数理解析研究所講究録
第 801 巻 1992 年 1-13

Non-Cohen-Macaulay symbolic blow-ups for space monomial curves and counterexamples to Cowsik's question

明大・理工 後藤四郎 (Shiro Goto)

Let $\mathbf{p}$ be a prime ideal in a commutative Noetherian ring A and put

$$R_s(\mathbf{p}) := \sum_{n\geq 0} \mathbf{p}^{(n)}t^n \subseteq A[t],$$

where t denotes an indeterminate over A. Let me call it the symbolic Rees algebra of $\mathbf{p}$. In my lecture, I'm interested in their ring-theoretic properties and especially, in the following two questions:

Questions (1) When is $R_s(\mathbf{p})$ a Noetherian ring, that is, when is $R_s(\mathbf{p})$ a finitely generated A-algebra?
(2) When is $R_s(\mathbf{p})$ a Cohen-Macaulay or Gorenstein ring, provided that it is Noetherian?

Today I will answer these questions in the following special situation, that is,

Let k be a field, and let n_1, n_2, and n_3 be positive integers with $GCD(n_1, n_2, n_3) = 1$. Let $A = A_k := k[[X, Y, Z]]$ be a formal power series ring over k and let $\varphi : A \to k[[t]]$ be the k-algebra map defined by

$$\varphi(X) = t^{n_1}, \quad \varphi(Y) = t^{n_2}, \quad \text{and} \quad \varphi(Z) = t^{n_3}.$$

Let me denote by $\mathbf{p} := \mathbf{p}_k(n_1, n_2, n_3)$ the kernel of φ .

Then A is a regular local ring of dimension 3 and $\mathbf{p}$ is a prime ideal in A of height 2 . So in some sense, this is the simplest non-trivial case for the above questions. And my answer is

<u>Theorem</u> 1 (with Nishida and Watanabe). Let m and n be positive integers such that $n \geq 4$ and $2m > n + 1$. Let $n_1 = 7m - 3$, $n_2 = 5mn - m - n$, and $n_3 = 8n - 3$. Assume that $GCD(n_1, n_2, n_3) = 1$ and let $\mathbf{p} = \mathbf{p}_k(n_1, n_2, n_3)$. Then the symbolic Rees algebra $R_s(\mathbf{p})$ of $\mathbf{p}$ is a Noetherian ring if and only if the characteristic of the ground field k is positive. When this is the case, $R_s(\mathbf{p})$ is not a Cohen-Macaulay ring.

The simplest example obtained by this theorem is the ideal

$$\mathbf{p} = \mathbf{p}_k(18, 53, 29) \qquad \text{(here } m = 3,\ n = 4\text{)}$$

$$= I_2\begin{bmatrix} X^4 & Y^2 & Z^5 \\ Y & Z^3 & X^7 \end{bmatrix}$$

$$= (Z^8 - X^7Y^2,\ X^{11} - YZ^5,\ Y^3 - X^4Z^3)A_k .$$

Therefore, if we consider the same prime ideal $P = (Z^8 - X^7Y^2, X^{11} - YZ^5, Y^3 - X^4Z^3)B$ inside of the polynomial ring $B = k[X, Y, Z]$, the symbolic Rees algebra $R_s(P)$ is a finitely generated k-algebra but not a Cohen-Macaulay ring if ch k is positive, and if ch k = 0 , say $k = \mathbf{Q}$, then it is not a finitely generated $\mathbf{Q}$-algebra.

Let me add one question:

Question What about the prime ideal

$$\mathbf{p} = \mathbf{p}_k(11, 25, 21)$$

$$= I_2\begin{bmatrix} X^3 & Y^2 & Z^3 \\ Y & Z^2 & X^5 \end{bmatrix}$$

(that is, choose $m = 2$ and $n = 3$)? Of course, this ideal doesn't satisfy my condition. But by a theorem of Cutkosky you can easily check that $R_s(\mathbf{p})$ is a Noetherian ring, if ch $k > 0$. However I couldn't know whether it is a Noetherian ring or not in the case where ch $k = 0$, though I believe that the answer is negative.

