TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 352, Number 4, Pages 1647–1674
S 0002-9947(99)02434-4
Article electronically published on July 26, 1999

A BRACKET POWER CHARACTERIZATION OF ANALYTIC SPREAD ONE IDEALS

L. J. RATLIFF, JR. AND D. E. RUSH

ABSTRACT. The main theorem characterizes, in terms of bracket powers, analytic spread one ideals in local rings. Specifically, let $b_1, \ldots, b_g, x$ be regular nonunits in a local (Noetherian) ring (R, M) and assume that $I \subseteq (xR)_a$, the integral closure of xR, where $I = (b_1, \ldots, b_g, x)R$. Then the main result shows that for all but finitely many units $u_1, \ldots, u_g$ in R that are non-congruent modulo M and for all large integers n and k it holds that $I^{jn} = I^{[j]n}$ for $j = 1, \ldots, k$ and j not divisible by $char(R/M)$, where $I^{[j]}$ is the j-th bracket power $((b_1 + u_1x)^j, \ldots, (b_g + u_gx)^j, x^j)R$ of $I = (b_1 + u_1x, \ldots, b_g + u_gx, x)R$. And, conversely, if there exist positive integers g, n, and $k \geq \binom{n+g}{g}$ such that I has a basis $\beta_1, \ldots, \beta_g, x$ such that $I^{kn} = ({\beta_1}^k, \ldots, {\beta_g}^k, x^k)^n R$, then I has analytic spread one.

1. INTRODUCTION

This paper considers the relationship between the analytic spread $a(I)$ and the equality $I^{[k]n} = I^{kn}$, where I is a regular ideal in a local ring (R, M) and $k \geq 2$ and n are positive integers. Our main result (mentioned in the Abstract) shows that such an equality can be used to characterize when $a(I) = 1$. The proof that an analytic spread one ideal I yields such an equality for all positive integers $k \not\equiv 0 \ mod \ char(R/M)$ (and for a fixed number of basis elements) is quite long; it requires three main steps. The first step, carried out in Section 2, shows that if (R, M) is a local ring such that $char(R/M) > n$, if x is a regular nonunit in R, and if b is an element in R that satisfies an equation of integral dependence on xR of degree n, then for all but finitely many units u in R that are non-congruent modulo M it holds that $b + ux$ satisfies an equation of integral dependence on xR of degree n whose coefficients are all units in R. The second step involves proving a couple of new results concerning superficial elements (since if $I = (\beta_1, \ldots, \beta_g, x)R$ and x is a superficial element for I such that x^k is a superficial element for $I^{[k]}$, then the equality $I^{[k]n} = I^{kn}$, for some positive integers k and n, yields the equality $R[I/x] = R[I^{[k]}/x^k]$ (see (5.6.4)), so $I^{kn} = x^{kn}R[I/x] \cap R = x^{kn}R[I^{[k]}/x^k] \cap R = I^{[k]n}$ for all large integers n); so Section 3 is concerned with superficial elements. The third step is to show that a certain type of large matrices (involving binomial coefficients) is invertible. This third step in itself is quite lengthy and is of independent interest, so

Received by the editors December 20, 1997.
1991 *Mathematics Subject Classification.* Primary 13A15, 13B20, 13C10; Secondary 13H99.
Key words and phrases. Analytic spread, asymptotic prime divisor, binomial coefficient, bracket power of an ideal, essential prime divisor, integral closure of an ideal, local ring, Noetherian ring, persistent prime divisor, prenormal ideal, projectively equivalent ideals, Ratliff-Rush closure of an ideal, reduction of an ideal, superficial element.

the detailed argument that these matrices are invertible is given in [RR2]; however, the details concerned with analytic spread one ideals are given in the proof of (4.1).

On the other hand, the proof that $I^{[k]n} = I^{kn}$ (for some large integer k and with a fixed number of basis elements) implies that $a(I) = 1$ is easy; it consists of counting the number of elements required to generate $I^{[k]n}$ and I^{kn}. (That the number of basis elements be fixed as k varies is important, as shown by (5.5.2).) Therefore, if $char(R/M) = 0$ and $I = (b_1, \ldots, b_g, x)R$, then $a(I) = 1$ if and only if there exists a positive integer n such that for all positive integers k there exists a basis $\beta_1, \ldots, \beta_g, x$ of I such that $I^{jn} = ({\beta_1}^j, \ldots, {\beta_g}^j, x^j)^n R$ for $j = 1, \ldots, k$ (see (4.9)).

(It should probably be mentioned here that the characterization, as given in the Abstract, only holds for regular ideals with a principal reduction. However, the characterization can readily be adjusted to cover all analytic spread one ideals by considering J in place of I, where $J = IR(X)/q$ with q a minimal primary ideal in R.)

The equality $I^{[k]n} = I^{kn}$ for some integer $k \geq 2$ and for all large integers n is equivalent to "$I^{[k]}$ and I^k have the same Ratliff-Rush closure", so in Section 5 we prove a number of new results concerning the Ratliff-Rush closure of I.

In Section 6 we prove two additional converses of (4.4). The first of these is that if $I^{[p]} = I^p$ when $char(R) = p$ (where p is a prime integer), then $a(IR_P) = 1$ holds for all prime ideals P in R that contain I. And the second proves a similar result when it is assumed that (R, M) is a local ring such that $char(R/M) = p$.

In Section 7 we use the results in Section 6 to show that if $char(R)$ is prime, if I is a regular ideal of height at least two, if $\mathbf{P}$ is the set of prime ideals in R that contain I, and if S is a finite subset of $\mathbf{P}$ that contains the essential prime divisors of I, then there exists an ideal J in R that is projectively equivalent to I such that $Ass(R/J^n) = S$ for all positive integers n. Finally, in Section 8 we prove some additional results concerning analytic spread one ideals; these include several additional characterizations of such ideals.

The concept of the analytic spread of an ideal I in a local ring, introduced by D. G. Northcott and D. Rees in [NR], is fundamental to a considerable body of research in commutative algebra. The results in the present paper add to the known properties of analytic spread, and we think these new properties will prove useful to others.

2. Equations of integral dependence

Assume that a nonunit b in a Noetherian ring R is integrally dependent on the ideal generated by a regular nonunit $x \in R$. Then the main result in this section constructs, for each element u in R, an equation of integral dependence of $b + ux$ on xR that is closely related to the given equation of integral dependence of b on xR. To construct this equation, we need the following result concerning sums of products of binomial coefficients.

(2.1) Lemma. *Let n, i, j be positive integers such that $n \geq i$. Then the following hold:*

(2.1.1) $\sum_{k=1}^{j} \binom{n-i+k}{k}(-1)^{j-k+1}\binom{n-i+j}{j-k} = (-1)^j\binom{n-i+j}{j}$.

(2.1.2) *If i is odd, then* $\sum_{k=1}^{i-1} \binom{n-i+k}{k}(-1)^{i-k+1}\binom{n}{i-k} = 0$.

(2.1.3) *If i is even, then* $\sum_{k=1}^{i-1} \binom{n-i+k}{k}(-1)^{i-k+1}\binom{n}{i-k} = 2\binom{n}{i}$.

Proof. For (2.1.1), note that the k-th summand can be written as

$$\frac{(-1)^{j-k+1}(n-i+j)\cdots(n-i+1)}{k!(j-k)!}.$$

Let $X = (n-i+j)\cdots(n-i+1)$ and note that X is independent of k, so

$$\sum_{k=1}^{j}\binom{n-i+k}{k}(-1)^{j-k+1}\binom{n-i+j}{j-k} = X\sum_{k=1}^{j}\frac{(-1)^{j-k+1}}{k!(j-k)!}.$$

Multiply the numerator and denominator of the k-th summand on the right-hand side by $\binom{j}{k}$ and simplify to get $\frac{(-1)^{j-k+1}}{k!(j-k)!} = \frac{(-1)^{j-k+1}\binom{j}{k}}{j!}$. Therefore

$$\sum_{k=1}^{j}\binom{n-i+k}{k}(-1)^{j-k+1}\binom{n-i+j}{j-k} = \frac{X}{j!}\sum_{k=1}^{j}(-1)^{j-k+1}\binom{j}{k}.$$

But

$$\begin{aligned}0 &= (1-1)^j\\ &= \sum_{k=0}^{j}(-1)^{j-k}\binom{j}{k}\\ &= (-1)^j - \sum_{k=1}^{j}(-1)^{j-k+1}\binom{j}{k},\end{aligned}$$

so

$$\sum_{k=1}^{j}(-1)^{j-k+1}\binom{j}{k} = (-1)^j.$$

Therefore

$$\sum_{k=1}^{j}\binom{n-i+k}{k}(-1)^{j-k+1}\binom{n-i+j}{j-k} = \frac{X}{j!}(-1)^j = (-1)^j\binom{n-i+j}{j},$$

so (2.1.1) holds.

