Eq(22) for $q = 1$, i.e.

$$(23)\quad (\delta_{i+1} - \delta_i)\delta_j = H(j-i)\delta_{|i-j|} - \delta_{(|i-j|+1)} + \cdots \pm \delta_c + H(i+j-p)\delta_p,$$

then we get the proposition. But Eq(23) can be easily checked by using Proposition 3.2. Notice that there are four cases here to be considered.

Proposition 3.6 *For $0 \le i, j \le p-1$, we have*

$$(24)\qquad \lambda_{iq}\lambda_{jq} = \sum_{k=0}^{c'}\lambda_{(|i-j|+2k)q} + \sum_{k=1}^{c'}\lambda_{(|i-j|+2k)q-1}$$

where $c' := \min(i, j, p-1-i, p-1-j)$.

Proof. By Eq(18), the proposition is clear when $p = 2$. Now suppose that $p \neq 2$. By Eq(14), Eq(24) is valid for $q = 1$. Let $i \ge j$. We prove this

by induction on j. The case of $j = 0$ is trivial, and the case of $j = 1$ is immediate by Lemma 3.2. For $j \geq 2$, by Eq(17), we have

$$\lambda_{jq} = \lambda_q \lambda_{(j-1)q} - \lambda_{(j-2)q} - \lambda_{(j-1)q+q-1}.$$

Then

$$\begin{aligned}\lambda_{iq}\lambda_{jq} &= \lambda_{iq}\lambda_q\lambda_{(j-1)q} - \lambda_{iq}\lambda_{(j-2)q} - \lambda_{iq}\lambda_{(j-1)q}\lambda_{q-1} \\ &= \lambda_{iq}\lambda_{(j-1)q}(\lambda_q - \lambda_{q-1}) - \lambda_{iq}\lambda_{(j-2)q}.\end{aligned}$$

Let $c := \min(j-1, p-1-i)$, $d := \min(j-2, p-1-i)$, and $\delta_{a,b}$ the Kronecker symbol. From Eq(9), Eq(10), Lemma 3.2 and by inductive hypothesis, we have

$$\begin{aligned}&\lambda_{iq}\lambda_{jq} \\ =&\lambda_q(\lambda_{(i-j+1)q} + \lambda_{(i-j+3)q-1} + \lambda_{(i-j+3)q} \\ &+ \cdots + \lambda_{(i-j+1+2c)q-1} + \lambda_{(i-j+1+2c)q}) \\ &- \lambda_{q-1}(\lambda_{(i-j+1)q} + \lambda_{(i-j+3)q-1} + \lambda_{(i-j+3)q} \\ &+ \cdots + \lambda_{(i-j+1+2c)q-1} + \lambda_{(i-j+1+2c)q}) \\ &- \lambda_{(i-j+2)q} + \lambda_{(i-j+4)q-1} + \lambda_{(i-j+4)q} \\ &+ \cdots + \lambda_{(i-j+2+2d)q-1} + \lambda_{(i-j+2+2d)q}) \\ =&[\lambda_{(i-j)q} + \lambda_{(i-j+2)q-1} + \lambda_{(i-j+2)q}] \\ &+ [\lambda_{(i-j+2)q-1} + \lambda_{(i-j+2)q} + \lambda_{(i-j+4)q-1}] \\ &+ [\lambda_{(i-j+2)q} + \lambda_{(i-j+4)q-1} + \lambda_{(i-j+4)q}] \\ &+ \cdots + [\lambda_{(i-j+2c)q-1} + \lambda_{(i-j+2c)q} + \lambda_{(i-j+2+2c)q-1}] \\ &+ [\lambda_{(i-j+2c)q} + (1 - \delta_{i+j,p})(\lambda_{(i-j+2c+2)q-1} + \lambda_{(i-j+2c+2)q})] \\ &- (\lambda_{(i-j+2)q-1} + \lambda_{(i-j+2)q} + \lambda_{(i-j+4)q-1} \\ &+ \cdots + \lambda_{(i-j+2c)q} + \lambda_{(i-j+2+2c)q-1}) \\ &- (\lambda_{(i-j+2)q} + \lambda_{(i-j+4)q-1} + \lambda_{(i-j+4)q} \\ &+ \cdots + \lambda_{(i-j+2+2d)q-1} + \lambda_{(i-j+2+2d)q}).\end{aligned}$$

If $p - 1 - i \geq j$ then $c = j - 1, d = j - 2$, and $p - i - j \geq 1$. We have

$$\lambda_{iq}\lambda_{jq} = \lambda_{(i-j)q} + \lambda_{(i-j+2)q-1} + \lambda_{(i-j+2)q} + \cdots + \lambda_{(i+j)q-1} + \lambda_{(i+j)q}.$$

If $p-1-i = j-1$ then $c = p-1-i$, $d = p-2-i$, $p = i+j$. We have

$$\lambda_{iq}\lambda_{jq} = \lambda_{(i-j)q}+\lambda_{(i-j+2)q-1}+\lambda_{(i-j+2)q}+\cdots+\lambda_{(2p-2-i-j)q-1}+\lambda_{(2p-2-i-j)q}.$$

If $p-1-i \leq j-2$ then $c = d = p-1-i$, and $p-i-j \leq -1$. We have

$$\lambda_{iq}\lambda_{jq} = \lambda_{(i-j)q}+\lambda_{(i-j+2)q-1}+\lambda_{(i-j+2)q}+\cdots+\lambda_{(2p-2-i-j)q-1}+\lambda_{(2p-2-i-j)q}.$$

Let $Q \in \Gamma$ and $Q = \sum \alpha_i\lambda_i$. We call α_i the coefficient of λ_i in Q. We say that λ_i appears in Q if the coefficient of λ_i in Q is not zero.

Let $a = iq+j, b = kq+l$ where $0 \leq i,k < p$ and $0 \leq j,l < q$. We can now have an algorithm to decompose $\delta_a\delta_b$ (resp. $\lambda_a\lambda_b$) into a sum of δ_n's (resp. λ_i) by the following recursive formulae:

$$\begin{aligned}\delta_a\delta_b &= [(-1)^{iq}\lambda_{iq}\delta_k + \delta_{iq}][(-1)^{jq}\lambda_{jq}\delta_l + \delta_{jq}]\\ &= [(-1)^{(i+j)q}\lambda_{iq}\lambda_{jq}](\delta_k\delta_l) + k(-1)^{iq}\lambda_{iq}\delta_{jq} + l(-1)^{jq}\lambda_{jq}\delta_{iq} + \delta_{iq}\delta_{jq},\end{aligned}$$

$$\lambda_a\lambda_b = (\lambda_{iq}\lambda_{kq})(\lambda_j\lambda_l)$$

and by the formulae list in this section.