Now let me give a sketch of proof of the theorem. To do this I need a theorem due to Craig (Huneke). For a moment, let me assume that (A, m) is a regular local ring of dimension 3 and $\mathbf{p}$ is a prime ideal in A of $\dim A/\mathbf{p} = 1$.

Theorem 2 (C. Huneke). If there exist two elements $f \in \mathbf{p}^{(k)}$ and $g \in \mathbf{p}^{(l)}$ with positive integers k, l such that the equality

$$l_A(A/(x, f, g)) = kl \cdot l_A(A/\mathbf{p} + xA)$$

holds for some (and hence for any) element $x \in m \setminus \mathbf{p}$, then the symbolic Rees algebra $R_s(\mathbf{p})$ is a Noetherian ring. If the field A/m is infinite, the converse is also true.

By this theorem, Huneke showed that $R_s(\mathbf{p})$ is a Noetherian ring for $\mathbf{p} = \mathbf{p}_k(n_1, n_2, n_3)$, if $\min\{n_1, n_2, n_3\} \leq 4$.

If $R = R_s(\mathbf{p})$ is a Noetherian ring, then you can easily get an isomorphism $K_R \cong R(-1)$. Therefore R is a Gorenstein ring, once it is Cohen-Macaulay. To check the Cohen-Macaulay property of R, you have the following

Theorem 3 (___, Nishida and Shimoda). Let f and g be the elements in the above theorem. Then the following two conditions are equivalent.

(1) The symbolic Rees algebra $R_s(\mathbf{p})$ is a Gorenstein ring.

(2) For any integer $1 \leq n \leq k + l - 2$, the ring $A/(f, g) + p^{(n)}$ is a Cohen-Macaulay ring.

When this is the case, the rings $A/(f) + \mathbf{p}^{(n)}$, $A/(g) + \mathbf{p}^{(n)}$, and $A/(f, g) + \mathbf{p}^{(n)}$ are Cohen-Macaulay for all $n \geq 1$, and we have the equality

$$R_s(\mathbf{p}) = A[\{\mathbf{p}^{(n)}t^n\}_{1 \leq n \leq k + l - 2}, ft^k, gt^l].$$

Using this criterion, you can show that $R_s(\mathbf{p})$ is a Gorenstein ring for $\mathbf{p} = \mathbf{p}_k(n_1, n_2, n_3)$, if $\min\{n_1, n_2, n_3\} \leq 4$. But in general, the Cohen-Macaulay property of $R_s(\mathbf{p})$ depends on the characteristic of the ground field. Let me give one example:

Example Let $\mathbf{p} = \mathbf{p}_k(7, 11, 13)$. Then $R_s(\mathbf{p})$ is always a Noetherian ring, but it is a Gorenstein ring if and only if $\mathrm{ch}\, k \neq 2, 3$.

Now let's start the proof of the theorem. In what follows, let m and n be positive integers such that $n \geq 4$ and $2m > n$

+ 1. Let $n_1 = 7m - 3$, $n_2 = 5mn - m - n$, and $n_3 = 8n - 3$. We assume that $GCD(n_1, n_2, n_3) = 1$. Then

$$\mathbf{p} = \mathbf{p}_k(n_1, n_2, n_3)$$

$$= I_2\begin{bmatrix} X^n & Y^2 & Z^{2m-1} \\ Y & Z^m & X^{2n-1} \end{bmatrix}.$$

Let $a = Z^{3m-1} - X^{2n-1}Y^2$, $b = X^{3n-1} - YZ^{2m-1}$, and $c = Y^3 - X^nZ^m$. Then $\mathbf{p} = (a, b, c)$ and we have two equations

$$X^na + Y^2b + Z^{2m-1}c = 0,$$
$$Ya + Z^mb + X^{2n-1}c = 0.$$

I claim that

Lemma There exist elements $d_2 \in \mathbf{p}^{(2)}$, and d_3, $d_3' \in \mathbf{p}^{(3)}$ such that $d_2 \equiv Z^{5m-2}$, $d_3 \equiv Z^{7m-2}$, $d_3' \equiv Y^8Z^{2m-2}$ mod (X), and

$$Xd_3 + Ybc^2 + Zd_3' = 0.$$

Proof. First of all, consider two expressions of $-Y^2ab$:

$$-Y^2ab = Yb(-Ya) = Yb(Z^mb + X^{2n-1}c)$$
$$= a(-Y^2b) = a(X^na + Z^{2m-1}c).$$