For (2.1.2) and (2.1.3), note that the k-th summand can be written as

$$\frac{(-1)^{i-k+1}n(n-1)\cdots(n-i+1)}{k!(i-k)!}.$$

Let $X = n(n-1)\cdots(n-i+1)$ and note that X is independent of k, so

$$\sum_{k=1}^{i-1}\binom{n-i+k}{k}(-1)^{i-k+1}\binom{n}{i-k} = X\sum_{k=1}^{i-1}\frac{(-1)^{i-k+1}}{k!(i-k)!}.$$

Multiply the numerator and denominator of the k-th summand on the right-hand side by $\binom{i}{k}$ and simplify to get $\frac{(-1)^{i-k+1}}{k!(i-k)!} = \frac{(-1)^{i-k+1}\binom{i}{k}}{i!}$. Therefore

$$\sum_{k=1}^{i-1}\binom{n-i+k}{k}(-1)^{i-k+1}\binom{n}{i-k} = \frac{X}{i!}\sum_{k=1}^{i-1}(-1)^{i-k+1}\binom{i}{k}.$$

But

$$\begin{aligned} 0 &= (1-1)^i \\ &= \sum_{k=0}^{i} (-1)^{i-k} \binom{i}{k} \\ &= (-1)^i - \sum_{k=1}^{i-1} (-1)^{i-k+1} \binom{i}{k} + 1, \end{aligned}$$

so it follows that $\sum_{k=1}^{i-1} (-1)^{i-k+1} \binom{i}{k}$ is equal to either 0 (if i is odd) or 2 (if i is even). Therefore

$$\sum_{k=1}^{i-1} \binom{n-i+k}{k} (-1)^{i-k+1} \binom{n}{i-k} = \frac{X}{i!}(e) = \binom{n}{i}(e),$$

where e is equal to either 0 (if i is odd) (so (2.1.2) holds) or 2 (if i is even) (so (2.1.3) holds). □

For (2.3), the main result in this section, we need the following definition.

(2.2) Definition. Let I be an ideal in a ring R. Then I_a denotes the **integral closure in R of I**, so $I_a = \{r \in R;\ r$ is a root of a polynomial of the form $X^n + r_1 X^{n-1} + \cdots + r_n$, where $r_i \in I^i$ for $i = 1, \ldots, n\}$.

(2.3) Theorem. *Let x be a regular nonunit in a Noetherian ring R and let $b \in (xR)_a$, say $b^n = \sum_{i=1}^n r_i x^i b^{n-i}$, where $r_1, \ldots, r_n \in R$. Let T be an indeterminate and for $i = 1, \ldots, n$ let $C_i(T) = (-1)^{i+1}\binom{n}{i} T^i + \sum_{j=0}^{i-1} (-1)^j \binom{n-i+j}{j} r_{i-j} T^j$. Then for each element u in R, $(b+ux)^n = \sum_{i=1}^n C_i(u) x^i (b+ux)^{n-i}$ is an equation of integral dependence of $b+ux$ on xR. Moreover, if R is local with maximal ideal M and if $\mathrm{char}(R/M) > n$, then there exist only finitely many units u in R that are non-congruent modulo M such that $C_i(u) \in M$ for some $i = 1, \ldots, n$.*

Proof. Let $\beta = b + xT$. We will first construct the polynomial equation $\beta^n = \sum_{i=1}^n C_i(T) x^i \beta^{n-1}$, where

$$C_i(T) = (-1)^{i+1} \binom{n}{i} T^i + \sum_{j=0}^{i-1} (-1)^j \binom{n-i+j}{j} r_{i-j} T^j. \tag{2.3.1}$$

(Here, the r_h are the coefficients in the above equation of integral dependence of b on xR.)

For this, raise $\beta = b + xT$ to the n-th power to get

$$\begin{aligned} \beta^n &= b^n + \sum_{j=1}^{n} \binom{n}{j} (xT)^j b^{n-j} \\ &= \sum_{i=1}^{n} r_i x^i b^{n-i} + \sum_{j=1}^{n} \binom{n}{j} (xT)^j b^{n-j}, \end{aligned}$$

since $b^n = \sum_{i=1}^n r_i x^i b^{n-i}$, so

$$\beta^n = \sum_{i=1}^{n} (r_i + \binom{n}{i} T^i) x^i b^{n-i}. \tag{p_0}$$

Let

$$d_{1,j} = r_j + \binom{n}{j} T^j \text{ for } j = 1, \ldots, n,$$

and let

$$C_1(T) = nT + r_1,$$

so $C_1(T) = d_{1,1}$ and $C_1(T)$ is as described by (2.3.1). Also, it follows from (p_0) that

$$(p_0') \qquad \beta^n = C_1(T)xb^{n-1} + \sum_{j=2}^{n} d_{1,j}x^j b^{n-j}.$$

Raise $\beta = b + xT$ to the $n-1$-st power, solve for b^{n-1}, and then substitute this value for b^{n-1} in (p_0') to get

$$\beta^n = C_1(T)x[\beta^{n-1} - \sum_{i=1}^{n-1} \binom{n-1}{i} (xT)^i b^{n-1-i}] + \sum_{j=2}^{n} d_{1,j}x^j b^{n-j},$$

so

$$(p_1) \qquad \beta^n = C_1(T)x\beta^{n-1} + \sum_{j=2}^{n} (d_{1,j} - \binom{n-1}{j-1} C_1(T)T^{j-1})x^j b^{n-j}.$$

Let

$$d_{2,j} = d_{1,j} - \binom{n-1}{j-1} C_1(T)T^{j-1} \text{ for } j = 2, \ldots, n,$$

and let

$$C_2(T) = d_{1,2} - (n-1)C_1(T)T,$$

so

$$\begin{aligned} C_2(T) &= d_{2,2} \\ &= (\binom{n}{2}T^2 + r_2) - ((n-1)(nT + r_1)T) \\ &= (\binom{n}{2} - (n-1)\binom{n}{1})T^2 - (n-1)r_1T + r_2 \\ &= -\binom{n}{2}T^2 - (n-1)r_1T + r_2, \end{aligned}$$

so $C_2(T)$ is as described by (2.3.1). Also, it follows from (p_1) that

$$(p_1') \qquad \beta^n = C_1(T)x\beta^{n-1} + C_2(T)x^2 b^{n-2} + \sum_{j=3}^{n} d_{2,j}x^j b^{n-j}.$$

Raise $\beta = b + xT$ to the $n-2$-nd power, solve for b^{n-2}, and then substitute this value for b^{n-2} in (p_1') to get

$$\beta^n = C_1(T)x\beta^{n-1} + C_2(T)x^2[\beta^{n-2} - \sum_{i=1}^{n-2} \binom{n-2}{i} (xT)^i b^{n-2-i}] + \sum_{j=3}^{n} d_{2,j}x^j b^{n-j},$$

so

$$\beta^n = C_1(T)x\beta^{n-1} + C_2(T)x^2\beta^{n-2} + \sum_{j=3}^{n}(d_{2,j} - \binom{n-2}{j-2}C_2(T)T^{j-2})x^j b^{n-j}. \tag{p_2}$$

Now assume that $i > 2$ and that $C_1(T), \dots, C_{i-1}(T)$ have been constructed by this process (and are as described by (2.3.1)). To construct $C_i(T)$, let

$$d_{i,j} = d_{i-1,j} - \binom{n-(i-1)}{j-(i-1)}C_{i-1}(T)T^{j-(i-1)} \text{ for } j = i, \dots, n,$$

and let

$$C_i(T) = d_{i-1,i} - (n-(i-1))C_{i-1}(T)T,$$

so $C_i(T) = d_{i,i}$.