4. An algorithm. Throughout this section, we fix p, d_k's and n. Now we return to the discussion in §2. Eq(5) can be rewritten as

$$\psi(M(n)) = \prod_{k=1}^{t}((-1)^{a_k}r_k\lambda_{a_k} + d_k\delta_{a_k}), \tag{25}$$

where $p^n = a_kd_k + r_k$ with $0 \leq r_k < a_k$. For nonnegative integers $u_1, \ldots, u_t$, we define

$$\Xi(u_1, \ldots, u_t) := \prod_{k=1}^{t}((-1)^{u_k}r_k\lambda_{u_k} + d_k\delta_{u_k}). \tag{26}$$

If we write $1/d_k$ into p-adic form

$$\frac{1}{d_k} := b_k(0) + b_k(1)p^{-1} + b_k(2)p^{-2} + \cdots \tag{27}$$

we will have

$$a_k = b_k(0)p^n + b_k(1)p^{n-1} + \cdots + b_k(n).$$

Let $c_k(\mu) := \sum_{i=\mu}^{n} b_k(i)p^{n-i}$ for $0 \le \mu \le n$. Then $c_k(\mu) = b_k(\mu)p^{n-\mu} + c_k(\mu+1)$. Since $c_k(\mu) < p^{n-\mu+1}$, we have

$$\Xi(c_1(\mu), \ldots, c_t(\mu)) = \sum_{i=0}^{p^{n-\mu+1}-1} \beta_i(\mu)\lambda_i \tag{28}$$

for some integers $\beta_i(\mu)'s$. Note that

$$D_F(\Xi(c_1(\mu), \ldots, c_t(\mu))) = \beta_0(\mu). \tag{29}$$

For the rest of this section, we denote $b_k := b_k(\mu)$, $s_k := c_k(\mu+1)$ and $q := p^{n-\mu}$. Then, by Eq(9) and Eq(12),

$$\begin{aligned}
&\Xi(c_1(\mu), \ldots, c_t(\mu)) \\
&= \prod_{k=1}^{t} \left[r_k(-1)^{b_k q}\lambda_{b_k q}(-1)^{s_k}\lambda_{s_k} + (-1)^{b_k q} d_k \lambda_{b_k q}\delta_{s_k} + d_k\delta_{b_k q}\right] \\
&= \prod_{k=1}^{t} \left\{(-1)^{b_k q}\lambda_{b_k q}[r_k(-1)^{s_k}\lambda_{s_k} + d_k\delta_{s_k}] + d_k\delta_{b_k q}\right\} \\
&= \prod_{k=1}^{t} \left[(-1)^{b_k q}\lambda_{b_k q}\right]\Xi(s_1, \ldots, s_t) + Q(n, \mu)
\end{aligned}$$

for some $Q(n,\mu) \in \Gamma$. We can easily check that

$$Q(n,\mu) = \sum_{\phi \ne S \subseteq X} \prod_{k \notin S} \left\{(-1)^{b_k q}\lambda_{b_k q}[r_k(-1)^{s_k}\lambda_{s_k} + d_k\delta_{s_k}]\right\} \prod_{k \in S} d_k\delta_{b_k q}$$

with $X := \{1, 2, \ldots, t\}$. From Eq(6) and E(11) we have

$$Q(n,\mu) = \sum_{\phi \ne S \subseteq X} \prod_{k \notin S} \left\{(r_k + d_k s_k)(-1)^{b_k q}\lambda_{b_k q}\right\} \prod_{k \in S} d_k\delta_{b_k q}.$$

Note that $r_k + d_k s_k$ is the residue of p^n divided by $d_k q$; we will denote the residue by $(p^n \bmod d_k q)$.

$$\begin{aligned} Q(n,\mu) &= \sum_{\phi\neq S\subseteq X}\prod_{k\notin S}\{(p^n \bmod d_k q)(-1)^{b_{kq}}\lambda_{b_{kq}}\}\prod_{k\in S} d_k\delta_{b_{kq}} \\ &= \sum_{\phi\neq S\subseteq X}\prod_{k\notin S}\{q(p^\mu \bmod d_k)(-1)^{b_{kq}}\lambda_{b_{kq}}\}\prod_{k\in S} d_k\delta_{b_{kq}} \\ &= \sum_{\phi\neq S\subseteq X} q^{t-|S|}\prod_{k\notin S}\{(p^\mu \bmod d_k)(-1)^{b_{kq}}\lambda_{b_{kq}}\}\prod_{k\in S} d_k\delta_{b_{kq}}. \end{aligned}$$

Let

$$\prod_{k\notin S}\{(p^\mu \bmod d_k)(-1)^{b_k}\lambda_{b_k}\}\prod_{k\in S} d_k\delta_{b_k} = \sum_{i=1}^{p}\eta_i(\mu,S)\delta_i.$$

By Propositions 3.4 and 3.5, we have

$$\begin{aligned} & q^{t-|S|}\prod_{k\notin S}\{(p^\mu \bmod d_k)(-1)^{b_{kq}}\lambda_{b_{kq}}\}\prod_{k\in S} d_k\delta_{b_{kq}} \\ =& q^{t-|S|}\sum_{i=1}^{p} q^{|S|-1}\eta_i(\mu,S)\delta_{iq} \\ =& q^{t-1}\sum_{i=1}^{p}\eta_i(\mu,S)\delta_{iq}. \end{aligned} \tag{30}$$

In fact, for any μ, Eq(30) is true for all $q \in \{1, p, p^2, ..\}$. Let

$$\sum_{\phi\neq S\subseteq X}\prod_{k\notin S}\{(p^\mu \bmod d_k)(-1)^{b_k}\lambda_{b_k}\}\prod_{k\in S} d_k\delta_{b_k} = \sum_{i=1}^{p}\gamma_i(\mu)\delta_i. \tag{31}$$

Then we have

$$Q(n,\mu) = q^{t-1}\sum_{i=1}^{p}\gamma_i(\mu)\delta_{iq}.$$

For formulating a program to calculate $\gamma_i(\mu)$'s, using the following Eq(32) is better than using Eq(31).

$$\begin{aligned} & \prod_{k=1}^{t}\left[(p^\mu \bmod d_k)(-1)^{b_k}\lambda_{b_k} + d_k\delta_{b_k}\right] - \prod_{k=1}^{t}\left[(p^\mu \bmod d_k)(-1)^{b_k}\lambda_{b_k}\right] \\ =& \sum_{i=1}^{p}\gamma_i(\mu)\delta_i. \end{aligned} \tag{32}$$

b_k's are independent of n, so are $\gamma_i(\mu)$'s. Thus, for given p and d_k's, the $\gamma_i(\mu)$'s are functions of μ only. Especially $\gamma_i(\mu)$'s are independent of n. Now

we get

$$\Xi(c_1(\mu),\ldots,c_t(\mu)) = \prod_{k=1}^{t}[(-1)^{b_k(\mu)q}\lambda_{b_k(\mu)q}]\Xi(c_1(\mu+1),..,c_t(\mu+1)) + q^{(t-1)}\sum_{i=1}^{p}\gamma_i(\mu)\delta_{iq}.$$

Define the following symbols:

$$\Lambda(n,\mu) := \prod_{k=1}^{t}(-1)^{b_k(\mu)q}\lambda_{b_k(\mu)q}, \tag{33}$$

$$Z(n,\mu) := \sum_{i=1}^{p}\gamma_i(\mu)\delta_{iq}. \tag{34}$$

Then

(35)

$$\Xi(c_1(\mu),\ldots,c_t(\mu)) = \Lambda(n,\mu)\Xi(c_1(\mu+1),\ldots,c_t(\mu+1)) + p^{(n-\mu)(t-1)}Z(n,\mu).$$

From Eq(9), Eq(10) and Eq(24), we can easily check the following proposition.