And you get

$$X^n(a^2 - X^{n-1}Ybc) = Z^m(Yb^2 - Z^{m-1}ac);$$

hence there exists an element d_2 of A such that

$$X^nd_2 = Yb^2 - Z^{m-1}ac, \text{ and}$$

$$Z^m d_2 = a^2 - X^{n-1}Ybc .$$

Of course, d_2 is in $\mathbf{p}^{(2)}$. To get Yd_2, consider

$$\begin{aligned} -Yad_2 &= d_2(-Ya) \\ &= d_2(Z^m b + X^{2n-1}c) \\ &= b \cdot Z^m d_2 + X^{n-1}c \cdot X^n d_2 \\ &= b(a^2 - X^{n-1}Ybc) + X^{n-1}c(Yb^2 - Z^{m-1}ac) \\ &= -a(-ab + X^{n-1}Z^{m-1}c^2). \end{aligned}$$

Thus $Yd_2 = -ab + X^{n-1}Z^{m-1}c$ and we have two equations:

$$Yd_2 = -ab + X^{n-1}Z^{m-1}c^2 ,$$

$$Z^m d_2 = a^2 - X^{n-1}Ybc .$$

We compare two expressions of a^2b :

$$\begin{aligned} a^2b &= b(Z^m d_2 + X^{n-1}Ybc) \\ &= a(-Yd_2 + X^{n-1}Z^{m-1}c^2). \end{aligned}$$

Then we have

$$Z^{m-1}(-Zbd_2 + X^{n-1}ac^2) = Y(a d_2 + X^{n-1}bc^2).$$

and so we get an element $d_3 \in \mathbf{p}^{(3)}$ such that

$$Yd_3 = -Zbd_2 + X^{n-1}ac^2 .$$

As $Yd_2 \equiv -ab \mod (X)$, we know

$$Yd_2 \equiv -Z^{3m-1}(-YZ^{2m-1});$$

hence $d_2 \equiv Z^{5m-2} \mod (X)$. As $Yd_3 \equiv -Zbd_2 \mod (X)$, we get

$$Yd_3 \equiv -Z(-YZ^{2m-1})Z^{5m-2} \mod (X);$$

hence $d_3 \equiv Z^{7m-2} \mod (X)$. Notice that $Yd_3 \equiv X^{n-1}ac^2$ $\equiv X^{n-1}(-X^{2n-1}Y^2)(Y^3)^2 \mod (Z)$ and we have

$$d_3 \equiv -X^{3n-2}Y^7 \mod (Z),$$

so that

$$Xd_3 + Ybc^2 \equiv X \cdot (-X^{3n-2}Y^7) + Y \cdot X^{3n-1} \cdot (Y^3)^2 \equiv 0$$

mod (Z). Thus there is an element d_3' of $\mathbf{p}^{(3)}$ such that

$$Xd_3 + Ybc^2 + Zd_3' = 0 .$$

Clearly $d_3' \equiv Y^8Z^{2m-2} \mod (X)$. This proves the lemma.

Proposition $\mathbf{p}^{(2)} = \mathbf{p}^2 + (d_2)$, $\mathbf{p}^{(3)} = \mathbf{p}\mathbf{p}^{(2)} + (d_3, d_3')$, and $\mathbf{p}^{(4)} \neq \mathbf{p}\mathbf{p}^{(3)} + (\mathbf{p}^{(2)})^2$.