Now note that if $i \le j \le n$, then

$$\begin{aligned} d_{i.j} &= d_{i-1,j} - \binom{n-i+1}{j-i+1}C_{i-1}(T)T^{j-i+1} \\ &= [d_{i-2,j} - \binom{n-i+2}{j-i+2}C_{i-2}(T)T^{j-i+2}] - \binom{n-i+1}{j-i+1}C_{i-1}(T)T^{j-i+1} \\ &= \cdots \\ &= d_{1,j} - \sum_{k=1}^{i-1}\binom{n-i+k}{j-i+k}C_{i-k}(T)T^{j-i+k} \\ &= [r_j + \binom{n}{j}T^j] - \sum_{k=1}^{i-1}\binom{n-i+k}{j-i+k}C_{i-k}(T)T^{j-i+k}. \end{aligned}$$

In particular, when $j = i$ we have

$$C_i(T) = d_{i,i} = r_i + \binom{n}{i}T^i - \sum_{k=1}^{i-1}\binom{n-i+k}{k}C_{i-k}(T)T^k. \tag{2.3.2}$$

Now it follows from (2.3.2) that, for $j = 1, \dots, i-1$, the coefficient of T^j in $C_i(T)$ is

$$-\sum_{k=1}^{j}\binom{n-i+k}{k}(C_{i-k}(T))_{j-k}, \tag{2.3.3}$$

where $(C_{i-k}(T))_{j-k}$ denotes the coefficient of T^{j-k} in $C_{i-k}(T)$. And, by induction,

$$C_k(T) = (-1)^{k+1}\binom{n}{k}T^k + \sum_{h=0}^{k-1}(-1)^h\binom{n-k+h}{h}r_{k-h}T^h \quad \text{for } k = 1, \dots, i-1. \tag{2.3.4}$$

Therefore it follows from (2.3.4) that

$$(C_{i-k}(T))_{j-k} = (-1)^{j-k}\binom{n-(i-k)+(j-k)}{j-k}r_{(i-k)-(j-k)},$$

so by (2.3.3) the coefficient of T^j in $C_i(T)$ is

$$-\sum_{k=1}^{j}\binom{n-i+k}{k}(-1)^{j-k}\binom{n-i+j}{j-k}r_{i-j}$$
$$=\sum_{k=1}^{j}\binom{n-i+k}{k}(-1)^{j-k+1}\binom{n-i+j}{j-k}r_{i-j}.$$

However, (2.1.1) shows that this coefficient is $(-1)^j\binom{n-i+j}{j}r_{i-j}$, so it follows that for each $j = 1, \ldots, i-1$ the coefficient of T^j in $C_i(T)$ is as described in (2.3.1).

Also, it follows from (2.3.2) that the coefficient of T^i in $C_i(T)$ is

$$\binom{n}{i}-\sum_{k=1}^{i-1}\binom{n-i+k}{k}(C_{i-k}(T))_{i-k}, \tag{2.3.5}$$

and (2.3.4) shows that

$$(C_{i-k}(T))_{i-k}=(-1)^{i-k+1}\binom{n}{i-k},$$

so by (2.3.5) the coefficient of T^i in $C_i(T)$ is

$$\binom{n}{i}-\sum_{k=1}^{i-1}\binom{n-i+k}{k}(-1)^{i-k+1}\binom{n}{i-k}.$$

However, it follows from (2.1.2) and (2.1.3) that this coefficient is $(-1)^{i+1}\binom{n}{i}$, as desired.

Finally, it follows from (2.3.2) that the constant term in $C_i(T)$ is r_i, as desired.

Therefore $\beta^n = \sum_{i=1}^{n} C_i(T)x^i\beta^{n-i}$ with each $C_i(T)$ as described by (2.3.1). Hence, if $u \in R$, then it is clear that

$$(b+ux)^n=\sum_{i=1}^{n}C_i(u)x^i(b+ux)^{n-i}$$

is an equation of integral dependence of $b+ux$ on xR, and, if $char(R/M) > n$, then the leading coefficient $(-1)^{i+1}\binom{n}{i}$ of $C_i(T)$ is not zero, so none of the $C_i(u)$ is the zero polynomial modulo M. Therefore, if S is the set of elements in R/M that are a root of at least one of these n polynomials, then S is a finite set. Thus it follows that there exist only finitely many units u in R that are non-congruent modulo M such that $C_i(u) \in M$ for some $i = 1, \ldots, n$ (namely, the u such that $u + M \in S$). □

(2.4) Remark. Note that if $C_n(u)$ is a unit in (2.3), then it follows that x is integrally dependent on $b+ux$ (and satisfies an equation of integral dependence on $b+ux$ of degree n). Therefore $\frac{b+ux}{x}$ is a unit in $R[\frac{b+ux}{x}]$ and (even stronger) it follows that $R[\frac{b+ux}{x}] = R[\frac{x}{b+ux}]$.

3. Superficial elements

Superficial elements have been useful in many research areas, so there are many results concerning them in the literature. (For basic references, see [N, Section 22] or [ZS2, p. 285].) In this section we prove a couple of new results concerning such elements that are needed to prove the main theorem (4.4). We begin by recalling the appropriate definitions.

(3.1) Definition. Let R be a Noetherian ring, let I be a regular ideal in R, and let $b_1, \ldots, b_g, x$ $(g \geq 1)$ be regular nonunits of R that generate I (note that $b_1, \ldots, b_g, x$ are not assumed to be a minimal generating set for I).
(3.1.1) A **reduction** of I is an ideal $J \subseteq I$ such that $JI^n = I^{n+1}$ for some positive integer n.
(3.1.2) A **regular superficial element** for I is a regular element $b \in I$ such that $I^n : bR = I^{n-1}$ for all large integers n.
(3.1.3) $\mathbf{R}(R, I)$ denotes the **Rees ring of** R **with respect to** I, so $\mathbf{R}(R, I)$ is the graded subring $R[u, tI]$ of $R[u, t]$, where t is an indeterminate and $u = 1/t$.
(3.1.4) A prime ideal P in the Rees ring $R[u, tI]$ is said to be **relevant** in case $tI \not\subseteq P$.
(3.1.5) If R is local with maximal ideal M, then $a(I)$ denotes the **analytic spread** of I, so $a(I) = altitude(\mathbf{R}(R, I)/(u, M)\mathbf{R}(R, I))$.
(3.1.6) For a positive integer k, the k-th **bracket power** of I is the ideal $I^{[k]} = ({b_1}^k, \ldots, {b_g}^k, x^k)R$, and $I^{\langle k \rangle}$ denotes the ideal $(\{b^k;\ b \in I\})R$, so $I^{[k]}$ is the ideal generated by the k-th powers of $b_1, \ldots, b_g, x$ and $I^{\langle k \rangle}$ is the ideal generated by the k-th powers of all elements in I. (It should be noted that $I^{[k]} \subseteq I^{\langle k \rangle} \subseteq I^k$ and that $I^{[k]}$ depends on the generators $b_1, \ldots, b_g, x$ of I, whereas $I^{\langle k \rangle}$ does not.)

Section 5 contains a number of results concerning bracket powers of ideals.

(3.2) Remark (3.2.1). Concerning (3.1.1) and (3.1.6), it is readily checked that $I^{[k]}$ is a reduction of I^k (in fact, $(I^k)^{g+1} = I^{[k]}(I^k)^g$), so $(I^{[k]})_a = (I^k)_a$; hence if R is local, then $a(I^{[k]}) = a(I^k) = a(I)$.
(3.2.2) Concerning (3.1.2), a regular element $b \in I$ is a regular superficial element for I if and only if $bt \notin U = \bigcup\{p;\ p$ is a relevant prime divisor of $u\mathbf{R}(R, I)\}$ (equivalently, $bt \in tI\mathbf{R} - U$).