Proposition 4.1 *Let p be an odd prime, and $q = 1, p, p^2, \ldots$ We have*

$$\Lambda(n,\mu) = \alpha_0(\mu)\lambda_0 + \alpha_{2p-1}(\mu)\lambda_{2q-1} + \alpha_{2p}(\mu)\lambda_{2q} + \alpha_{4p-1}(\mu)\lambda_{4q-1} + \cdots + \alpha_{(p-1)p-1}(\mu)\lambda_{(p-1)q-1} + \alpha_{(p-1)p}(\mu)\lambda_{(p-1)q}$$

if $\sum_k b_k(\mu)$ *is even, and*

$$\Lambda(n,\mu) = \alpha_{p-1}(\mu)\lambda_{q-1} + \alpha_p(\mu)\lambda_q + \alpha_{3p-1}(\mu)\lambda_{3q-1} + \alpha_{3p}(\mu)\lambda_{3q} + \cdots + \alpha_{(p-2)p}(\mu)\lambda_{(p-2)q} + \alpha_{p^2-1}(\mu)\lambda_{pq-1}$$

if $\sum_k b_k(\mu)$ *is odd.*

There are some properties about the coefficients $\alpha_i(\mu)$.

Proposition 4.2 *For odd prime p and $t \geq 2$, we have*

$$|\alpha_i(\mu)| \leq p^{t-2}$$

for all i.

Proof. While we write

$$\lambda_{kq}(\alpha_{p-1}\lambda_{q-1} + \alpha_p\lambda_q + \alpha_{3p-1}\lambda_{3q-1} + \alpha_{3p}\lambda_{3q} + \cdots + \alpha_{p^2-1}\lambda_{pq-1}) = \sum_j \alpha'_j\lambda_j$$

or

$$\lambda_{kq}(\alpha_0\lambda_0 + \alpha_{2p-1}\lambda_{2q-1} + \alpha_{2p}\lambda_{2q} + \alpha_{4p-1}\lambda_{4q-1} + \cdots + \alpha_{(p-1)p}\lambda_{(p-1)q}) = \sum_j \alpha'_j\lambda_j$$

then, by Eq(10) and Eq(24), we shall have

$$|\alpha'_i| \le \sum_j |a_j| \le p \max_j\{\alpha_j\}.$$

Thus it is sufficient to show the proposition for $t = 2$, but Eq(24) implies this case.

Corollary 2. *If $t \ge 3$ and $i \in I := \{0, p-2, p^2-p, p^2-1\}$, we have*

$$|\alpha_i(\mu)| \le p^{t-3}.$$

Proof. By Eq(10) and Eq(24), λ_0 appears in $\lambda_{jq}\lambda_{kq}$ if and only if $k = j$. λ_{q-1} appears in $\lambda_{jq}\lambda_{kq-1}$ if and only if $k - 1 = j$. Therefore, if

$$\prod_{k=1}^{t-1} \lambda_{b_k(\mu)q} = \sum \alpha'_j\lambda_j$$

then the coefficients of λ_0 and λ_{q-1} in $\prod_{k=1}^{t} \lambda_{b_k(\mu)q}$ are some of α'_j, thus are less than or equal to p^{t-3}. The proofs for α_{p^2-1} and α_{p^2-p} are similar.

Remark: If

$$(\lambda_{(p-1)q/2})^t = \alpha_0\lambda_0 + \alpha_{p-1}\lambda_{q-1} + \cdots + \alpha_{p^2-p}\lambda_{(p-1)q} + \alpha_{p^2-1}\lambda_{pq-1}$$

and

$$\prod_{k=1}^{t} \lambda_{b_kq} = \alpha'_0\lambda_0 + \alpha'_{p-1}\lambda_{q-1} + \cdots + \alpha'_{p^2-p}\lambda_{(p-1)q} + \alpha'_{p^2-1}\lambda_{pq-1},$$

then $\max_{i\in I}\{\alpha_i'\} \leq \max_{i\in I}\{\alpha_i\}$. If $t \geq 5$, then $\alpha < p^{t-3}$. Actually, by Eq(24), we can prove in Corollary 2 that when $t = 5$, $|\alpha_i(\mu)| \leq (p^2+1)/2$.

While $p = 2$, we have $\lambda_0\lambda_0 = \lambda_0$, $\lambda_q\lambda_q = \lambda_0$, $\lambda_q\lambda_0 = \lambda_0$, hence we have the following simple formulae:

Proposition 4.3 *Let $p = 2$. Then*

$$\Lambda(n,\mu) = \lambda_0$$

if $\sum_k b_k(\mu)$ is even, and

$$\Lambda(n,\mu) = (-1)^q\lambda_q$$

if $\sum_k b_k(\mu)$ is odd.

Note: $\alpha_i(\mu)$'s are functions of μ and are independent of n.

Now we assume that in

$$\Xi(c_1(\mu+1),\dots c_t(\mu+1)) = \sum_{i=0}^{q-1}\beta_i(\mu+1)\lambda_i, \tag{36}$$

the $\beta_i(\mu+1)$'s have already been evaluated by using the recursive process. By Proposition 4.1, we can write

$$\begin{aligned}\Lambda(n,\mu) =&\alpha_0(\mu)\lambda_0 + \alpha_{p-1}(\mu)\lambda_{q-1} + \alpha_p(\mu)\lambda_q + \alpha_{2p-1}(\mu)\lambda_{2q-1} + \cdots\\ &+ \alpha_{(p-1)p}(\mu)\lambda_{(p-1)q} + \alpha_{p^2-1}(\mu)\lambda_{pq-1}.\end{aligned}$$

Then

$$\begin{aligned}&\Lambda(n,\mu)\Xi(c_1(\mu+1),\dots c_t(\mu+1))\\ =&[\alpha_0(\mu)\beta_0(\mu+1) + \alpha_{p-1}(\mu)\beta_{q-1}(\mu+1)]\lambda_0 + \cdots\\ &+ [\alpha_{(p-1)p}(\mu)\beta_{q-1}(\mu+1) + \alpha_{p^2-1}(\mu)\beta_0(\mu+1)]\lambda_{pq-1}\end{aligned} \tag{37}$$

by Eq(9) and Eq(10). Thus, by Eq(28), Eq(34), Eq(35) and Eq(37),

$$\beta_0(\mu) = \alpha_0(\mu)\beta_0(\mu+1) + \alpha_{p-1}(\mu)\beta_{q-1}(\mu+1) + p^{(t-1)(n-\mu)}\sum_{i=1}^{p}\gamma_i(\mu). \tag{38}$$

Let

$$T(n,\mu) := \beta_{pq-1}(\mu),$$

$$U(n,\mu) := \beta_0(\mu).$$

Write

$$\sum_{i=1}^{p} \gamma_i(\mu)\delta_{iq} = \sum_{i=0}^{pq-1} \beta_i'(\mu)\lambda_i.$$

