J. Math. Soc. Japan
Vol. 26, No. 4, 1974

On the unboundedness of generators of prime ideals in powerseries rings of three variables

By T. T. MOH*

(Received Aug. 15, 1973)

§1. Introduction.

In [7] p. 36 F. S. Macaulay has given a famous set of prime ideals $\{P_n\}$ in the polynomial ring in 3 variables which need at least n generators. In fact all the examples are ideals defining irreducible curves in affine 3-space with singularities at the origin. A modern explanatorial presentation of those classical examples has been delivered by S. S. Abhyankar (Notes by A. Sathaye) in [1]. F. S. Macaulay's examples illustrate in the best way that "There is no higher limit to the number of members that may be required for the basis of a prime module (=ideal)" (quoted from [7]).

However, F. S. Macaulay's classical examples cannot be adapted directly to show the same result for power series rings in three variables. In fact, locally, in the sense of analytic geometry, Macaulay's curves dissolve into a bunch of straight lines. It is the purpose of this article to furnish a new set of curves in 3-dimensional space to illustrate the unboundedness of generators for prime ideals in the polynomial ring and power series ring in three variables at the same time. To this end we shall construct a set $\{C_n\}$ of rational irreducible curves in 3-dimensional affine space which are analytically irreducible at the origin. Moreover the corresponding prime ideals P_n need at least n generators in $k[[x, y, z]]$ and hence in $k[x, y, z]$.

In §2 we shall introduce the concept of binomial vectors and prove the linear independence of them under projections.

In §3 an arithmetic property, namely "residuely equal distributions", about semigroups will be introduced. The above mentioned property is a refinement of a well-known fact about semigroups observed by Sylvester, Aprey [2], Gorenstein [4] et al.

In §4 we shall provide a proof by constructing examples of the following theorem:

THEOREM. *Let k be a field of characteristic zero and $A=k[[x, y, z]]$, the powerseries ring in 3 variables over k. Then for each $n \geqq 1$ there exists a prime*

* This work was supported in part by NSF grant GP-37689.

ideal $P_n \subset k[[x, y, z]]$ such that P_n needs at least n generators.

The author was informed about this problem by the speech of J. Herzog at Purdue University and the discussions after it with S. S. Abhyankar. Recently D. Eisenbud and M. Hochster greatly encouraged him to search for examples. To the above mentioned persons the author wishes to express his thanks. The author's gratitude is due to his wife, Lii meei-huey, who helped prove Theorem 2.1. Finally, he wants to thank Mrs. Louise Ruppert for typing this manuscript.

§ 2. The linear independence of binomial vectors.

Let k be any field of characteristic zero. Let the ring of integer $\boldsymbol{Z}$ be canonically imbedded in k. Let k^m(resp. k^∞) be the canonical m-dimensional (∞-dimensional) vector space over k. We define

DEFINITION 2.1. *Let $b_{n,0}, b_{n,1}, \cdots, b_{n,n}$ be the sequence of binomial coefficients of n-th power. Then the n-th binomial vector b_n (in k^∞) is defined to be* $(b_{n,0}, \cdots, b_{n,n}, 0, \cdots)$.

EXAMPLES. $b_0 = (1, 0, \cdots, 0, \cdots)$, $b_1 = (1, 1, 0, \cdots)$, $b_2 = (1, 2, 1, 0, \cdots)$, $b_3 = (1, 3, 3, 1, 0, \cdots)$.

NOTATIONS. Let ρ_m denote the mapping from k^∞ to k^m defined by

$$\rho_m(r_1, r_2, \cdots, r_m, \cdots) = (r_1, r_2, \cdots, r_m)\,.$$

Let ρ'_m denote the mapping from k^∞ to k^{m-1} defined by

$$\rho'_m(r_1, r_2, \cdots, r_m, \cdots) = (r_2, r_3, \cdots, r_m)\,.$$

Let $T = \{t_1, \cdots, t_m\}$ be a subset of non-negative integers. Moreover, let $t_1, \cdots, t_m$ be labeled as $t_1 < t_2 < \cdots < t_m$. Let $B_{t_1,\cdots,t_m}$ be the $m \times m$ matrix defined by

$$\begin{aligned} B_{t_1,\cdots,t_m} &= (\rho_m(b_{t_1}), \cdots, \rho_m(b_{t_m})) \\ &= \begin{pmatrix} b_{t_1,0}, & \cdots, & b_{t_1,m-1} \\ \vdots & & \vdots \\ b_{t_m,0}, & \cdots, & b_{t_m,m-1} \end{pmatrix}. \end{aligned}$$

Moreover let

$$ {}_iA = \begin{pmatrix} 1 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 1 & & & 0 & \cdots & & 0 \\ & & & \ddots & & & & & \\ & & & & 1 & -1 & \cdots & & 0 \\ & & & & 0 & 1 & \cdots & & 0 \\ & & & & & & & 1 & 0 \\ 0 & 0 & & & & & & 0 & 1 \end{pmatrix} i\text{-th} $$

be a $m\times m$ matrix. Let $A_m=\prod_{i=1}^{m-1}{}_iA$.