Proof. For (3.2.2), assume first that $bt \notin U$, so bt is not in any relevant prime divisor of $u^k\mathbf{R}$ for all positive integers k. Fix a large integer k and note that for all large integers n the prime divisors of $u^k\mathbf{R} : (tI)^n\mathbf{R}$ are the relevant prime divisors of $u\mathbf{R}$. Therefore $(u^k\mathbf{R} : (tI)^n\mathbf{R}) : bt\mathbf{R} = u^k\mathbf{R} : (tI)^n\mathbf{R}$, so it follows that $u^{k+n+1}\mathbf{R} : bI^n\mathbf{R} = u^{k+n}\mathbf{R} : I^n\mathbf{R}$ for all large integers n. Contracting this equality of ideals to R yields $I^{k+n+1} : bI^n = I^{k+n} : I^n$. However, $I^{k+n} : I^n = I^k$ for all large integers k, by [RR1, (2.3.2)], so it follows that $I^{k+1} : bR = I^k$ for all large integers k, so b is a regular superficial element for I.

For the converse, assume that bt is in some relevant prime divisor of $u\mathbf{R}$ and fix a large integer k. Then it follows that $(u^k\mathbf{R} : (tI)^n\mathbf{R}) : bt\mathbf{R}$ properly contains $u^k\mathbf{R} : (tI)^n\mathbf{R}$ for all large integers n. Therefore $u^{k+n}\mathbf{R} : I^n\mathbf{R} \subset u^{k+n+1}\mathbf{R} : bI^n\mathbf{R}$, so (since these ideals are homogeneous) there exists a homogeneous element $rt^m \in (u^{k+n+1}\mathbf{R} : bI^n\mathbf{R}) - (u^{k+n}\mathbf{R} : I^n\mathbf{R})$. (Note that there is such an element rt^m for all positive integers m. To see this, let n be a large integer and fix $m \geq 1$. Then if $(tI)^m\mathbf{R} \cap (u^k\mathbf{R} : bt(tI)^n\mathbf{R}) \subseteq u^k\mathbf{R} : (tI)^n\mathbf{R}$, then $((tI)^m\mathbf{R})(u^k\mathbf{R} : bt(tI)^n\mathbf{R}) \subseteq u^k\mathbf{R} : (tI)^n\mathbf{R}$ and $(tI)^m\mathbf{R}$ is not contained in any prime divisor of $u^k\mathbf{R} : (tI)^n\mathbf{R}$, so $u^k\mathbf{R} : bt(tI)^n\mathbf{R}$ is contained in each primary component of $u^k\mathbf{R} : (tI)^n\mathbf{R}$, and this contradicts the fact that $(u^k\mathbf{R} : (tI)^n\mathbf{R}) : bt\mathbf{R}$ properly contains $u^k\mathbf{R} : (tI)^n\mathbf{R}$ for all large integers n.) It then follows that $rbI^n \subseteq u^{k+n+1+m}\mathbf{R} \cap R = I^{k+n+1+m}$ and that $rI^n \not\subseteq u^{k+n+m}\mathbf{R} \cap R = I^{k+n+m}$. Therefore $rb \in I^{k+1+m+n} : I^n = I^{k+1+m}$ (by [RR1, (2.3.2)], since k is large) and $r \notin I^{k+m+n} : I^n = I^{k+m}$, so b is not a superficial element for I. □

(3.3) Lemma. *Let (R, M) be a local ring such that R/M is infinite and let I be a regular ideal in R. Fix a positive integer k. Then there exists a regular superficial element b for I such that b^k is a regular superficial element for $I^{\langle k\rangle}$.*

Proof. Let $\mathbf{R} = R[u, tI]$ and $\mathbf{R}_k = R[u^k, t^k I^{\langle k\rangle}]$, so $\mathbf{R}_k \cong \mathbf{R}(R, I^{\langle k\rangle})$ and $\mathbf{R}$ contains and is integrally dependent on $\mathbf{R}_k$. Let $p_1, \ldots, p_h$ be the prime ideals in $\mathbf{R}$ that are either a relevant prime divisor of $u\mathbf{R}$ or that lie over a relevant prime divisor of $u^k\mathbf{R}_k$. (Note: since R is local, I is regular, and u is regular in $\mathbf{R}$, it follows that each prime divisor of zero in both $\mathbf{R}$ and $\mathbf{R}_k$ is contained in at least one of the p_i. Also note that relevant prime ideals in $\mathbf{R}$ contract to relevant prime ideals in $\mathbf{R}_k$.) Then since R/M is infinite there exists a (regular) element $bt \in \mathbf{R}$ that is not in any of these prime ideals. Therefore it follows from (3.2.2) (and from $\mathbf{R}_k \cong \mathbf{R}(R, I^{\langle k\rangle})$) that b (resp., b^k) is a regular superficial element for I (resp., $I^{\langle k\rangle}$). □

By starting with a given basis $b_1, \ldots, b_g, x$ for I, we do not know how to prove the result corresponding to (3.3) for $I^{[k]}$ in place of $I^{\langle k\rangle}$. The difficulty is, of course, that b^k may not be in $I^{[k]}$. However, (3.4) shows that (3.3) can be strengthened to include several different values of k simultaneously, and (3.7) shows that we can often find such an element b for $I^{[k]}$ in place of $I^{\langle k\rangle}$ when $a(I) = 1$.

(3.4) Remark. A proof similar to that given for (3.3) shows that, if k is a given positive integer, then (since $\mathbf{R}$ is integrally dependent on each of the rings $\mathbf{R}_i = R[u^i, t^i I^{\langle i\rangle}] \cong \mathbf{R}(R, I^{\langle i\rangle})$ for $i = 1, \ldots, k$) by letting $p_1, \ldots, p_w$ be the prime ideals in $\mathbf{R}$ that are either a relevant prime divisor of $u\mathbf{R}$ or that lie over a relevant prime divisor of $u^i\mathbf{R}_i$ for at least one $i = 2, \ldots, k$, there exists a regular superficial element b for I such that b^i is a regular superficial element for $I^{\langle i\rangle}$ for $i = 2, \ldots, k$.

(3.5) Lemma. *If b is a regular superficial element for a regular ideal I in a Noetherian ring R, and if $A = R[I/b]$, then $b^n A \cap R = I^n$ for all large integers n.*

Proof. Let b be a regular superficial element for I and let n be large enough that $I^i : bR = I^{i-1}$ for all integers $i \geq n$. Then if $r \in b^n A \cap R$, then there exist a positive integer m and an element $\alpha \in I^m$ such that $r = b^n(\alpha/b^m)$. If $n \geq m$, then $r = b^{n-m}\alpha \in I^n$, and if $n < m$, then $b^{m-n}r = \alpha \in I^m$, so $r \in I^m : b^{m-n}R = I^n$. Therefore $b^n A \cap R \subseteq I^n$ for all large integers n, and the opposite inclusion is clear; hence $b^n A \cap R = I^n$ for all large integers n. □

We close this section with two more results concerning superficial elements. (It should be noted that the hypotheses in (3.6) that I has a principal reduction does hold when R/M is infinite and $a(I) = 1$.)

(3.6) Proposition. *Let (R, M) be a local ring, let I be a regular ideal in R, and assume that I has a reduction generated by one element. Then for each reduction cR of I, c is a regular superficial element for I.*

Proof. Let cR be a reduction of I. Then c is regular in R (since I is regular and $I^{m+1} = cI^m \subseteq cR$ for some positive integer m), and there exists a positive integer n such that $I^{m+1} = cI^m$ for all integers $m \geq n$. Therefore $I^{m+1} : cR = cI^m : cR = I^m$ for all integers $m \geq n$, so c is a regular superficial element for I. □

(3.7) Corollary. *Let (R, M) be a local ring, let $I = (b_1, \ldots, b_g, x)R$ be a regular ideal in R, and assume that $I \subseteq (xR)_a$. Then for each integer $k \geq 1$ it holds that $x^k R$ is a reduction of $I^{[k]} = ({b_1}^k, \ldots, {b_g}^k, x^k)R$ and that x^k is a regular superficial*

element for $I^{[k]}$. Moreover, if n_i is an integer such that $(b_i, x)^{n_i}R = x(b_i, x)^{n_i-1}R$ for $i = 1, \ldots, g$, if $n^* = (\sum_{i=1}^{g} n_i) - g$, and if $A = R[b_1/x, \ldots, b_g/x]$, then $x^nA = x^nA \cap R = I^n$ for all integers $n \geq n^*$.