Then

$$\beta'_{pq-1}(\mu) = (-1)^{pq-1}\gamma_p(\mu). \tag{39}$$

From Eq(35), Eq(37) and Eq(39) we get

$$\begin{aligned} T(n,\mu) =& \alpha_{p^2-p}(\mu)\beta_{q-1}(\mu+1) + \alpha_{p^2-1}(\mu)\beta_0(\mu+1) \\ &+ (-1)^{pq-1}p^{(t-1)(n-\mu)}\gamma_p(\mu). \end{aligned} \tag{40}$$

Combining Eq(38) and Eq(40) we obtain

$$\begin{aligned} \begin{bmatrix} T(n,\mu) \\ U(n,\mu) \end{bmatrix} =& \begin{bmatrix} \alpha_{p^2-p}(\mu) & \alpha_{p^2-1}(\mu) \\ \alpha_{p-1}(\mu) & \alpha_0(\mu) \end{bmatrix} \begin{bmatrix} T(n,\mu+1) \\ U(n,\mu+1) \end{bmatrix} \\ &+ p^{(t-1)(n-\mu)} \begin{bmatrix} (-1)^{pq-1}\gamma_p(\mu) \\ \sum_{i=1}^{p} \gamma_i(\mu) \end{bmatrix}. \end{aligned} \tag{41}$$

Let

$$\mathbf{H}_{n,\mu} := \begin{bmatrix} T(n,\mu) \\ U(n,\mu) \end{bmatrix}, \tag{42}$$

$$\mathbf{A}_\mu := \begin{bmatrix} \alpha_{p^2-p}(\mu) & \alpha_{p^2-1}(\mu) \\ \alpha_{p-1}(\mu) & \alpha_0(\mu) \end{bmatrix}, \tag{43}$$

$$\Gamma_\mu := \begin{bmatrix} (-1)^{pq-1}\gamma_p(\mu) \\ \sum_{i=1}^{p} \gamma_i(\mu) \end{bmatrix}. \tag{44}$$

We will have the following recursive formula:

$$\mathbf{H}_{n,\mu} = \mathbf{A}_\mu \mathbf{H}_{n,\mu+1} + p^{(t-1)(n-\mu)}\Gamma_\mu. \tag{45}$$

For specific p, $\{d_1, \ldots, d_t\}$, and n, the Hilbert-Kunz function of the ring $\mathcal{O}$ in Eq(1) is

$$D_F(\Xi(a_1, \ldots, a_t)) = D_F(\Xi(c_1(0), \ldots, c_t(0)) = \beta_0(0).$$

Using Eq(9), Eq(10), Eq(20) and Eq(24), we formulate a computer program to evaluate the coefficients $\alpha_i(\mu)$'s of λ_i's in $\Lambda(n, \mu)$ defined in Eq(33), and to evaluate $\gamma_i(\mu)$'s defined in Eq(32). Thus, the matrices $\mathbf{A}_\mu$ and Γ_μ can be obtained; $\mathbf{H}_{n,n}$ can also be obtained by directly decompsing the product

$$\Xi(c_1(n), \ldots, c_t(n)) = \prod_{k=1}^{t} (r_k(\delta_{c_k(n)+1} - \delta_{c_k(n)}) + d_k \delta_{c_k(n)})$$

for $c_k(n) < p$. Now the value of $D_F(\Xi(c_1(0), \ldots, c_t(0))$ can be evaluated by the recursive formula Eq(45). The recursion ends at the $n+1$-th step.

5. General formulae and the proof of Theorem 1.1 If $d_k = p^{\epsilon_k} d'_k$ where d'_k is not divisible by p, the function $\mu \mapsto (p^\mu \bmod d_k)$ is periodic for $\mu > \epsilon_k$, and the period is just as that of the function $\mu \mapsto (p^\mu \bmod d'_k)$. Note that in the p-adic expression of $1/d_k = \sum_{\mu=0}^{\infty} b_k(\mu) p^{-\mu}$, we have $b_k(\mu) = b_k(\nu)$ if $p^{\mu-1} \equiv p^{\nu-1} (\bmod\ d_k)$. Thus if $p^{\mu-1} \equiv p^{\nu-1} (\bmod\ d_k)$, we will have $\mathbf{A}_\mu = \mathbf{A}_\nu$ and $\Gamma_\mu = \Gamma_\nu$. Hence $\mathbf{A}_\mu$ and Γ_μ as functions of μ will also be periodic when $\mu > \Delta := \max_{k=1,\ldots,t}\{\epsilon_k\}$. The period ω is a divisor of the least common multiple of the periods of the maps $\mu \mapsto (p^\mu \bmod d'_k)$.

Now we apply our algorithm in §4 to a sufficiently large n. Let

$$n = \Delta + 1 + \tau(n)\omega + \kappa(n)$$

where $0 \le \kappa(n) < \omega$.

$$\begin{aligned}
&\mathbf{H}_{n,0} \\
=&\mathbf{A}_0 \mathbf{H}_{n,1} + p^{n(t-1)} \Gamma_0 \\
=&\mathbf{A}_0 (\mathbf{A}_1 \mathbf{H}_{n,2} + p^{(n-1)(t-1)} \Gamma_1) + p^{n(t-1)} \Gamma_0 \\
=&\mathbf{A}_0 \mathbf{A}_1 \mathbf{H}_{n,2} + p^{(n-1)(t-1)} \mathbf{A}_0 \Gamma_1 + p^{n(t-1)} \Gamma_0 \\
=&\cdots \\
=&\mathbf{A}_0 \ldots \mathbf{A}_\Delta \mathbf{H}_{n,\Delta+1} + p^{(n-\Delta)(t-1)} \mathbf{A}_0 \cdots \mathbf{A}_{\Delta-1} \Gamma_\Delta + \cdots + p^{n(t-1)} \Gamma_0.
\end{aligned}$$

$$C := \mathbf{A}_0 \cdots \mathbf{A}_\Delta, \tag{46}$$

$$\mathbf{b} := \mathbf{A}_0 \cdots \mathbf{A}_{\Delta-1}\Gamma_\Delta + \cdots + p^{\Delta(t-1)}\Gamma_0. \tag{47}$$

Then

$$\mathbf{H}_{n,0} = \mathbf{C} \cdot \mathbf{H}_{n,\Delta+1} + p^{(n-\Delta)(t-1)}\mathbf{b}. \tag{48}$$

Since A_μ and Γ_μ are periodic as $\mu > \Delta$, with period ω, we have

$$\begin{aligned}
&\mathbf{H}_{n,\Delta+1}\\
=&\mathbf{A}_{\Delta+1}\mathbf{H}_{n,\Delta+2} + p^{(t-1)(n-\Delta-1)}\Gamma_{\Delta+1}\\
=&\mathbf{A}_{\Delta+1}(\mathbf{A}_{\Delta+2}\mathbf{H}_{n,\Delta+3} + p^{(t-1)(n-\Delta-2)}\Gamma_{\Delta+2}) + p^{(t-1)(n-\Delta-1)}\Gamma_{\Delta+1}\\
=&\mathbf{A}_{\Delta+1}\mathbf{A}_{\Delta+2}\mathbf{H}_{n,\Delta+3} + p^{(t-1)(n-\Delta-2)}\mathbf{A}_{\Delta+1}\Gamma_{\Delta+2} + p^{(t-1)(n-\Delta-1)}\Gamma_{\Delta+1}\\
=&\mathbf{A}_{\Delta+1}\cdots\mathbf{A}_{\Delta+\omega}\mathbf{H}_{n,\Delta+1+\omega}\\
&+ p^{(t-1)(n-\Delta-\omega)}\mathbf{A}_{\Delta+1}\mathbf{A}_{\Delta+2}\cdots\mathbf{A}_{\Delta+\omega-1}\Gamma_{\Delta+\omega}\\
&+ \cdots + p^{(t-1)(n-\Delta-2)}\mathbf{A}_{\Delta+1}\Gamma_{\Delta+2} + p^{(t-1)(n-\Delta-1)}\Gamma_{\Delta+1}.
\end{aligned}$$