LEMMA 2.1. *Suppose* $t_1>0$. *Then*

$$B_{t_1,t_2,\cdots,t_m}A_m=B_{t_1-1,t_2-1,\cdots,t_m-1}\,.$$

Moreover

$$\det B_{t_1,t_2,\cdots,t_m}=\det B_{t_1-1,t_2-1,\cdots,t_m-1}\,.$$

PROOF. Certainly it is enough to prove the first equation. Let us consider the left hand side of it. Clearly

$$B_{t_1,t_2,\cdots,t_m}A_m=\begin{pmatrix} b_{t_1,0},\ b_{t_1,1}-b_{t_1-1,0}\ \ ,\cdots,\ b_{t_1,m-1}-b_{t_1-1,m-2} \\ \vdots \qquad\qquad\qquad \vdots \\ b_{t_m,0},\ b_{t_m,1}-b_{t_m-1,0},\cdots,\ b_{t_m,m-1}b_{t_m-1,m-2} \end{pmatrix}$$

$$=\begin{pmatrix} b_{t_1-1,0},\ b_{t_1-1,1}\ \ ,\cdots,\ b_{t_1-1,m-1} \\ \vdots \qquad\qquad \vdots \\ b_{t_m-1,0},\ b_{t_m-1,1},\cdots,\ b_{t_m-1,m-1} \end{pmatrix}$$

$$=B_{t_1-1,t_2-1,\cdots,t_m-1}\,.$$

Since

$$b_{t_i,0}=b_{t_i-1,0}=1$$

and

$$b_{t_i,j}-b_{t_i-1,j-1}=b_{t_i-1,j}\,. \qquad \text{Q. E. D.}$$

LEMMA 2.2. *Suppose* $t_1=0$. *Then*

$$\det B_{t_1,t_2,\cdots,t_m}=\det(\rho'_m(b_{t_2}),\cdots,\rho'_m(b_{t_m}))\,.$$

PROOF. Routine.

LEMMA 2.3. *We have*

$$\det(\rho'_m(b_{t_2}),\cdots,\rho'_m(b_{t_m}))=(t_2\cdots t_m)/(m-1)!\det B_{t_2-1,\cdots,t_m-1}\,.$$

PROOF. It is trivial to check that

$$b_{t_i,j}=t_i(t_i-1)\cdots(t_i-j+k)/j!$$
$$=t_i/jb_{t_i-1,j-1}\,.$$

Hence if in the following matrix we multiply the j-th column by j and i-th row by $1/t_{i+1}$

$$(\rho'_m(b_{t_2}),\cdots,\rho'_m(b_{t_m}))=\begin{pmatrix} b_{t_2,1},\ \cdots,\ b_{t_2,m-1} \\ \vdots \qquad\qquad \vdots \\ b_{t_m,1},\ \cdots,\ b_{t_m,m-1} \end{pmatrix}$$

then we get

$$\begin{pmatrix} b_{t_2-1,0},\ \cdots,\ b_{t_2-1,m-1} \\ \vdots \qquad\qquad \vdots \\ b_{t_m-1,0},\ \cdots,\ b_{t_m-1,m-1} \end{pmatrix}=B_{t_2-1,\cdots,t_m-1}\,.$$

Now our lemma follows trivially.

We shall establish

THEOREM 2.1. *The set* $\{\rho_m(b_{t_1}), \cdots, \rho_m(b_{t_m})\}$ *forms a basis for* k^m.

PROOF. We shall make inductions on m. If $m=1$, then $\rho_1(b_{t_1})=(1)$ which is a basis for k'. Let us assume the theorem holds for all positive integers less than $m>1$. We shall prove the case $t_1=0$ firstly. It follows from lemmas 2.2 and 2.3 that

$$\det b_{t_1,t_2,\cdots,t_m}=(t_2 \cdots t_m)/(m-1)!\det b_{t_2-1,\cdots,t_m-1}.$$

It follows from the hypothesis of mathematical induction that the right hand side, hence the left hand side, is nonzero. In other words $\{b_{t_1}, \cdots, b_{t_m}\}$ forms a basis for k^m. Inductively let us assume the theorem has been proved for certain $t_1 \geqq 0$. Let us consider $b_{t_1+1}, b_{t_2}, \cdots, b_{t_m}$ with $t_1+1<t_2<\cdots<t_m$. Then it follows from lemma 2.1 that

$$\det B_{t_1+1,t_2,\cdots,t_m}=\det B_{t_1,t_2-1,\cdots,t_m-1}.$$

Again it follows from the hypothesis of mathematical induction that the right hand side, hence the left hand side, is nonzero. Thus $\{b_{t_1+1}, b_{t_2}, \cdots, b_{t_m}\}$ forms a basis for k^m. Q.E.D.

For completeness we shall include the following theorem in this section. However since it will not be needed in this article, the proof is left to readers.