Proof. It is clear that $x^k \in I^{[k]} \subseteq I^k \subseteq (x^kR)_a$, so x^kR is a reduction of $I^{[k]}$, so x^k is a regular superficial element for $I^{[k]}$, by (3.6).

For the last statement of the corollary, note that it follows from the definition of n^* that $I^n = x^{n-n^*}I^{n^*}$ for all integers $n \geq n^*$. Also, A is integrally dependent on R, since each b_i/x is integral over R, so A is a finite R-module. In fact, since $I^n = x^{n-n^*}I^{n^*}$, it follows that each element in A can be written in the form β/x^{n^*} for some $\beta \in I^{n^*}$, so it readily follows that $x^nA = x^nA \cap R = I^n$ for all integers $n \geq n^*$. □

4. The main theorem

In this section we prove the main theorem and a couple of useful related results.

Our first result in this section is the case $g = 1$ and $k \geq 2$ of the main theorem, that is, the case where $I = (b, x)R$.

(4.1) Theorem. *Let b and x be regular nonunits in a local ring (R, M) such that b is integrally dependent on xR, say $b^n = \sum_{i=1}^{n} r_i x^i b^{n-i}$, where $r_1, \ldots, r_n \in R$. Let $k \geq 2$ be an integer that is not divisible by $char(R/M)$. Then for all but finitely many units u in R that are non-congruent modulo M it holds that:*

(4.1.1) *$(b, x)^{jn}R = (b + ux, x)^{jn}R = x^j((b + ux)^j, x^j)^{n-1}R$ for $j = 1, \ldots, k$ and $j \not\equiv 0$ mod $char(R/M)$.*

(4.1.2) *$(b, x)^{j(n-1)}R = (b + ux, x)^{j(n-1)}R = ((b + ux)^j, x^j)^{n-1}R$ for $j = 1, \ldots, k$ and $j \not\equiv 0$ mod $char(R/M)$.*

Proof. Let $\beta = b + xT$, where T is an indeterminate, so the proof of (2.3) shows that $\beta^n = \sum_{i=1}^{n} C_i(T)x^i\beta^{n-i}$, where $C_i(T) = (-1)^{i+1}\binom{n}{i}T^i + \sum_{j=0}^{i-1}(-1)^j\binom{n-i+j}{j}r_{i-j}T^j$. (Here, we do not need to assume that $char(R/M) > n$ (see (2.3)), since we are not trying to make all the coefficients $C_1(u), \ldots, C_n(u)$ units in R. Our goal will be to choose u so that $Det(H_{n,k}{}^*)$ (see (4.1.4)) is a unit in R/M, and for this we will only require that k is not divisible by $char(R/M)$; see the proof of (4.1.4) and the paragraph that follows its proof.)

Let $s = kn - n$ and successively multiply both sides of the equation $\beta^n = \sum_{i=1}^{n} C_i(T)x^i\beta^{n-i}$ by β^s, $x\beta^{s-1}$, …, $x^{s-1}\beta, x^s$ to obtain the $s + 1$ equations:

$$\beta^{n+s} = \sum_{i=1}^{n} C_i(T)x^i\beta^{n-i+s},$$

$$x\beta^{n+s-1} = \sum_{i=1}^{n} C_i(T)x^{i+1}\beta^{n-i+s-1},$$

$$\cdots$$

$$x^{s-1}\beta^{n+1} = \sum_{i=1}^{n} C_i(T)x^{i+s-1}\beta^{n+1-i},$$

$$x^s\beta^n = \sum_{i=1}^{n} C_i(T)x^{i+s}\beta^{n-i}.$$

(Note that $n + s = kn$, so when T is replaced by any unit u in R these $s + 1$ equations involve the $kn + 1$ generators $(b + ux)^{kn}, x(b + ux)^{kn-1}, \ldots, x^{kn-1}(b + ux), x^{kn}$ of $(b + ux, x)^{kn}R$.)

Rewrite each of these $s + 1$ equations with the n terms involving $x^{ki}\beta^{k(n-i)}$ $(i = 1, \ldots, n)$ on the right-hand side and the remaining $s + 1 = (kn + 1) - n$ terms on the left-hand side. Now view these equations in this form as the system $H_{n,k}(T)Y = G$ of $s+1$ linear equations in the $s+1$ variables in the set $\{x^i\beta^{kn-i};\ i = 1, \ldots, kn-1$ and $i \not\equiv 0\ mod\ k\} \cup \{\beta^{kn}\}$. Here: Y is the $s+1$-tuple (column vector) $(\beta^{kn}, x\beta^{kn-1}, \ldots, x^i\beta^{kn-i}, \ldots, x^{kn-1}\beta)^t$ (with $i = 1, \ldots, kn-1$ and $i \not\equiv 0\ mod\ k$); G is the the $s + 1$-tuple (column vector) $(g_1, \ldots, g_{s+1})^t$, where g_j is the sum of the terms of the j-th equation involving $x^{kn}, x^{k(n-1)}\beta^k, \ldots, x^k\beta^{n+s-k}$ (including the coefficients $C_1, \ldots, C_n$ (and -1 for $j = k+1, 2k+1, \ldots$)) (so each g_j becomes a linear combination of the generators of $x^k((b + ux)^k, x^k)^{n-1}R$ when $b + ux$ is substituted for β); and, $H_{n,k}(T)$ is the $s + 1$ by $s + 1$ coefficient matrix, which is obtained as follows:

(4.1.3) Construction. *Fix integers $n \geq 2$ and $k \geq 2$, let $s = kn - n$, and let $m = kn+1$. Let A_0 be the $s+1$ by m matrix whose first row is $-1\ C_1(T)\ C_2(T)\ \ldots\ C_n(T)$ followed by $kn - n$ zeros (so the row has m entries), whose second row consists of* 0 *followed by the first row with its last* 0 *deleted, whose third row consists of* 0 *followed by the second row with its last* 0 *deleted, ..., and whose $s + 1$-st row consists of* 0 *followed by the s-th row with its last* 0 *deleted. (Note that column j of A_0 contains the coefficients of $x^{j-1}\beta^{kn-(j-1)}$ in the above equations rewritten in the form $-x^h\beta^{kn-h} + \sum_{i=1}^{n} C_i(T)x^{i+h}\beta^{kn-i-h} = 0$.) Then $H_{n,k}(T)$ is the $s+1$ by $s+1$ matrix obtained by deleting columns $k+1, 2k+1, \ldots, nk+1 = m$ from A_0 (so the n columns that involve the coefficients of the elements $\beta^{k(n-i)}x^{ki}$ $(i = 1, \ldots, n)$ are deleted), leaving $s + 1$ columns.*

The following are three examples of $H_{n,k}(T)$. The first is $H_{n,2}(T)$ with n even (so $H_{n,2}(T)$ is an $n + 1$ by $n + 1$ matrix); the second is $H_{n,2}(T)$ with n odd (so $H_{n,2}(T)$ is an $n + 1$ by $n + 1$ matrix); and the third is $H_{n,n+1}(T)$ (so $H_{n,n+1}(T)$ is an $n^2 + 1$ by $n^2 + 1$ matrix).