For example, let $I = \mathbf{p}^2 + (d_2)$. Then as $(X) + I = (X) + (Z^{3m-1}, YZ^{2m-1}, Y^3)^2 + (Z^{5m-2})$, you have

$$\begin{aligned} \ell_A(A/(X)+I) &= 3 \cdot (7m-3) \\ &= 3 \cdot \ell_A(A/(X)+\mathbf{p}). \end{aligned}$$

On the other hand, because $\ell_A(A/(X)+\mathbf{p}^{(2)}) = e_{XA}(A/\mathbf{p}^{(2)}) = \ell_A(A/(X)+\mathbf{p}) \cdot \ell_{A_\mathbf{p}}(A_\mathbf{p}/\mathbf{p}^2A_\mathbf{p}) = 3 \cdot \ell_A(A/(X)+\mathbf{p})$, you get that

$\ell_A(A/(X) + I) = \ell_A(A/(X) + \mathbf{p}^{(2)})$; hence $(X) + I = (X) + \mathbf{p}^{(2)}$, because $I \subseteq \mathbf{p}^{(2)}$. Consequently $\mathbf{p}^{(2)} = I + (X) \cap \mathbf{p}^{(2)} = I + X\,\mathbf{p}^{(2)}$. Thus we have $\mathbf{p}^{(2)} = I$ by Nakayama's lemma. Similarly you can show that $\mathbf{p}^{(3)} = \mathbf{p}\mathbf{p}^{(2)} + (d_3, d_3')$. As

$$\begin{aligned}\ell_A(A/(X) + \mathbf{p}^{(4)}) &= e_{XA}(A/\mathbf{p}^{(4)}) \\ &= \ell_A(A/(X) + \mathbf{p}) \cdot \ell_{A_\mathbf{p}}(A_\mathbf{p}/\mathbf{p}^4A_\mathbf{p}) \\ &= 10 \cdot \ell_A(A/(X) + \mathbf{p}) \\ &< \ell_A(A/(X) + \mathbf{p}\mathbf{p}^{(3)} + (\mathbf{p}^{(2)})^2),\end{aligned}$$

we have

$$\mathbf{p}^{(4)} \neq \mathbf{p}\mathbf{p}^{(3)} + (\mathbf{p}^{(2)})^2 .$$

Corollary The ring $A/(c) + \mathbf{p}^{(3)}$ is not Cohen-Macaulay.

In fact, notice that

$$\begin{aligned}\ell_A(A/(X, c) + \mathbf{p}^{(3)}) &= 3 \cdot (7m - 3) + 1 \\ &> e_{XA}(A/(c) + \mathbf{p}^{(3)}) \\ &= 3 \cdot (7m - 3);\end{aligned}$$

hence $A/(c) + \mathbf{p}^{(3)}$ cannot be a Cohen-Macaulay ring.

Now let me assume that $\operatorname{ch} k = p > 0$. First of all, assume that $p \geq 3$ and write $p = 2q + 1$ (hence $q \geq 1$). Then by the equations

$$Xd_3 + Ybc^2 + Zd_3' = 0 ,$$

we get

$$\begin{aligned}0 &\equiv X^p d_3{}^p + Y^p b^p c^{2p} \quad \mod (Z^p) \\ &= X^p d_3{}^p + (Y^2 b)^q Y b^{q+1} c^{2p} .\end{aligned}$$

As $X^n a + Y^2 b + Z^{2m-1} c = 0$, we furthermore have

$$0 \equiv X^p d_3{}^p + (-1)^q \sum_{i=0}^{q} \binom{q}{i} X^{n(q-i)} Y Z^{(2m-1)i} a^{q-i} b^{q+1} c^{2p+i}$$

$$\equiv X^p d_3{}^p + (-1)^q \sum_{(2m-1)i < p} \binom{q}{i} X^{n(q-i)} Y Z^{(2m-1)i} a^{q-i} b^{q+1} c^{2p+i}$$

mod (Z^p).

Now recall that $2m > n + 1$ and $n \geq 4$. Then we have $n(q - i) \geq p$ or $(2m - 1)i \geq p$ for each $0 \leq i \leq q$. (In fact, if $n(q - i) < p$ and $(2m - 1)i < p$, then we get $n(q - i) \leq 2q$ and $(2m - 1)i \leq 2q$ so that $nq + (2m - n - 1)i \leq 4q$. Hence we must have $n = 4$ and $i = 0$ and so $n(q - i) = 4q \leq 2q$, which is impossible.) Thus

$$0 \equiv X^p \Big\{ d_3{}^p + (-1)^q \sum_{(2m-1)i<p} \binom{q}{i} X^{n(q-i)-p} Y Z^{(2m-1)i} a^{q-i} b^{q+1} c^{2p+i} \Big\}$$

mod (Z^p) and thus we have an element $h \in \mathbf{p}^{(3p)}$ such that

$$Z^p h = d_3{}^p + (-1)^q \sum_{(2m-1)i<p} \binom{q}{i} X^{n(q-i)-p} Y Z^{(2m-1)i} a^{q-i} b^{q+1} c^{2p+i} \Big\}.$$