THEOREM 2.2. *Let* $C_{n,s}$ *be the following* $m \times m$ *matrix,*

$$C_{n,s}=\begin{pmatrix} b_{n,s}, b_{n,s+1}, \cdots, b_{n,s+m-1} \\ \vdots \qquad\qquad \vdots \\ b_{n+m-1,s}\ , \cdots, b_{n+m-1,s+m-1} \end{pmatrix}.$$

Then

$$\det C_{n,s}=\prod_{i=n}^{n+m-1} b_{i,s}\Big/\prod_{i=s}^{s+m-1} b_{i,s}.$$

EXAMPLE.

$$\det\begin{pmatrix} 10, & 10, & 5, & 1 \\ 15, & 20, & 15, & 6 \\ 21, & 35, & 35, & 21 \\ 28, & 56, & 70, & 56 \end{pmatrix}=10\times15\times21\times28/1\times3\times6\times10=490.$$

Note that the sequence $(b_{s,s}, b_{s+1,s}, \cdots)$ is the standard s-th order arithmetic sequence. Incidently, it follows from Theorem 2.2 that

COROLLARY. *The product of m consecutive members of the standard s-th order arithmetic sequence is divisible by the product of the first m ones.*

PROOF. It follows from the fact that $\det C_{n,s}$ is an integer.

§ 3. Equal distributions of semigroups.

Apéry [2], and subsequently Gorenstein [4], proved that if Q is a point on a plane curve then $n_Q = 2\delta_Q$, where $\delta_Q = \dim O_Q/O'_Q$ and $n_Q = \dim O_Q/C_Q$, O'_Q being the local ring of Q, O_Q its normalization, and C_Q the conductor. The above statement is equivalent to the following; let S be the semigroup of orders of all holomorphic functions defined on the plane curve and centered at Q, let L be the largest integer which is not in S. Then the number of elements in S which are less than L is $(L+1)/2$. To refine the above concept we shall define

DEFINITION 3.1. A semigroup S of nonnegative integers is said to be residuely equally distributed $\bmod n$, where n is a positive integer, if

$$\mathrm{Card}\,(S \cap \{i+n\boldsymbol{Z}\} \cap Z_L) = (L+1)/2n \qquad \text{for all} \quad i\,,$$

where

1) Card A = Cardinal number of set A.

2) L is the largest integer not in S.

3) $Z_L = \{i : i \in Z,\ 0 \leqq i \leqq L\}$.

REMARK. The fact observed by Apéry and Gorenstein is equivalent to that the semigroup S is residuely equally distributed mod 1.

The following proposition is trivial.

PROPOSITION 3.1. *Let n, m be two positive integers with $n|m$. Suppose S is residuely equally distributed* $\bmod m$. *Then it is residuely equally distributed* $\bmod n$.

Clearly the conditions in Definition 3.1 cannot be satisfied by arbitrary S and n. However we shall prove that they can be satisfied in some interesting cases. Namely

THEOREM 3.1. *Let n be an odd positive integer. Then the semigroup S generated by $(n+1)$ and $(n+2)$ is residuely equally distributed* $\bmod n$.

PROOF. The following two well-known properties of S will be assumed.

1) The largest integer L not in S is $n(n+1)-1$.

2) The semigroup S is residuely equally distributed mod 1.

Let us write down all integers between 0 and L in the following $n \times (n+1)$ matrix

$$\begin{pmatrix} 0 & 1 & ,\cdots, & n \\ n+1\;, & n+2 & ,\cdots, & 2n+1 \\ \vdots & \vdots & & \vdots \\ i(n+1)\;, & i(n+1)+1 & ,\cdots, & (i+1)(n+1)-1 \\ \vdots & \vdots & & \vdots \\ (n-1)(n+1), & (n-1)(n+1)+1, & \cdots, & n(n+1)-1 \end{pmatrix} = (d_{ij}) = D\,.$$

We shall prove $d_{ij} \in S$ if $i \geqq j$. Clearly

$$\begin{aligned} d_{ij} &= (i-1)(n+1)+(j-1) \\ &= (i-j)(n+1)+(j-1)(n+2) \in S . \end{aligned}$$

In view of the second well-known property of S, one concludes that $d_{ij} \notin S$ if $i<j$.

Next we shall find the set $\{k+nZ\} \cap Z_L$ in the previous matrix. Without losing generality one could assume that $0 \leqq k < n$. Clearly the components of D on the following arrow sign is in $\{k+nZ\} \cap Z_L$,

$$\begin{pmatrix}
 & & & \swarrow & & \\
a_{11}, & a_{12}, & \cdots & , a_{1,k+1}, \cdots & & a_{1,n+1} \\
 & & & \swarrow & & \\
a_{21}, & a_{22}, & \cdots, a_{2,k}, & & & a_{2,n+1} \\
\vdots & \vdots & \swarrow & & & \vdots \\
 & & \swarrow & & & \\
a_{k,1}, & a_{k,2}, & & & & a_{k,n+1} \\
\swarrow & & & & & \swarrow \\
a_{k+1,1}, & a_{k+1,2}, & & & & a_{k+1,n+1} \\
 & & & & \swarrow & \\
a_{k+2,1}, & a_{k+2,2} & & & a_{k+2,n}, & a_{k+2,n+1} \\
\vdots & \vdots & & & \swarrow & \vdots \\
 & & & & \swarrow & \\
a_{n,1}, & a_{n,2}, & \cdots & & , a_{n,k+2}, \cdots , & a_{n,n+1}
\end{pmatrix} .$$