For n even:

$$H_{n,2}(T) = \begin{pmatrix} -1 & C_1(T) & C_3(T) & C_5(T) & \ldots & C_{n-1}(T) & 0 & 0 & \ldots & 0 & 0 \\ 0 & -1 & C_2(T) & C_4(T) & \ldots & C_{n-2}(T) & C_n(T) & 0 & \ldots & 0 & 0 \\ 0 & 0 & C_1(T) & C_3(T) & \ldots & C_{n-3}(T) & C_{n-1}(T) & 0 & \ldots & 0 & 0 \\ 0 & 0 & -1 & C_2(T) & \ldots & C_{n-4}(T) & C_{n-2}(T) & C_n(T) & \ldots & 0 & 0 \\ 0 & 0 & 0 & C_1(T) & \ldots & C_{n-5}(T) & C_{n-3}(T) & C_{n-1}(T) & \ldots & 0 & 0 \\ 0 & 0 & 0 & -1 & \ldots & C_{n-6}(T) & C_{n-4}(T) & C_{n-2}(T) & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & & & & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \ldots & C_1(T) & C_3(T) & C_5(T) & \ldots & C_{n-1}(T) & 0 \\ 0 & 0 & 0 & 0 & \ldots & -1 & C_2(T) & C_4(T) & \ldots & C_{n-2}(T) & C_n(T) \\ 0 & 0 & 0 & 0 & \ldots & 0 & C_1(T) & C_3(T) & \ldots & C_{n-3}(T) & C_{n-1}(T) \end{pmatrix}.$$

For n odd:

$$H_{n,2}(T) = \begin{pmatrix} -1 & C_1(T) & C_3(T) & C_5(T) & \dots & C_n(T) & 0 & 0 & \dots & 0 \\ 0 & -1 & C_2(T) & C_4(T) & \dots & C_{n-1}(T) & 0 & 0 & \dots & 0 \\ 0 & 0 & C_1(T) & C_3(T) & \dots & C_{n-2}(T) & C_n(T) & 0 & \dots & 0 \\ 0 & 0 & -1 & C_2(T) & \dots & C_{n-3}(T) & C_{n-1}(T) & 0 & \dots & 0 \\ 0 & 0 & 0 & C_1(T) & \dots & C_{n-4}(T) & C_{n-2}(T) & C_n(T) & \dots & 0 \\ 0 & 0 & 0 & -1 & \dots & C_{n-5}(T) & C_{n-3}(T) & C_{n-1}(T) & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & C_1(T) & C_3(T) & C_5(T) & \dots & C_n(T) \\ 0 & 0 & 0 & 0 & \dots & -1 & C_2(T) & C_4(T) & \dots & C_{n-1}(T) \end{pmatrix},$$

$$H_{n,n+1}(T) = \begin{pmatrix} -1 & C_1(T) & C_2(T) & \dots & C_n(T) & 0 & 0 \dots 0\,0 & 0 & \dots & 0 & 0 \\ 0 & -1 & C_1(T) & \dots & C_{n-1}(T) & 0 & 0 \dots 0\,0 & 0 & \dots & 0 & 0 \\ 0 & 0 & -1 & \dots & C_{n-2}(T) & C_n(T) & 0 \dots 0\,0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & & & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \dots 0\,0 & C_1(T) & \dots & C_{n-1}(T) & C_n(T) \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \dots 0\,0 & -1 & \dots & C_{n-2}(T) & C_{n-1}(T) \end{pmatrix}.$$

Now consider the matrix $H_{n,k}(T)$ modulo M, and recall that each $C_i(T)$ is a polynomial in T of degree i whose leading coefficient is $(-1)^{i+1}\binom{n}{i}$. It follows from this that $Det(H_{n,k}(T))$ is a polynomial $P(T)$; in fact, the following holds:

(4.1.4) $$Det(H_{n,k}(T)) \text{ is a polynomial of degree } \frac{n(n-1)(k-1)}{2} \text{ whose leading coefficient is } Det({H_{n,k}}^*),$$

where ${H_{n,k}}^*$ is the $s+1$ by $s+1$ matrix obtained from $H_{n,k}(T)$ by substituting the leading coefficient $(-1)^{i+1}\binom{n}{i}$ of C_i for C_i (for $i = 0, 1, \dots, n$). (In the three cases above:

For n even:

$${H_{n,2}}^* = \begin{pmatrix} -\binom{n}{0} & \binom{n}{1} & \binom{n}{3} & \binom{n}{5} & \dots & \binom{n}{n-1} & 0 & 0 & \dots & 0 & 0 \\ 0 & -\binom{n}{0} & -\binom{n}{2} & -\binom{n}{4} & \dots & -\binom{n}{n-2} & -\binom{n}{n} & 0 & \dots & 0 & 0 \\ 0 & 0 & \binom{n}{1} & \binom{n}{3} & \dots & \binom{n}{n-3} & \binom{n}{n-1} & 0 & \dots & 0 & 0 \\ 0 & 0 & -\binom{n}{0} & -\binom{n}{2} & \dots & -\binom{n}{n-4} & -\binom{n}{n-2} & -\binom{n}{n} & \dots & 0 & 0 \\ 0 & 0 & 0 & \binom{n}{1} & \dots & \binom{n}{n-5} & \binom{n}{n-3} & \binom{n}{n-1} & \dots & 0 & 0 \\ 0 & 0 & 0 & -\binom{n}{0} & \dots & -\binom{n}{n-6} & -\binom{n}{n-4} & -\binom{n}{n-2} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & & & & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & \binom{n}{1} & \binom{n}{3} & \binom{n}{5} & \dots & \binom{n}{n-1} & 0 \\ 0 & 0 & 0 & 0 & \dots & -\binom{n}{0} & -\binom{n}{2} & -\binom{n}{4} & \dots & -\binom{n}{n-2} & -\binom{n}{n} \\ 0 & 0 & 0 & 0 & \dots & 0 & \binom{n}{1} & \binom{n}{3} & \dots & \binom{n}{n-3} & \binom{n}{n-1} \end{pmatrix}.$$

For n odd:

$${H_{n,2}}^* = \begin{pmatrix} -\binom{n}{0} & \binom{n}{1} & \binom{n}{3} & \binom{n}{5} & \dots & \binom{n}{n} & 0 & 0 & \dots & 0 \\ 0 & -\binom{n}{0} & -\binom{n}{2} & -\binom{n}{4} & \dots & -\binom{n}{n-1} & 0 & 0 & \dots & 0 \\ 0 & 0 & \binom{n}{1} & \binom{n}{3} & \dots & \binom{n}{n-2} & \binom{n}{n} & 0 & \dots & 0 \\ 0 & 0 & -\binom{n}{0} & -\binom{n}{2} & \dots & -\binom{n}{n-3} & -\binom{n}{n-1} & 0 & \dots & 0 \\ 0 & 0 & 0 & \binom{n}{1} & \dots & \binom{n}{n-4} & \binom{n}{n-2} & \binom{n}{n} & \dots & 0 \\ 0 & 0 & 0 & -\binom{n}{0} & \dots & -\binom{n}{n-5} & -\binom{n}{n-3} & -\binom{n}{n-1} & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \binom{n}{1} & \binom{n}{3} & \binom{n}{5} & \dots & \binom{n}{n} \\ 0 & 0 & 0 & 0 & \dots & -\binom{n}{0} & -\binom{n}{2} & -\binom{n}{4} & \dots & -\binom{n}{n-1} \end{pmatrix}.$$

$$H_{n,n+1}{}^* = \begin{pmatrix} -\binom{n}{0} & \binom{n}{1} & -\binom{n}{2} & \dots & (-1)^{n+1}\binom{n}{n} & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & -\binom{n}{0} & \binom{n}{1} & \dots & (-1)^{n}\binom{n}{n-1} & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & 0 & -\binom{n}{0} & \dots & (-1)^{n-1}\binom{n}{n-2} & (-1)^{n+1}\binom{n}{n} & \dots & 0 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & & & \vdots & & \vdots & & \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & \binom{n}{1} & \dots & (-1)^{n}\binom{n}{n-1} & (-1)^{n+1}\binom{n}{n} \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & -\binom{n}{0} & \dots & (-1)^{n-1}\binom{n}{n-2} & (-1)^{n}\binom{n}{n-1} \end{pmatrix}.$$

To prove (4.1.4), let A_1 be the $kn+1$ by $kn+1$ matrix obtained by adjoining to the bottom of A_0 in (4.1.3) the n rows e_{ik+1} $(i = 1, \dots, n)$, where e_{ik+1} is the $kn+1$-tuple whose only nonzero entry is 1 in the $ik+1$-st component. Then it is readily seen that $Det(A_1) = \pm Det(H_{n,k}(T))$ (by expanding the determinant of A_1 by its last row to get the kn by kn matrix B_1 obtained by deleting the last row and column of A_1, so $Det(B_1) = Det(A_1)$; then expand the determinant of B_1 by its last row to get the matrix B_2 obtained by deleting the last row and the $(n-1)k+1$-st column of B_1, so $Det(B_2) = (-1)^{kn+(n-1)k+1}Det(B_1)$; and repeat this $n-2$ more times). Therefore to prove (4.1.4) it is sufficient to prove that each nonzero summand of $Det(A_1)$ has degree $\frac{n(n-1)(k-1)}{2}$.