If we denote

$$\mathbf{B} := \mathbf{A}_{\Delta+1}\cdots\mathbf{A}_{\Delta+\omega}, \tag{49}$$

$$\begin{aligned}
\mathbf{v} :=&\mathbf{A}_{\Delta+1}\mathbf{A}_{\Delta+2}\cdots\mathbf{A}_{\Delta+\omega-1}\Gamma_{\Delta+\omega} + \cdots + p^{(t-1)(\omega-2)}\mathbf{A}_{\Delta+1}\Gamma_{\Delta+2}\\
&+ p^{(t-1)(\omega-1)}\Gamma_{\Delta+1},
\end{aligned} \tag{50}$$

we will have

$$\mathbf{H}_{n,\Delta+1} = \mathbf{B}\mathbf{H}_{n,\Delta+1+\omega} + p^{(t-1)(n-\Delta-\omega)}\mathbf{v}. \tag{51}$$

Once the p and $\{d_k\}_{k=1}^t$ are given the $\mathbf{C}$, $\mathbf{b}$, $\mathbf{B}$, $\mathbf{v}$ are determined.

By Proposition 4.1, $\mathbf{A}_\mu$ is diagonal or of the form $\begin{bmatrix} 0 & * \\ * & 0 \end{bmatrix}$, so are $\mathbf{B}$ and $\mathbf{C}$. Thus $\mathbf{B}^2$ must be diagonal. The corollary to Proposition 4.2 says that the eigenvalues of $\mathbf{B}^2$ do not exceed $p^{2(t-3)\omega}$ for $t \geq 3$. It is harmless for us to take the period ω to be 2ω. In this case $\mathbf{B}$ itself is diagonal.

Take

$$\mathbf{B} = \begin{bmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{bmatrix},$$

where the ξ_i's are nonnegative integers with $|\xi_i| \leq p^{(t-3)\omega}$ for $t \geq 3$. The eigenvalues of $\mathbf{B}$ never are $p^{(t-1)\omega}$, and we can take

$$\mathbf{u} := p^{t-1}(p^{(t-1)\omega}\mathbf{I} - \mathbf{B})^{-1}\mathbf{v}. \tag{52}$$

Eq(51) becomes

$$\mathbf{H}_{n,\Delta+1} - p^{(t-1)[n-(\Delta+1)]}\mathbf{u} = \mathbf{B}(\mathbf{H}_{n,\Delta+1+\omega} - p^{(t-1)[n-(\Delta+1+\omega)]}\mathbf{u}).$$

Thus

$$\mathbf{H}_{n,\Delta+1} = p^{(t-1)(n-\Delta-1)}\mathbf{u} + \mathbf{B}^{\tau(n)}(\mathbf{H}_{n,n-\kappa(n)} - p^{(t-1)\kappa(n)}\mathbf{u}). \tag{53}$$

Now $\mathbf{H}_{n,0}$ can be evaluated:

$$\begin{aligned}
&\mathbf{H}_{n,0} \\
=&\mathbf{C}\cdot\left[p^{(t-1)(n-\Delta-1)}\mathbf{u} + \mathbf{B}^{\tau(n)}(\mathbf{H}_{n,n-\kappa(n)} - p^{(t-1)\kappa(n)}\mathbf{u})\right] + p^{(n-\Delta)(t-1)}\mathbf{b} \\
=&\mathbf{C}\cdot\mathbf{B}^{\tau(n)}\left[\mathbf{H}_{n,n-\kappa(n)} - p^{(t-1)\kappa(n)}\mathbf{u}\right] + p^{(t-1)(n-\Delta-1)}\mathbf{C}\mathbf{u} + p^{(n-\Delta)(t-1)}\mathbf{b}.
\end{aligned}$$

Set

$$\mathbf{z} := p^{-(t-1)(\Delta+1)}\mathbf{C}\mathbf{u} + p^{-\Delta(t-1)}\mathbf{b}. \tag{54}$$

Then

$$\mathbf{H}_{n,0} = \mathbf{C}\cdot\mathbf{B}^{\tau(n)}\left[\mathbf{H}_{n,n-\kappa(n)} - p^{(t-1)\kappa(n)}\mathbf{u}\right] + p^{(t-1)n}\mathbf{z}. \tag{55}$$

Note that $\kappa(n) \equiv n - \Delta - 1 (\mathrm{mod}\ \omega)$ is periodic for $n > \Delta$.

$$\begin{aligned}
&\mathbf{H}_{n,n-\kappa(n)} \\
=&\mathbf{A}_{\Delta+1}\mathbf{H}_{n,n-\kappa(n)+1} + p^{(t-1)\kappa(n)}\Gamma_{\Delta+1} \\
=&\cdots \\
=&\mathbf{A}_{\Delta+1}\cdots\mathbf{A}_{\Delta+\kappa(n)}\mathbf{H}_{n,n} + p^{t-1}\mathbf{A}_{\Delta+1}\mathbf{A}_{\Delta+2}\cdots\mathbf{A}_{\Delta+\kappa(n)-1}\Gamma_{\Delta+\kappa(n)} + \cdots \\
&+ p^{(t-1)(\kappa(n)-1)}\mathbf{A}_{\Delta+1}\Gamma_{\Delta+2} + p^{(t-1)\kappa(n)}\Gamma_{\Delta+1}
\end{aligned}$$

where $\mathbf{H}_{n,n}$ is determined by the product

$$\prod_{k=1}^{t}\left[(-1)^{b_k(n)}(p^n \bmod d_k)\lambda_{b_k(n)} + d_k\delta_{b_k(n)}\right]$$
$$= \prod_{k=1}^{t}\left[(-1)^{b_k(\Delta+1+\kappa(n))}(p^n \bmod d_k)\lambda_{b_k(\Delta+1+\kappa(n))} + d_k\delta_{b_k(\Delta+1+\kappa(n))}\right].$$

It will be periodic for $n > \Delta + 1$. Denote

$$\Phi(n) := \mathbf{H}_{n,n-\kappa(n)} - p^{(t-1)\kappa(n)}\mathbf{u}. \tag{56}$$

Eq(55) thus becomes

$$\mathbf{H}_{n,0} = \mathbf{C}\cdot\mathbf{B}^{\tau(n)}\Phi(n) + p^{(t-1)n}\mathbf{z} \tag{57}$$

where $\Phi(n)$ is periodic for $n > \Delta + 1$. Now $\mathbf{B}$ is diagonal and $\mathbf{C}$ is diagonal or of the form $\begin{bmatrix} 0 & * \\ * & 0 \end{bmatrix}$, hence we have

$$h(n) = (\mathbf{H}_{n,0})_{2,1} = \xi^{\tau(n)}\phi(n) + cp^{(t-1)n}$$

for some rational c and periodic function ϕ, here $(\mathbf{H}_{n,0})_{2,1}$ means the (2,1)-entry of the matrix $\mathbf{H}_{n,0}$, and ξ is one of the (integral) eigenvalues of $\mathbf{B}$. By corollary to Proposition 4.2 and Proposition 4.3, we have $\xi \le p^{(t-3)\omega}$ if p is odd prime and $t \ge 3$, and $\xi = 0$ or 1 if $p = 2$ or $t < 3$. This completes the proof of Theorem 1.1.