There are precisely $(n+1)$ elements on the arrow. Thus

$$\{k+nZ\} \cap Z_L = \{a_{1,k+1}, a_{2,k}, \cdots , a_{k+1,1}, a_{k+1,n+1}, \cdots , a_{n,k+2}\} .$$

Now we shall use a simple counting to show that half of the elements in $\{k+nZ\} \cap Z_L$ are in S and half are not. Suppose $k+1$ is even. Then the first $(k+1)/2$ elements are not in S, the next $(k+1)/2$ are in S, the $(n-k)/2$ elements after that are not and the last $(n-k)/2$ are in S. Suppose $(k+1)$ is odd. Then the first $k/2$ elements are not in S, the next $k/2+1$ elements are in S, the $(n-k-1)/2+1$ elements are not in S and the last $(n-k-1)/2$ elements are in S. In either case the required property has been established. Now it is trivial to check that

$$\begin{aligned} \mathrm{Card}\,(S \cap \{k+nZ\} \cap Z_L) &= (n+1)/2 \\ &= (L+1)/2n . \end{aligned}$$

Q. E. D.

§ 4. The construction of P_n.

To prove the theorem stated in § 1 we shall construct explicitly a set of prime ideals $\{P_n\}$ with the required properties.

Let n be an odd positive integer, and $m=(n+1)/2$. Let S be the semigroup generated by $(n+1)$ and $(n+2)$. Let λ be an integer $>n(n+1)m$ with $(\lambda, m)=1$. Let ρ be a mapping: $k[[x, y, z]]\rightarrow k[[t]]$ defined by

$$\rho(x)=t^{nm}+t^{nm+\lambda}$$

$$\rho(y)=t^{(n+1)m}$$

$$\rho(z)=t^{(n+2)m}$$

where $k[[t]]$ is a powerseries ring of one variable over k. Let $P_n=P=\ker\rho$.

It is obvious that P is a prime ideal in $k[[x, y, z]]$. To prove that P needs at least n generators, we shall investigate the mapping $\sigma: k[[x, y, z]]\rightarrow k[[x, y, z]]$ defined by

$$\sigma(z)=x^{n}$$

$$\sigma(y)=y^{n+1}$$

$$\sigma(z)=z^{n+2}.$$

For self-containedness we shall give the following common definition.

DEFINITION 4.1. *The σ-order of $f(x, y, z)\in k[[x, y, z]]$ is* $\operatorname{ord}\sigma f(x, y, z)$. *The σ-leading form of $f(x, y, z)$ is σ^{-1} (the leading form of $\sigma f(x, y, z)$). The powerseries $f(x, y, z)$ is said to be σ-homogeneous if $f(x, y, z)=$ the σ-leading form of $f(x, y, z)$.*

Note that, as usual, all σ-homogeneous powerseries of a fixed σ-order r form a vector space W_r over ground field k. Let its dimension be d_r.

LEMMA 4.1. *The numbers d_r are all finite.*

PROOF. It follows trivially from the fact that $W_r\subset$ the vector space generated by $\{x^{\alpha}y^{\beta}z^{\gamma}: \alpha, \beta, \gamma\leqq r\}$. Q. E. D.

Let $\bar{U}_r=W_r\cap k[[y, z]]$ and $e_r=\dim\bar{U}_r$. Then

THEOREM 4.1. *Let the notations be as previous. One has*

1) $d_r=\sum_{i} e_i$ *where* $i\in S\cap\{r+nZ\}\cap Z_r$.

Especially

2) $d_r\leqq m$ *if* $r<n(n+1)$.

3) $d_r=m+s$ *if* $n(n+s)\leqq r<n(n+s+1)$ *and* $r<(n+1)(n+2)$.

PROOF. Clearly $d_r=$ number of monomials in W_r. For a fixed α let us consider all possible monomials $x^{\alpha}y^{\beta}z^{\gamma}$ in W_r. It is obvious that $\alpha n+\beta(n+1)+\gamma(n+2)=r$ or $\beta(n+1)+\gamma(n+2)=r-\alpha n$. Clearly any pair (β, γ) which satisfies the above equation will correspond to a monomial in $\bar{U}_{r-\alpha n}$. Conversely any monomial in $\bar{U}_{r-\alpha n}$ will give a monomial in W_r which is of the form $x^{\alpha}y^{\beta}z^{\gamma}$. Note that a necessary and sufficient condition for a given (β, γ) to satisfy $\beta(n+1)+\gamma(n+2)=r-\alpha n$ for some nonnegative integer α is $\beta(n+1)+\gamma(n+2)\in S\cap\{r+nZ\}\cap Z_r$. Hence if we let

$$W_{r,\alpha}=W_r\cap x^{\alpha}k[[y, z]]$$

then

$$\begin{aligned} W_r &= \bigoplus_{\alpha} W_{r,\alpha} \\ &\cong \bigoplus_{\alpha} \bar{U}_{r-\alpha n} \\ &= \bigoplus \bar{U}_i \text{ where } i\in S\cap\{r+nZ\}\cap Z_r\,. \end{aligned}$$

And

$$d_r=\sum e_i\,.$$

Note that if $i\leqq r<(n+1)(n+2)$ and $\beta(n+1)+\gamma(n+2)=\varepsilon(n+1)+\delta(n+2)$ then $\beta=\varepsilon$ and $\gamma=\delta$. Hence $e_i=1$ $\forall i<(n+1)(n+2)$. Thus

$$d_r=\text{Card}\,(S\cap\{r+nZ\}\cap Z_r)\;,$$

if $r<(n+1)(n+2)$. Now it follows from Theorem 3.1 that

$$\text{Card}\,(S\cap\{r+nZ\}\cap Z_r)\leqq m$$

if $r<n(n+1)$. Hence 2) follows.