As $Z^p h \equiv d_3{}^p \equiv Z^{(7m-2)p}$ mod (X, c), we get $h \equiv Z^{(7m-3)p}$ mod (X, c). Thus we have the following

Lemma There exists an element $h \in \mathbf{p}^{(3p)}$ such that $h \equiv Z^{(7m-3)p}$ mod (X, c).

(You can prove this lemma also in the case $p = 2$.)

Now recall Huneke's theorem. First we take $f = c$ and $g = h$. Then

$$\begin{aligned} l_A(A/(X, c, h)) &= l_A(A/(X, c, Z^{(7m-3)p})) \\ &= l_A(A/(X, Y^3, Z^{(7m-3)p})) \\ &= 3p \cdot (7m-3) \\ &= 1 \cdot 3p \cdot l_A(A/(X) + \mathbf{p}) . \end{aligned}$$

Hence $R_s(\mathbf{p})$ is a Noetherian ring by Theorem 2. Because $A/(c) + \mathbf{p}^{(3)}$ is not a Cohen-Macaulay ring, $R_s(\mathbf{p})$ cannot be Cohen-Macaulay by Theorem 3.

To study the case of ch $k = 0$, we need further information in the case where ch $k = p > 0$. Let $\mathbf{F} = \{ 0 < l \in \mathbf{Z} \mid \exists g \in \mathbf{p}^{(l)}$ such that $l_A(A/(X, c, g)) = l \cdot l_A(A/(X) + \mathbf{p}) \}$. Then $3p \in \mathbf{F}$. Let $l_0 = \min \mathbf{F}$ and choose $g_0 \in \mathbf{p}^{(l_0)}$ so that $l_A(A/(X, c, g_0)) = l_0 \cdot l_A(A/(X) + \mathbf{p})$. Then we have

Lemma (1) $l_0 \mid l$ for all $l \in \mathbf{F}$.

(2) $R_s(\mathbf{p}) = A[\{\mathbf{p}^{(n)}t^n\}_{1 \le n \le l_0 - 1}, ct, g_0 t^{l_0}]$.

(3) $g_0 t^{l_0}$ is not contained in $A[\{\mathbf{p}^{(n)}t^n\}_{1 \le n \le l_0 - 1}]$.

Let me use this lemma without proof. First, we have by (1) that $l_0 \mid 3p$; hence $l_0 = 1, 3, p$, or $3p$. But if $l_0 \neq p, 3p$, then we have by (2) that $R_s(\mathbf{p}) = A[\mathbf{p}t, \mathbf{p}^{(2)}t^2, \mathbf{p}^{(3)}t^3]$, which is impossible because $\mathbf{p}^{(4)} \neq \mathbf{p}\mathbf{p}^{(3)} + (\mathbf{p}^{(2)})^2$. Thus $l_0 \geq p$ and by (3) we get $g_0 t^{l_0}$ is not contained in $A[\{\mathbf{p}^{(n)}t^n\}_{1 \leq n \leq l_0 - 1}]$. This means, to generate the A-algebra $R_s(\mathbf{p})$, you need at least one new element of degree $\geq p$, depending on the characteristic $p = \mathrm{ch}\, k$. On the other hand, if $R_s(\mathbf{p})$ were a Noetherian ring in the case where $\mathrm{ch}\, k = 0$, say $k = \mathbf{Q}$, then because everything is defined over $\mathbf{Z}$, you can find a system of generators for the algebra $R_s(\mathbf{p_Q})$ so that passing to the field $k = \mathbf{Z}/p\mathbf{Z}$ for $p >> 0$, the system still generates the algebra $R_s(\mathbf{p}_k)$ (see the theorem below). This is impossible, because you need at least one new element of degree $\geq p$. Thus $R_s(\mathbf{p_Q})$ cannot be a Noetherian ring for our example $\mathbf{p}$.