Now we give an example here to show how the algorithm works.

Example 1. For odd prime $p, t = 4$, $d_1 = d_2 = d_3 = d_4 = 2$, we want to prove that

$$h(n) = \frac{4p^{3n} - p^n}{3}.$$

Let $a := \frac{p-1}{2}$. It is easy to check that

$$\frac{1}{2} = ap^{-1} + ap^{-2} + \cdots = 0.\bar{a}.$$

Thus the period ω is 1, and the length of non-periodic section Δ is 0. Since $b_k(0) = 0$ for $k = 1, \ldots, 4$, we have $\Lambda(n, 0) = \lambda_0$ and $\Gamma_0 = \mathbf{0} = \mathbf{b}$.

$$\Lambda(n,1) = (\lambda_{aq}^2)^2$$
$$= (\lambda_0 + \lambda_{2q-1} + \lambda_{2q} + \cdots + \lambda_{(p-1)q-1} + \lambda_{(p-1)q})^2.$$

By Eq(10) and Eq(24), we find that λ_0 appears in λ_{2iq} λ_{2jq} and in λ_{2iq-1} λ_{2jq-1} if and only if $i = j$. We also find that λ_0 never appears in $\lambda_{2iq}\lambda_{2jq-1}$. There are p choices of the pairs (k,l) where $k,l \in \{2iq, 2jq-1 : 0 \le i \le \frac{p-1}{2}, 1 \le j \le \frac{p-1}{2}\}$, such that λ_0 appears in $\lambda_k\lambda_l$. The coefficient of λ_0 in $\Lambda(n,\mu)$ is p. Similarly, the coefficient of $\lambda_{(p-1)q}$ in $\Lambda(n,\mu)$ is also p. We have

$$\Lambda(n,\mu) = p\lambda_0 + \alpha_{2p-1}(\mu)\lambda_{2q-1} + \cdots + p\lambda_{(p-1)q}$$

for all $\mu \ge 1$. Thus $\mathbf{C} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ and $\mathbf{B} = \mathbf{A}_\mu = \begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix}$. The (2,1)-entry of Γ_1 is

$$D_F([(-1)^{(p-1)/2}\lambda_{(p-1)/2} + 2\delta_{(p-1)/2}]^4 - \lambda_{(p-1)/2}^4) = h(1) - p$$

So we have

$$\mathbf{v} = \Gamma_1 = \begin{bmatrix} * \\ h(1) - p \end{bmatrix},$$

$$\mathbf{u} = p^{t-1}(p^{(t-1)\omega}\mathbf{I} - \mathbf{B})^{-1}\mathbf{v} = \frac{p^3}{p^3 - p}\mathbf{v} = \frac{p^3}{p^3 - p}\Gamma_1,$$

$$\mathbf{z} = p^{-(t-1)(\Delta+1)}\mathbf{C}\mathbf{u} + p^{-\Delta(t-1)}\mathbf{b} = \frac{1}{p^3 - p}\Gamma_1.$$

For $\omega = 1, \kappa(n)$ is always 0.

$$\Phi(n) = \mathbf{H}_{n,n} - \mathbf{u}.$$

Note that the (2,1)-entry of $\mathbf{H}_{n,n}$ is $D_F([(-1)^{(p-1)/2}\lambda_{(p-1)/2} + 2\delta_{(p-1)/2}]^4)$ $= h(1)$.

$$\Phi(n)_{2,1} = h(1) - \frac{p^3}{p^3 - p}(h(1) - p) = \frac{ph(1) - p^4}{p^3 - p},$$

$$h(n) = (\mathbf{H}_{n,0})_{2,1} = p^{n-1}\Phi(n)_{2,1} + p^{3n}\mathbf{z}_{2,1} = p^n \frac{h(1)-p^3}{p^3-p} + p^{3n}\frac{h(1)-p}{p^3-p}.$$

We are going to show that

$$h(1) = (4p^3 - p)/3.$$

If we do, we will have $h(n) = (4p^{3n} - p^n)/3$.

Note that $h(1) = D_F([(-1)^{(p-1)/2}\lambda_{(p-1)/2} + 2\delta_{(p-1)/2}]^4)$
$= D_F([\delta_{(p+1)/2} + \delta_{(p-1)/2}]^4)$.

$$\begin{aligned}
&(\delta_{(p+1)/2} + \delta_{(p-1)/2})^4 \\
=&(\delta^2_{(p-1)/2} + 2\delta_{(p-1)/2}\delta_{(p+1)/2} + \delta^2_{(p+1)/2})^2 \\
=&[(\delta_1 + \delta_3 + \cdots + \delta_{p-2}) + 2(\delta_2 + \delta_4 + \cdots + \delta_{p-1}) \\
&+ (\delta_1 + \delta_3 + \cdots + \delta_{p-2} + \delta_p)]^2 \\
=&(2\delta_1 + 2\delta_2 + \cdots + 2\delta_{p-1} + \delta_p)^2.
\end{aligned}$$

it is easy to show that

$$D_F(\delta_i\delta_j) = \min(i,j) \tag{58}$$

for all i, j. To prove this, if $i \le j$, we observe that

$$D_F(\delta_i\delta_j) = \dim_F F[x,y]/(x^i, y^j, x+y).$$

Because $F[x,y]/(x^i, y^j, x+y) = F[x]/(x^i)$, Eq(58) follows.

$$\begin{aligned}
&D_F([\delta_{(p+1)/2} + \delta_{(p-1)/2}]^4) \\
=&D_F([2\delta_1 + 2\delta_2 + \cdots + 2\delta_{p-1} + \delta_p]^2) \\
=&D_F(2\delta_1[2\delta_1 + 2\delta_2 + \cdots + 2\delta_{p-1} + \delta_p]) \\
&+ D_F(2\delta_2[2\delta_1 + 2\delta_2 + \cdots + 2\delta_{p-1} + \delta_p]) \\
&+ \cdots + D_F(2\delta_{p-1}[2\delta_1 + 2\delta_2 + \cdots + 2\delta_{p-1} + \delta_p]) \\
&+ D_F(\delta_p[2\delta_1 + 2\delta_2 + \cdots + 2\delta_{p-1} + \delta_p]) \\
=&2[2(p-1)+1] + 2[2 + 4(p-2) + 2] + \cdots \\
&+ 2[2 + 4 + \cdots + 2(p-1) + p - 1] + [p(p-1) + p] \\
=&(4p^3 - p)/3.
\end{aligned}$$

Note: In Theorem 1.1, while $t \geq 4$ and p is odd, we actually have $|l| = p^{\omega(t-3)}$ if and only if $t = 4$ and for each $i, d_i = 2p^{e_i}$ for some non-negative integers e_i. For given $p > 2$ and t, the maximal value of l in Theorem 1.1 will be attained while $d_i = 2p^{e_i}$ for each i. These can be easily shown by the remark following Corollary 2 to Proposition 4.2.