To prove 3) it is enough to observe that $S\supset\{i: i\geqq n(n+1)\}$ (cf. the property 1) listed in the proof of theorem 3.1). Q. E. D.

To use the results in § 2, we shall define

DEFINITION 4.2. *Let $x^{\alpha}y^{\beta}z^{\gamma}$ be a monomial. Then the associated binomial vector $b(x^{\alpha}y^{\beta}z^{\gamma})$ is $b(_{\alpha,0}, b_{\alpha,1}, \cdots, b_{\alpha,\alpha,0}, \cdots)\in k^{\infty}$. The associated binomial m-vector $b_m(x^{\alpha}y^{\beta}z^{\gamma})$ is defined to be $\rho_m b(x^{\alpha}y^{\beta}z^{\gamma})\in k^m$,* (cf. § 2). *Let $\sum c_{\alpha\beta\gamma}x^{\alpha}y^{\beta}z^{\gamma}$ be σ-homogeneous. Then $b(\sum c_{\alpha\beta\gamma}x^{\alpha}y^{\beta}z^{\gamma})$ is defined to be $\sum c_{\alpha\beta\gamma}b(x^{\alpha}y^{\beta}z^{\gamma})$ and $b_m(\sum C_{\alpha\beta\gamma}x^{\alpha}y^{\beta}z^{\gamma})=\rho_m b(\sum C_{\alpha\beta\gamma}x^{\alpha}y^{\beta}z^{\gamma})$. In general let $f(x, y, z)$ be an element in $k[[x, y, z]]$, then $b(f(x, y, z))$ is defined to be b (σ-leading form of $f(x, y, z)$) and $b_m(f(x, y, z))$ is defined to be $\rho_m b(f(x, y, z))$.*

We shall prove

PROPOSITION 4.1. *If $f(x, y, z)\in P=P_n$, then*

$$b_m(f(x, y, z))=0\,.$$

PROOF. Let $r=\sigma$-order of $f(x, y, z)$. Then $f(x, y, z)$ can be written as $g(x, y, z)+h(x, y, z)$ with $g(x, y, z)$ as its σ-leading form. Let $a_{\alpha\beta\gamma}x^{\alpha}y^{\beta}z^{\gamma}$ (resp. $a_{\varepsilon\delta\mu}x^{\varepsilon}y^{\delta}z^{\mu}$) be a nonzero term in the expansion of $g(x, y, z)$ (resp. $h(x, y, z)$). Let σ-order of $a_{\varepsilon\delta\mu}x^{\varepsilon}y^{\delta}z^{\mu}$ be $s>r$. Then

$$\rho(a_{\alpha\beta\gamma}x^{\alpha}y^{\beta}z^{\gamma})=a_{\alpha\beta\gamma}[b_{\alpha,0}t^{rm}+b_{\alpha,1}t^{rm+\lambda}+\cdots+b_{\alpha,m-1}t^{rm+(m-1)\lambda}+\cdots]$$

and

$$\rho(a_{\varepsilon\delta\mu}x^{\varepsilon}y^{\delta}z^{\mu})=a_{\varepsilon\delta\mu}[b_{\varepsilon,0}t^{sm}+b_{\varepsilon,1}t^{sm+\lambda}+\cdots+b_{\varepsilon,m-1}t^{sm+(m-1)\lambda}+\cdots]\,.$$

Suppose $t^{rm+u\lambda}=t^{sm+v\lambda}$ with $u<m$. Since $s>r$, then $v<u<m$. Moreover $m\mid(u-v)$. Thus $u=v$ and $t^{rm+u\lambda}\neq t^{sm+v\lambda}$. In other words, terms of the form

$t^{rm+u\lambda}$ can only be produced from σ-leading forms of $f(x, y, z)$ and hence can only be cancelled among them.

Now let us consider the equation $t^{rm+u\lambda}=t^{rm+v\lambda}$ with $u<m$. Clearly $u=v$. Suppose

$$g(x, y, z)=\sum a_{\alpha\beta\gamma}x^{\alpha}y^{\beta}z^{\gamma},$$

$$h(x, y, z)=\sum a_{\varepsilon\delta\mu}x^{\varepsilon}y^{\delta}z^{\mu}.$$

Then

$$\begin{aligned}\rho(f(x, y, z))&=\rho(g(x, y, z))+\rho(h(x, y, z))\\&=\sum a_{\alpha\beta\gamma}[b_{\alpha,0}t^{rm}+b_{\alpha,1}t^{rm+\lambda}+\cdots+b_{\alpha,m-1}t^{rm+(m-1)\lambda}]\\&\qquad+[\text{non-interference terms}].\end{aligned}$$

Clearly

$$\sum a_{\alpha\beta\gamma}b_{\alpha i}=0 \qquad \forall i\leqq m-1.$$

It is obviously equivalent to

$$b_m(f(x, y, z))=0. \qquad \text{Q.E.D.}$$

Let $V_r=W_r\cap\{\sigma\text{-leading forms of elements in } P\}\cup\{0\}$. Then V_r is a vector space over k. Let its dimension be c_r. We shall establish

THEOREM 4.2. *Let the notations be as previous. Then*

1) $C_r=0$ *if* $r<n(n+1)$.