Let me state the required theorem more explicitly.

Theorem Let $C = \mathbf{Z}[X, Y, Z]$ and let $I = \mathrm{Ker}\,(\varphi : C \to \mathbf{Z}[t])$ where $\varphi(X) = t^{n_1}$, $\varphi(Y) = t^{n_2}$, and $\varphi(Z) = t^{n_3}$. Then if $R_s(\mathbf{p})$ is a Noetherian ring for the prime ideal $\mathbf{p} = \mathbf{p_Q}(n_1, n_2, n_3)$ in $\mathbf{Q}[[X, Y, Z]]$, there exist positive integers l and N and elements f and g of $I^{(l)}$ such that for all prime numbers $p \geq N$, we have

(1) $I^{(l)} A_k = p_k{}^{(l)}$ and

(2) $l_{A_k}(A_k/(X, f, g)A_k) = l^2 \cdot l_{A_k}(A_k/(X) + \mathbf{p}_k)$,

where $k = \mathbf{Z}/p\mathbf{Z}$.

Here $A_k = k[[X, Y, Z]]$ and $\mathbf{p}_k = \mathbf{p}_k(n_1, n_2, n_3)$.

Before closing my talk, let me give a few open problems.

Problems Let $\mathbf{p} = \mathbf{p}_k(n_1, n_2, n_3)$ and $n = \min\{n_1, n_2, n_3\}$.
(1) ch $k = p > 0 \Rightarrow R_s(\mathbf{p})$ is a Noetherian ring?
(2) ch $k = 0$ and $R_s(\mathbf{p})$ is Noetherian $\Rightarrow R_s(\mathbf{p})$ is a Gorenstein ring?
(3) $n \leq 8$, $n \neq 7 \Rightarrow R_s(\mathbf{p})$ is a Gorenstein ring? (For $\mathbf{p} = \mathbf{p}_k(9, 10\ 13)$ you can show that $R_s(\mathbf{p})$ is a Noetherian ring but not Cohen-Macaulay, if ch $k = 2, 3, 7$.)
(4) $n = 5 \Rightarrow R_s(\mathbf{p})$ is a Noetherian ring?
(5) $n = 6 \Rightarrow R_s(\mathbf{p})$ is a Gorenstein ring? (The Noetherian property of this case was guaranteed by Cutkosky.)
(6) $\mathbf{p} = \mathbf{p}_k(11, 16, 13) \Rightarrow$?????

References

[1] S. D. Cutkosky, Symbolic algebras of monomial primes, J. reine angew. Math., **416** (1991), 71-89.

[2] S. Goto and K. Nishida, On the structure of Noetherian Rees algebras of filtrations, preprint 1992.

[3] S. Goto, K. Nishida, and Y. Shimoda, The Gorensteinness of symbolic Rees algebras for space curves, J. Math. Soc. Japan, **43** (1991), 465-481.

[4] S. Goto, K. Nishida, and K. Watanabe, Non-Cohen-Macaulay symbolic Rees algebras for space monomial curves and counterexamples to Cowsik's question, preprint 1991.

[5] C. Huneke, On the finite generation of symbolic blow-ups, Math. Z., **179** (1982), 465-472.

[6] C. Huneke, Hilbert functions and symbolic powers, Michigan Math. J., **34** (1987), 293-318.

[7] M. Morales, Noetherian symbolic blow-ups, J. Alg., **140** (1991), 12-

25.

[**8**] M. Morimoto and S. Goto, Non-Cohen-Macaulay symbolic blow-ups for space monomial curves, to appear in Proc. Amer. Math. Soc.

[**9**] P. Roberts, An infinitely generated symbolic blow-up in a power series ring and a new counterexample to Hilbert's fourteenth problem, J. Alg., **132** (1990), 461-473.

[**10**] P. Roberts, A prime ideal in a polynomial ring whose symbolic blow-up is not Noetherian, Proc. Amer. Math. Soc., **94** (1985), 589-592.

[**11**] W. V. Vasconcelos, Symmetric algebras and factoriality, Mathematical Sciences Research Institute Publications, **15** (1989), 467-496.