For this, note first that it follows from (4.1.3) that, for $i = 1, \dots, kn-n+1$ and $j = i, \dots, k+n$, the (i,j)-entry of A_1 is C_{j-i} (with $C_0 = -1$), so this entry has degree $j-i$; the other entries of rows $i = 1, \dots, kn-n+1$ are zero. Also, the only nonzero entry in each of the last n rows is the 1 in the $ik+1$-st component (for $i = 1, \dots, n$). Therefore let $a_{1,i_1} \cdots a_{kn+1,i_{kn+1}}$ be a nonzero summand of $Det(A_1)$. Then $a_{1,i_1} \cdots a_{kn+1.i_{kn+1}} = C_{i_1-1} \cdots C_{i_{kn-n+1}-(kn-n+1)} 1 \cdots 1$ (there are n 1's). Therefore the degree of this summand is $(i_1-1)+\cdots+(i_{kn-n+1}-(kn-n+1))$ $= \sum_{j=1}^{kn-n+1} i_j - \sum_{j=1}^{kn-n+1} j$. However, since this is a nonzero summand and since, for $i = 1, \dots, n$, the $kn-n+1+i$-th row has its only nonzero entry $(= 1)$ in the $ik+1$-st component, it follows that the columns $i_1, \dots, i_{kn-n+1}$ must be the columns in $\{1, 2, \dots, kn+1\} - \{k+1, 2k+1, \dots, kn+1\}$. Therefore it follows that the degree of this summand is

$$\sum_{j=1}^{kn-n+1} i_j - \sum_{j=1}^{kn-n+1} j = ((\sum_{j=1}^{kn+1} j) - \frac{n(n+1)k}{2} + n) - \sum_{j=1}^{kn-n+1} j,$$

which simplifies to $\frac{n(n-1)(k-1)}{2}$. Since this is the degree of each nonzero summand of $Det(A_1)$, it follows that $Det(H_{n,k}(T))$ is a polynomial whose leading coefficient is $Det(H^*_{n,k})$, so (4.1.4) holds.

Now it is proved in [RR2, Corollary 2.6] that if $char(R/M) = 0$, then $Det(H_{n,k}{}^*)$ $= \pm k^{t_{n-1}}$ (since $k+1, 2k+1, \dots, kn+1$ is an arithmetic sequence); here, $t_{n-1} = \binom{n}{2}$ is the $n-1$-st triangular number (so t_{n-1} is the $n-1$-st integer in the sequence $1, 3, 6, 10, 15, \dots$). Since determinants are computed the same way over any commutative ring (as a sum of products of elements in the ring), it follows that if $char(R/M) = p \neq 0$ and $k \not\equiv 0 \ mod\ p$, then the leading coefficient of $P(T) = Det(H_{n,k}(T))$ is $Det(H_{n,k}{}^*) = \pm k^{t_{n-1}} \ mod\ p$, which is nonzero in R/M. Therefore this polynomial has only finitely many zeros (in fact, it has at most $\frac{n(n-1)(k-1)}{2}$ zeros, by (4.1.4)), so there exist only finitely many units u in R that are non-congruent modulo M such that $Det(H_{n,k}(u))$ is a nonunit in R. Hence if u is chosen to be none of these units in R, then $H_{n,k}(u)$ is invertible, so there exists a unique solution to the system $H_{n,k}(u)Y = G$ of linear equations.

Therefore it follows that the elements in $\{x^i(b+ux)^{kn-i};\ i=1,\dots,kn-1$ and $i \not\equiv 0\ mod\ k\} \cup \{(b+ux)^{kn}\}$ are in the ideal generated in R by the components of G when $b+ux$ is substituted for β, and it is clear that this latter ideal is contained in $x^k((b+ux)^k, x^k)^{n-1}R$, so $(b+ux,x)^{kn}R \subseteq x^k((b+ux)^k,x^k)^{n-1}R$. Since the opposite inclusion is clear, it follows that $(b+ux,x)^{kn}R = x^k((b+ux)^k,x^k)^{n-1}R$, and it is clear that $(b+ux,x)^{kn}R = (b,x)^{kn}R$.

Since the preceding holds for each integer $k \geq 2$ that is not divisible by $char(R/M)$ (that is, since there are only finitely many units u in R that are non-congruent modulo M such that $Det(H_{n,k}(u))$ is a nonunit in R), it follows that if $k \geq 2$, then there are only finitely many units u in R that are non-congruent modulo M such that $Det(H_{n,j}(u))$ is a nonunit in R for $j = 2,3,\dots,k$ and $j \not\equiv 0\ mod\ char(R/M)$. Therefore for all but finitely many units u in R that are non-congruent modulo M it holds that

$$(b,x)^{jn}R = (b+ux,x)^{jn}R = x^j((b+ux)^j,x^j)^{n-1}R$$

for $j = 1,\dots,k$ and $j \not\equiv 0\ mod\ char(R/M)$. Therefore (4.1.1) holds.

Finally, since $(b,x)^nR = x(b,x)^{n-1}R$, it follows that $(b,x)^{jn}R = x^j(b,x)^{j(n-1)}R$, so since x is regular in R it follows from what was shown in the preceding paragraph that $(b,x)^{j(n-1)}R = (b+ux,x)^{j(n-1)}R = ((b+ux)^j,x^j)^{n-1}R$ for $j = 1,\dots,k$ and $j \not\equiv 0\ mod\ char(R/M)$; hence (4.1.2) holds. □

(4.2) Remark. Concerning (4.1), it should be noted that the conclusion can be changed to: if $k \geq 2$ and $m \geq n-1$, then for all but finitely many units u in R that are non-congruent modulo M it holds that $(b,x)^{mj}R = (b+ux,x)^{mj}R = ((b+ux)^j,x^j)^mR$ for $j = 1,\dots,k$ and $j \not\equiv 0\ mod\ char(R/M)$. (This follows from the fact that if $b^n = \sum_{i=1}^n r_i x^i b^{n-i}$, then $b^m = \sum_{i=1}^m r_i x^i b^{m-i}$, where $r_{n+1},\dots,r_m$ are zero.)

(4.3) Corollary. *Let b and x be regular nonunits in a local ring (R,M) such that $b^2 = r_1xb + r_2x^2$ for some r_1, r_2 in R. Let $k \geq 2$ be an integer. Then for all but finitely many units u in R that are non-congruent modulo M it holds that $(b,x)^jR = (b+ux,x)^jR = ((b+ux)^j,x^j)R$ for $j = 1,\dots,k$ and $j \not\equiv 0\ mod\ char(R/M)$.*

Proof. This is the case $n = 2$ of (4.1.2). □

We can now prove the main theorem in this section.

(4.4) Theorem. *Let $b_1,\dots,b_g,x$ be regular nonunits in a local ring (R,M), let $I = (b_1,\dots,b_g,x)R$, and assume that $a(I) = 1$ and that $I \subseteq (xR)_a$, say $(b_i,x)^{n_i}R = x(b_i,x)^{n_i-1}R$ for $i = 1,\dots,g$. Let $n^* = (\sum_{j=1}^g n_j) - g$ and let $k \geq 2$ be an integer. Then for all but finitely many units $u_1,\dots,u_g$ in R that are non-congruent modulo M it holds that*

$$I^{jn} = (b_1+u_1x,\dots,b_g+u_gx,x)^{jn}R = ((b_1+u_1x)^j,\dots,(b_g+u_gx)^j,x^j)^nR$$

for all integers $n \geq n^*$ and for $j = 1,\dots,k$ and $j \not\equiv 0\ mod\ char(R/M)$.