2) $C_r=d_r-m$ *if* $r\geqq n(n+1)$.

Especially

3) $C_r=1$ *if* $n(n+1)\leqq r<n(n+2)$.

Moreover the kernel of the mapping $b_m: W_r\rightarrow k^m$ *is* V_r.

PROOF. Let $r<n(n+1)$. Let $\{x^{\alpha}y^{\beta}z^{\gamma}\}$ be the set of monomials in W_r. Note that

1) $\{x^{\alpha}y^{\beta}z^{\gamma}\}$ forms a basis for W_r.

2) distinct elements in this set have distinct α indices.

3) $b_m(x^{\alpha}y^{\beta}z^{\gamma})=\rho_m b_{\alpha}$.

Hence

$$\begin{aligned}d_r&=\text{Card}\,\{x^{\alpha}y^{\beta}z^{\gamma}\}\\&=\text{Card}\,\{\rho_m b_{\alpha}\}\\&\leqq m.\end{aligned}$$

It follows from Theorem 2.1 the set $\{\rho_m b_{\alpha}\}$, hence the set $\{b_m(x^{\alpha}y^{\beta}z^{\gamma})\}$, is linearly independent. Thus $b_m: W_r\rightarrow k^m$ is injective and $\ker b_m=0$. Now it follows from Proposition 4.1 that $V_r\subset\ker b_m$. Hence $V_r=0$. Case 1 has been proved.

Suppose $r \geqq n(n+1)$. We shall prove $b_m : W_r \to k^m$ is surjective. It follows from Theorem 3.1 that $\operatorname{Card}(S \cap \{r+nZ\} \cap Z_L) = m$. Let $\beta_i(n+1)+\gamma_i(n+2) \in S \cap \{r+nZ\} \cap Z_L$ and $\alpha_i n = r-(\beta_i(n+1)+\gamma_i(n+2))$ $\forall 1 \leqq i \leqq m$. Then $x^{\alpha_i} y^{\beta_i} z^{\gamma_i} \in W_r$ and $\alpha_i \neq \alpha_j$ if $i \neq j$. Since $b_m(x^{\alpha_i} y^{\beta_i} z^{\gamma_i}) = \rho_m b_{\alpha_i}$. It follows from Theorem 2.1 that $\{\rho_m b_{\alpha_i}\}$ hence $\{b_m(x^{\alpha_i} y^{\beta_i} z^{\gamma_i})\}$ forms a basis for k^m. Thus $b_m : W_r \to k^m$ is surjective and $\dim(\ker b_m) = d_r - m$. To finish our proof we shall show that $\ker b_m \subset \{\sigma\text{-leading forms of elements of } P\} \cup \{0\}$, since the other inclusion follows from Proposition 4.1.

Let $f(x, y, z)$ be a non-zero element in $\ker b_m$. Inductively we shall find elements $g_i(x, y, z)$ for all $i \geqq rm+m\lambda$ such that

1) $\operatorname{ord}_t \rho g_i(x, y, z) = s \geqq i$,
2) $\operatorname{ord}_t \rho(g_{i+1}(x, y, z) - g_i(x, y, z)) \geqq i$,
3) σ-leading form of $g_i(x, y, z)$ is $f(x, y, z)$,
4) $\operatorname{ord}(g_{i+1}(x, y, z) - g_i(x, y, z)) \geqq (i-m\lambda)/(m(n+2))$.

Once the set $\{g_i(x, y, z)\}$ has been found, if we let $g(x, y, z) = \lim_{i\to\infty} g_i(x, y, z)$, then

1) $\operatorname{ord}_t \rho g(x, y, z) = \infty$,
2) $g(x, y, z) \in P$,
3) σ-leading form of $g(x, y, z)$ is $f(x, y, z)$.

In other words $\ker b_m \subset \{\sigma\text{-leading forms of elements of } P\} \cup \{0\}$.

Let $g_i(x, y, z) = f(x, y, z)$ for $i = rm+m\lambda$. Since $b_m(h(x, y, z)) = 0$, then all terms of the form $t^{rm+j\lambda}$ with $j < m$ in $\rho(f(x, y, z))$ are cancelled out. The only possible terms left are with $j \geqq m$. So that conditions 1) and 3) have been proved. Note that conditions 2) and 4) are void for this step.