6. The proof of Theorem 1.2. In this section, by using the representation ring again, we want to prove Theorem 1.2.

Let $M := F[X_1, \ldots, X_s]/(X_1^{p^n}, \ldots, X_s^{p^n})$ with T-acting by multiplication by $X_1^{d_1} \cdots X_s^{d_s}$, i.e.,

$$Tf(X_1, X_2, \ldots, X_s) := X_1^{d_1} \cdots X_s^{d_s} f(X_1, \ldots, X_s).$$

Then M is an $F[T]$-object. We may assume that $d_1 \geq d_2 \geq \cdots \geq d_s$. It is easy to check that

$$\dim_F(M/T^j M) = p^{sn} - \prod_{i=1}^{s}(p^n - jd_i),$$

for $0 \leq j \leq [p^n/d_1]$. By the T action on M and the definition of ψ, we can also assume that

$$\psi(M) = \sum_{j=1}^{a_1+1} \alpha_j \delta_j,$$

where $a_i = [\frac{p^n}{d_i}]$ and $p^n = a_i d_i + r_i$. By a simple deduction, we have

$$\alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + j\alpha_j + j\alpha_{j+1} + \cdots + j\alpha_{a_1+1} = p^{sn} - \prod_{i=1}^{s}(p^n - jd_i).$$

Note here that the residue r_i is an eventually periodic function of n. From this, we can evaluate α_j's. The results are as follows:

$$\alpha_j = -2\prod_{i=1}^{s}(p^n - jd_i) + \prod_{i=1}^{s}(p^n - (j-1)d_i) + \prod_{i=1}^{s}(p^n - (j+1)d_i)$$

for $1 \leq j \leq a_1 - 1$ and

$$\alpha_{a_1} = -2\prod_{i=1}^{s}(p^n - a_1 d_i) + \prod_{i=1}^{s}(p^n - (a_1 - 1)d_i),$$

$$\alpha_{a_1+1} = \prod_{i=1}^{s}(p^n - a_1 d_i).$$

Similarly, let $e_1 \geq e_2 \geq \cdots \geq e_t$, $p^n = b_i e_i + w_i$ with $0 \leq w_i < e_i$, and let

$$N := F[Y_1, \ldots, Y_t]/(Y_1^{p^n}, \ldots, Y_t^{p^n})$$

with T-acting by multiplication by $Y_1^{e_1} \cdots Y_t^{e_t}$. Set

$$\psi(N) = \sum_{j=1}^{b_1+1} \beta_j \delta_j.$$

Then we have

$$\beta_j = -2\prod_{i=1}^{t}(p^n - je_i) + \prod_{i=1}^{t}(p^n - (j-1)e_i) + \prod_{i=1}^{t}(p^n - (j+1)e_i)$$

for $1 \leq j \leq b_1 - 1$ and

$$\beta_{b_1} = -2\prod_{i=1}^{t}(p^n - b_1 e_i) + \prod_{i=1}^{t}(p^n - (b_1 - 1)e_i),$$

$$\beta_{b_1+1} = \prod_{i=1}^{t}(p^n - b_1 e_i).$$

Now we want to evaluate

$$H := D_F\left(\left(\sum_{i=1}^{a_1+1} \alpha_i \delta_i\right)\left(\sum_{j=1}^{b_1+1} \beta_j \delta_j\right)\right).$$

Assume that $d_1 \geq e_1$. By Eq(58) we have

$$\begin{aligned} H =& \sum_i \sum_j \alpha_i \beta_j \min(i,j) \\ =& \alpha_1\left(\sum_{j=1}^{b_1+1} \beta_j\right) + \alpha_2\left(\beta_1 + 2\sum_{j=2}^{b_1+1} \beta_j\right) + \alpha_3\left(\beta_1 + 2\beta_2 + 3\sum_{j=3}^{b_1+1} \beta_j\right) \\ &+ \cdots + \alpha_{a_1+1}\left[\beta_1 + 2\beta_2 + 3\beta_3 + \cdots + a_1\beta_{a_1} + (a_1+1)\left(\sum_{j=a_1+1}^{b_1+1} \beta_j\right)\right]. \end{aligned}$$

Now

$$\beta_1 + 2\beta_2 + 3\beta_3 + \cdots + j\beta_j + j\beta_{j+1} + \cdots + j\beta_{b_1+1} = p^{tn} - \prod_{i=1}^{t}(p^n - je_i)$$

for $j \leq b_1$ and

$$\sum_{j=1}^{b_1+1} j\beta_j = p^{tn}.$$

Therefore, if $b_1 > a_1$,

$$H = \sum_{\mu=1}^{a_1+1} \alpha_\mu \left[p^{tn} - \prod_{i=1}^{t}(p^n - \mu e_i) \right], \tag{59}$$

and if $b_1 = a_1$,

$$H = \sum_{\mu=1}^{a_1} \alpha_\mu \left[p^{tn} - \prod_{i=1}^{t}(p^n - \mu e_i) \right] + \alpha_{a_1+1} p^{tn}. \tag{60}$$

Notice that the latter case happens for large n only if $d_1 = e_1$. We first consider the case $b_1 > a_1$. Let s_i and t_i be the i-th elementary symmetric polynomials in d_k's and e_k's respectively. For $\mu < a_1$,

$$\alpha_\mu = \sum_{j=2}^{s} (-1)^j s_j (2\mu^j - (\mu+1)^j - (\mu-1)^j) p^{n(t-j)},$$

and

$$p^{tn} - \prod_{i=1}^{t}(p^n - \mu e_i) = \sum_{l=1}^{t} (-1)^{l-1} t_l \mu^l p^{n(t-l)}.$$

Then

$$\begin{aligned}
&\alpha_\mu \left[p^{tn} - \prod_{i=1}^{t}(p^n - \mu e_i) \right] \\
&= \sum_{j=2}^{s} \sum_{l=1}^{t} \mu^l (2\mu^j - (\mu+1)^j - (\mu-1)^j)(-1)^{j+l-1} s_j t_l p^{n(s+t-l-j)} \\
&= \sum_{j=2}^{s} \sum_{l=1}^{t} \left[j(j-1)\mu^{j+l-2} + O(\mu^{j+l-4}) \right] (-1)^{j+l-1} s_j t_l p^{n(s+t-l-j)},
\end{aligned}$$

and

$$\begin{aligned}&\sum_{\mu=1}^{a_1-1}[j(j-1)\mu^{j+l-2}+O(\mu^{j+l-4})]\\ =&j(j-1)\frac{a_1^{j+l-1}}{j+l-1}+O(a^{j+l-2})\\ =&\frac{j(j-1)}{(j+l-1)d_1^{j+l-1}}p^{n(j+l-1)}+O(p^{n(j+l-2)}).\end{aligned}$$