Inductively, suppose $g_i(x, y, z)$ has been found for certain $i \geqq rm+m\lambda$. Let $\operatorname{ord}_t \rho(g_i(x, y, z)) = s \geqq i$. We shall assume $s < \infty$. Let $s \in u\lambda + mZ$ with $0 \leqq u < m$. Then $s-(rm+u\lambda) \geqq \lambda > n(n+1)m$ by the assumption on λ. Note that $s-(rm+u\lambda) \in mS$ (cf. the property 1) listed in the proof of Theorem 3.1). Since $b_m : W_r \to k^m$ is surjective, then there is a $h(x, y, z) \in W_r$ with $b_m(h(x, y, z)) = (0, 0, \cdots, 0, 1, 0, \cdots, 0)$ which is the $(u+1)$-th element in the standard basis of k^m. Thus $\operatorname{ord}_t \rho(h(x, y, z)) = rm+u\lambda$. Since $s-(rm+u\lambda) \in mS$, then there are β, γ such that $s-(rm+u\lambda) = \beta m(n+1)+\gamma m(n+2)$, or, $\operatorname{ord}_t(\rho(y^\beta z^\gamma)) = \beta m(n+1)+\gamma m(n+2) = s-(rm+u\lambda)$. We have established that $\operatorname{ord}_t \rho(y^\beta z^\gamma h(x, y, z)) = s$ and σ-order of $(y^\beta z^\gamma h(x, y, z)) > r$. Thus for suitable a, one has 1) $\operatorname{ord}_t \rho(g_i(x, y, z) + a y^\beta z^\gamma h(x, y, z)) > s \geqq i$, 2) $\operatorname{ord}_t \rho(a y^\beta z^\gamma h(x, y, z)) = s \geqq i$, 3) σ-leading form of $(g_i(x, y, z) + a y^\beta z^\gamma h(x, y, z))$ is $f(x, y, z)$ and 4) $\operatorname{ord}(a y^\beta z^\gamma h(x, y, z)) \geqq (i-m\lambda)/(m(n+2))$. The inductive process is finished by letting $g_{i+1}(x, y, z) = g_i(x, y, z) + a y^\beta z^\gamma h(x, y, z)$.

To state our next theorem we need the following

NOTATIONS: *Let α be a mapping from $k[[x, y, z]] \to k[[x, y, z]]$ defined by*

$$\alpha(x)=x^{\beta_1}$$
$$\alpha(y)=y^{\beta_2}$$
$$\alpha(z)=z^{\beta_3}$$

with $\beta=\min(\beta_1,\beta_2,\beta_3)$. *Let* ω_i *be the set of all* α*-homogeneous elements of* α*-order* i *in* $k[[x,y,z]]$.

THEOREM 4.3. *Let* Q *be an ideal in* $k[[x,y,z]]$. *Let* $s=\min\{\alpha\text{-order of } f(x,y,z): f(x,y,z)\in Q\}$. *Then the minimum number of generators of* $Q\geqq \sum_i \dim(\omega_i\cap\{\alpha\text{-leading forms of } Q\}\cup\{0\})=r$ *where* $s\leqq i<s+\beta$.

PROOF. Let η be a given number such that there is a set $\{g_1(x,y,z),\cdots,g_\eta(x,y,z)\}$ which generates Q. We shall prove $\eta\geqq r$.

Pick arbitrary $\{f_{i,1}(x,y,z),\cdots,f_{i,d_i}(x,y,z)\}\subset Q$ with α-leading forms of $f_{i,j}(x,y,z)$ form a basis for $\omega_i\cap\{\alpha\text{-leading forms of } Q\}\cup\{0\}$. Note that $r=\sum_{s=i<s+\beta} d_i$. Let the α-leading forms of $g_j(x,y,z)$ be $h_j(x,y,z)$. Let the α-leading forms of $f_{i,j}(x,y,z)$ be $h_{i,j}(x,y,z)$. Since $f_{s,1}(x,y,z),\cdots,f_{s,d_s}(x,y,z)\in Q$, then we have

$$f_{s,j}(x,y,z)=\sum_i u_{i,j}(x,y,z)g_i(x,y,z)\qquad \forall 1\leqq j\leqq d_s.$$

Note that the α-order of $g_i(x,y,z)\geqq s$. By considering α-homogeneous forms of α-order s on both sides we have

$$h_{s,j}(x,y,z)=\sum_i u_{j,i}h_i(x,y,z)$$

where $u_{j,i}$ are constants which are zeroes if the α-order of $h_i(x,y,z)>s$. Hence $\omega_s\cap\{h_i(x,y,z)\}$ generates $\omega_s\cap\{\alpha\text{-leading forms of } Q\}\cup\{0\}$. Let us assume $h_1(x,y,z),\cdots,h_{d_s}(x,y,z)$ form a basis. Replacing $g_j(x,y,z)$ by $g_j+\sum_{1\leqq i\leqq d_s} a_{j,i}g_i$ where $j>d_s$ and $a_{j,i}\in k$, we shall assume the α-order of $g_j(x,y,z)>s$. Note that we have proved $r\geqq d_s$. Inductively let us assume that we have proved that for the given η there is a set $\{g_1,\cdots,g_\eta\}$ which generates Q with

1) $r\geqq \sum_{s\leqq i<s'} d_i$,

2) $\{h_j(x,y,z): \sum_{s\leqq i<\bar{s}-1} d_i<j\leqq \sum_{s\leqq i<\bar{s}} d_i\}$ form a basis for $\omega_{\bar{s}}\cap\{\alpha\text{-leading forms of elements in } Q\}\cup\{0\}$ for all $\bar{s}<s'$,

3) α-order of $g_j(x,y,z)>s'-1\ \forall j>\sum_{s\leqq i<s'} d_i$.

Note that what we proved previously are the above statements for $s'=s+1$. Now we shall finish our inductive process by proving the above statements for $s'+1$. Since $f_{s',j}\in Q\ \forall 1\leqq j\leqq d_{s'}$, then we have

$$f_{s',j}(x,y,z)=\sum_i u_{j,i}(x,y,z)g_i(x,y,z).$$

Suppose for some $i\leqq \sum_{s\leqq i<s'} d_i$, $u_{j,i}(x,y,z)$ is a unit. Let us take the minimum

one. Clearly the α-order of $f_{s',j}(x, y, z)=$ the α-order of $g_i(x, y, z)<s'$ which is impossible. Hence $u_{j,i}(x, y, z)$ must be non-unit for all $i\leqq\sum_{s\leqq i<s'} d_i$ and the α-order of $u_{j,i}(x, y, z)g_i(x, y, z)\geqq\beta+s>s'$. By considering α-homogeneous forms of α-order s' on both sides of the above equation, we have

$$h_{s',j}(x, y, z)=\sum_i u_{j,i}h_i(x, y, z)$$

where $i>\sum_{s\leqq i<s'} d_i$ and $u_{j,i}$ are constants which are zeroes if the α-order of $h_i(x, y, z)>s'$. Hence $\omega_{s'}\cap\{h_i(x, y, z): i>\sum_{s\leqq i<s'} d_i\}$ generates $\omega_{s'}\cap\{\alpha$-leading forms of $Q\}\cup\{0\}$. Let us assume that $\{h_i(x, y, z): \sum_{s\leqq i<s'} d_i<i\leqq\sum_{s\leqq i<s'+1} d_i\}$ forms a basis. Note that 1) and 2) have been established. Replacing $g_j(x, y, z)$ by $g_j(x, y, z)+\sum_i a_{j,i}g_i(x, y, z)$ where $j>\sum_{s\leqq i<s'+1} d_i$, $\sum_{s\leqq i<s'} d_i<i\leqq\sum_{s\leqq i<s'+1} d_i$ and $a_{j,i}\in k$, we shall assume that the α-order of $g_j(x, y, z)>s'$. Q. E. D.

Now we shall prove the theorem listed in § 1 by establishing

THEOREM 4.4. *There are at least n generators for* P_n.

PROOF. In Theorem 4.3 let $\alpha=\sigma$ and $Q=P$. Then $W_r=\omega_r$, $\beta=n$ and $\dim(\omega_i\cap\{\alpha$-leading forms of $Q\}\cup\{0\})=c_i$. Note that it follows from Theorem 4.2 that $s=n(n+1)$. We have the minimum number of generators $\geqq\sum_{s\leqq i<s+n} c_i$ $=n$. Q. E. D.

To finish this article we list several remarks.

REMARK 1. The curves given in this section are ideal theoretically highly non-complete intersections. Are they set theoretic complete intersections?

REMARK 2. From some point of view it is very important to have many examples of curves which are idealtheoretic non-complete intersections to find out a set theoretic one if there is any. What are other examples which share the property of unboundedness of generators?

REMARK 3. M. Hochster suggested that examples of analytically irreducible prime ideals which require a large number of generators probably could be constructed by specializing Macaulay's curves.

REMARK 4. R. Harthorne gave (cf. 3.4.5 of [5]) a prime ideal (of space curves) in $k[[x, y, z]]$ which required 3 generators. J. Herzog extended the above result. In fact he has established (cf. [6]) for a certain class of curves either two or three generators are sufficient while for some members three generators are necessary. Lately J. Roberts had some unpublished examples which included one prime ideal in 7 variables which needed 9 generators, and generally in $(2r-1)$ variables there are prime ideals which need $(r-1)^2$ generators.

REMARK 5. In the construction of $\{P_n\}$ of this section the restriction on m, namely $m=(n+1)/2$, is not necessary. It suffices to pick $m\geqq(n+1)/2$.

Bibliography

[1] S. S. Abhyankar, On Macaulay's examples, Lecture Notes 311, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

[2] R. Apéry, La géométrie algebrique, Bull. Soc. Math. France, **71** (1943), 46-66.

[3] H. Bass, On the ubiquity of Gorenstein rings, Math. Zeit., **82** (1963), 8-28.

[4] D. Gorenstein, An arithmetic theory of adjoint plane curves, Trans. Amer. Math. Soc., **72** (1952), 414-436.

[5] R. Hartshorne, Complete intersections and connectedness, Amer. J. Math., **84** (1962), 497-508.

[6] J. Herzog, Generators and relations of Abelian semigroups and semigroup rings, Manuscript Math., **3** (1970), 175-193.

[7] F. S. Macaulay, Algebraic theory of modular systems, Cambridge Tracts Math., 19 Cambridge University Press, Cambridge, 1916.

[8] O. Zariski and P. Samuel, Commutative algebra I and II, van Nostrand, New York, 1958.

T. T. Moh
School of Mathematics
University of Minnesota
127 Vincent Hall
Mineapolis, Minnesota 55455
U. S. A.