We note here that

$$k\mapsto\sum_{\mu=1}^{k}\mu^j$$

is a polynomial function of k with leading term $k^{j+1}/(j+1)$. Therefore,

$$\begin{aligned}&\sum_{\mu=1}^{a_1-1}\alpha_\mu\left[p^{tn}-\prod_{i=1}^{t}(p^n-\mu e_i)\right]\\ =&\left[\sum_{j=2}^{s}\sum_{l=1}^{t}\frac{j(j-1)}{(j+l-1)d_1^{j+l-1}}(-1)^{j+l-1}s_jt_l\right]p^{n(s+t-1)}+O(p^{n(j+l-2)}).\end{aligned}\tag{61}$$

On the other hand,

$$\begin{aligned}&\alpha_{a_1}\left[p^{tn}-\prod_{i=1}^{t}(p^n-a_1e_i)\right]\\ =&-2\prod_{i=1}^{s}(p^n-a_1d_i)+\prod_{i=1}^{s}(p^n-(a_1-1)d_i)\left[p^{tn}-\prod_{i=1}^{t}(p^n-a_1e_i)\right]\\ =&\Bigg\{-2r_1\prod_{j=2}^{s}[((d_1-d_j)p^n+r_1d_j)/d_1]+(d_1+r_1)\prod_{j=2}^{s}[((d_1-d_j)p^n\\ &+r_1d_j)/d_1+d_j]\Bigg\}\times\left(p^{tn}-\prod_{i=1}^{t}\left[p^n-(p^n-r_1)e_i/d_1\right)\right]\\ =&(d_1-r_1)\prod_{j=2}^{s}(1-d_j/d_1)\left[1-\prod_{i=1}^{t}(1-e_i/d_1)\right]p^{(t+s-1)n}+O(p^{(t+s-2)n}),\end{aligned}\tag{62}$$

and for $a_1<b_1$, we have

$$\begin{aligned}
&\alpha_{a_1+1}\left[p^{tn}-\prod_{i=1}^{t}(p^n-(a_1+1)e_i)\right]\\
(63)\quad &=r_1\prod_{j=2}^{s}[((d_1-d_j)p^n+r_1d_j)/d_1]\left[p^{tn}-\prod_{i=1}^{t}(p^n-(a_1+1)e_i)\right]\\
&=r_1\prod_{j=2}^{s}(1-d_j/d_1)\left[1-\prod_{i=1}^{t}(1-e_i/d_1)\right]p^{(t+s-1)n}+O(p^{(t+s-2)n});
\end{aligned}$$

for $a_1 = b_1$, we have

$$\begin{aligned}
&\alpha_{a_1+1}p^{tn}\\
&=r_1\prod_{j=2}^{s}[((d_1-d_j)p^n+r_1d_j)/d_1]p^{tn}\\
&=r_1\prod_{j=2}^{s}(1-d_j/d_1)p^{(t+s-1)n}+O(p^{(t+s-2)n}).
\end{aligned}$$

But for $n \gg 0$, $a_1 = b_1$ only if $d_1 = e_1$. Hence the formula (63) is valid for $a_1 \le b_1$ if $n \gg 0$. By (59) to (63), we get

$$H = cp^{(t+s-1)n} + O(p^{(t+s-2)n})$$

for $n \gg 0$ where

$$\begin{aligned}
c :&= d_1\prod_{j=2}^{s}(1-d_j/d_1)\left[1-\prod_{i=1}^{t}(1-e_i/d_1)\right]\\
&+\sum_{j=2}^{s}\sum_{l=1}^{t}\left[\frac{j(j-1)}{(j+l-1)d_1^{j+l-1}}(-1)^{j+l-1}s_jt_l\right]
\end{aligned}$$

is a rational number.

Note that the $O(p^{(t+s-2)n})$ is a polynomial function of $1/d_1, d_1, d_2, \ldots, d_s, r_1, e_1, \ldots, e_t$ and p^n over $\mathbb{Q}$ and $r_1 = (p^n \bmod d_1)$ is an eventually periodic function. Thus

$$H = cp^{(t+s-1)n} + \Delta_{t+s-2}p^{(t+s-2)n} + \Delta_{t+s-3}p^{(t+s-3)n} + \cdots + \Delta_0$$

where Δ_i's are eventually periodic functions.

Example 2. Let $\mathcal{O} := \mathbb{Z}/(p)[|x,y,z,t|]/(xy+zt)$. We want to show that

$$e_n(\mathcal{O}) = (4p^{3n} - p^n)/3.$$

Let $q := p^n$. Then $M := \mathbb{Z}/(p)[x,y]/(x^q, y^q)$, $N := \mathbb{Z}/(p)[z,t]/(z^q, t^q)$ are $\mathbb{Z}/(p)$-objects if the T-action is defined as:

$$T(f) := (xy)f, \quad f \in M,$$

$$T(g) := (zt)g, \quad g \in N.$$

It is easy to see that

$$\psi(M) = \psi(N) = 2\delta_1 + 2\delta_2 + \cdots + 2\delta_{q-1} + \delta_q$$

Thus by a similar process as in Example 1, we have:

$$e_n(\mathcal{O}) = (4q^3 - q)/3.$$

Example 3. (cf.[7]) Let $\mathcal{O} := \mathbb{Z}/(p)[[x,y,z]]/(x^m + yz)$. We show that

$$e_n(\mathcal{O}) = (2 - 1/m)p^{2n} + (r^2/m - 1)$$

where r is the remainder of $q := p^n$ divided by m. Here we have to evaluate

$$D_F((2\delta_1 + 2\delta_2 + \cdots + 2\delta_{q-1} + \delta_q)[(m-r)\delta_a + r\delta_{a+1}]),$$

where $p^n = q = ma + r$. By Eq(58), it's easy.

Acknowledgments. It is for us a pleasure to thank Professor M. C. Kang; his advicement and constant encouragement convince us in making this article more complete.

References

1. L. Chiang, *Hilbert-Kunz functions*, Doctoral Thesis, National Taiwan Normal University, 1996.

2. A. Conca, *Hilbert-Kunz function of monomial ideals and binomial hypersurfaces*, Manuscripta Math. **90** (1996), 287-300.

3. C. Han, *The Hilbert-Kunz function of a diagonal hypersurface*, Doctoral Thesis, Brandeis University, 1992.

4. C. Han and P. Monsky, *Some surprising Hilbert-Kunz functions*, Math. Z. **214** (1993), 119-135.

5. E. Kunz, *Characterizations of regular local rings of characteristic p*, Amer. J. Math. **41** (1969), 772-784.

6. E. Kunz, *On Noetherian rings of characteristic p*, Amer. J. Math. **98** (1976), 999-1013.

7. P. Monsky, *The Hilbert-Kunz function*, Math. Ann. **263** (1983), 43-49.

Department of Mathematics, National Taiwan University, Taipei, Taiwan.
E-mail: chiangl@math.ntu.edu.tw. FAX:886-2-391-4439.

Department of Mathematics, National Taiwan Normal University, Taipei, Taiwan.
E-mail: hungyc@math.ntnu.edu.tw. FAX:886-2-933-2342.