Proof. Fix $h \in \{1,\dots,g\}$. Then the hypothesis implies that ${b_h}^{n_h} = \sum_{i=1}^{n_h} r_i x^i {b_h}^{n_h-i}$, where $r_1,\dots,r_{n_h} \in R$. Therefore (4.1.2) shows that for all but finitely many units u in R that are non-congruent modulo M it holds that

$$(b_h,x)^{j(n_h-1)}R = (b_h+ux,x)^{j(n_h-1)}R = ((b_h+ux)^j,x^j)^{n_h-1}R$$

for $j = 1, \dots, k$ and $j \not\equiv 0$ *mod* $char(R/M)$. Therefore (3.7) shows that $R[\beta_h/x] = R[{\beta_h}^j/x^j]$ for $j = 1, \dots, k$ *and* $j \not\equiv 0$ *mod* $char(R/M)$, where $\beta_h = b_h + ux$, and it is clear that $R[b_h/x] = R[\beta_h/x]$, so

$$R[b_h/x] = R[\beta_h/x] = R[{\beta_h}^j/x^j] \quad \text{for } j = 1, \dots, k \text{ and } j \not\equiv 0 \text{ mod } char(R/M). \tag{4.4.1}$$

Let $A = R[b_1/x, \dots, b_g/x]$. Then it follows from (4.4.1) that

$$A = R[\beta_1/x, \dots, \beta_g/x] = R[{\beta_1}^j/x^j, \dots, {\beta_g}^j/x^j] \quad \text{for } j = 1, \dots, k \text{ and } j \not\equiv 0 \text{ mod } char(R/M). \tag{4.4.2}$$

Also, it is clear that $(\beta_1, \dots, \beta_g, x)R = I$. Therefore, since xR is a reduction of I, (3.7) shows that xR (resp., x^jR) is a regular superficial element for I (resp., $({\beta_1}^j, \dots, {\beta_g}^j, x^j)R$) and that $x^nA = x^nA \cap R = I^n$ for all integers $n \geq n^*$.

Moreover, (4.1.1) shows that $({\beta_i}^j, x^j)^{n_i}R = x^j({\beta_i}^j, x^j)^{n_i - 1}R$ for $i = 1, \dots, g$ and $j = 1, \dots, k$ and $j \not\equiv 0$ *mod* $char(R/M)$. Therefore, since x^j is a regular superficial element for $({\beta_1}^j, \dots, {\beta_g}^j, x^j)R$ for $j = 1, \dots, k$ (by the preceding paragraph), it follows from (3.7) (with x^j and $I^{[j]}$ in place of x and I) and (4.4.2) that $x^{jn}A = x^{jn}A \cap R = ({\beta_1}^j, \dots, {\beta_g}^j, x^j)^nR$ for all integers $n \geq n^*$. Therefore it follows from what was shown at the end of the preceding paragraph that

$$I^{jn} = (b_1 + u_1x, \dots, b_g + u_gx, x)^{jn}R = ((b_1 + u_1x)^j, \dots, (b_g + u_gx)^j, x^j)^nR$$

for all integers $n \geq n^*$ and for $j = 1, \dots, k$ and $j \not\equiv 0$ *mod* $char(R/M)$. □

(4.5) Corollary. *Let $b_1, \dots, b_g, x$ be regular nonunits in a local ring (R, M), let $I = (b_1, \dots, b_g, x)R$, and assume that $a(I) = 1$ and that $I \subseteq (xR)_a$. Let $A = R[I/x]$. Then for all integers $k \geq 2$ that are not divisible by $char(R/M)$ there exists a basis $\beta_1, \dots, \beta_g, x$ of I such that $A = R[I^{[k]}/x^k]$.*

Proof. This was proved in the first two paragraphs of the proof of (4.4). □

For the following remark, the proof of (4.6.1) is similar to the proof of (4.1), and the proof of (4.6.2) is similar to the proof of (4.4), so the proofs will be omitted.

(4.6) Remark. (4.6.1). Let (R, M) and $I = (b, x)R$ be as in (4.1), assume that $char(R/M) > n$, and let $q \geq n - 1$ be an integer. Then for all but finitely many units u in R that are non-congruent modulo M it holds that $I = (b + ux, x)R$ and that I^j is generated by any set $S^* = \{x^{c_i - 1}(b + ux)^{j - (c_i - 1)};\ i = 1, \dots, n \text{ and } 1 \leq c_1 < \cdots < c_n \leq j + 1$ such that $c_i - c_h \not\equiv 0$ modulo $char(R/M)$ for $1 \leq h < i \leq n\}$ of n power products of degree j in $b + ux, x$ for $j = n - 1, \dots, q$.

(4.6.2) Let $b_1, \dots, b_g, x$ be regular nonunits in a local ring (R, M), let $I = (b_1, \dots, b_g, x)R$, and assume that $a(I) = 1$ and that $I \subseteq (xR)_a$, say $(b_i, x)^{n_i}R = x(b_i, x)^{n_i - 1}R$ for $i = 1, \dots, g$. Let $q \geq n_1 + \cdots + n_g - g + 1$ be an integer and assume that $char(R/M) > max\{n_1, \dots, n_g\}$. Then for all but finitely many units $u_1, \dots, u_g$ in R that are non-congruent modulo M it holds that $I = (b_1 + u_1x, \dots, b_g + u_gx, x)R$ and that, for $j = n_1 + \cdots + n_g - g + 1, \dots, q$, I^j is generated by any set of $n_1 \cdots n_g$ power products of the form $(b_1 + u_1x)^{e_1} \cdots (b_g + u_gx)^{e_g}x^{j - e_1 - \cdots - e_g}$, where $0 \leq e_i < n_i$ (for $i = 1, \dots, g$) and $e_1 + \cdots + e_g \leq j$.

Before proving a converse of (4.4), we first mention the following two results that are closely related to (4.1). These two results have the advantage that the original

basis b, x does not change, but they have the disadvantage that we can only prove them for $k = 2$.

(4.7) Remark. Let (R, M) be a local ring, let x be a regular element in M, and let b in R, such that $b^n = \sum_{i=1}^{n} r_i x^i b^{n-i}$ for some elements $r_1, \dots, r_n$ in R.
(4.7.1) Assume that n is even, that $r_1, \dots, r_{n-2}, r_n \in M$, and that $r_{n-1} \notin M$. Then $(b, x)^{2n} R = x^2 (b^2, x^2)^{n-1} R$.
(4.7.2) Assume that n is odd, that $r_1, \dots, r_{n-1} \in M$, and that $r_n \notin M$. Then $(b, x)^{2n} R = x^2 (b^2, x^2)^{n-1} R$.

Proof. For (4.7.1), successively multiply both sides of $b^n = \sum_{i=1}^{n} r_i x^i b^{n-i}$ by b^n, xb^{n-1}, ..., $x^{n-1}b, x^n$ to get the $n+1$ equations

$$b^{2n} = \sum_{i=1}^{n} r_i x^i b^{2n-i}$$

$$\dots$$

$$x^n b^n = \sum_{i=1}^{n} r_i x^{n+i} b^{n-i}.$$

Rewrite each of these $n+1$ equations with the n terms involving $x^{2i}\beta^{2(n-i)}$ ($i = 1, \dots, n$) on the right-hand side and the remaining $n+1$ terms on the left-hand side. Now view these equations in this form as the system $H_e Y = G$ of $n+1$ linear equations in the $n+1$ variables in the set

$$\{x^i b^{2n-i}; i = 1, \dots, 2n-1 \text{ and } i \not\equiv 0 \ mod\ 2\} \cup \{b^{2n}\}.$$

(Here, Y is the $n+1$-tuple (column vector) $(b^{2n}, xb^{2n-1}, \dots, x^i b^{2n-i}, \dots, x^{2n-1}b)^t$ (with $i = 1, \dots, 2n-1$ and $i \not\equiv 0 \ mod\ 2$), G is the the $n+1$-tuple (column vector) $(g_1, \dots, g_{n+1})^t$, where g_j is the sum of the terms of the j-th equation involving $x^{2n}, x^{2n-2}b^2, \dots, x^2 b^{2n-2}$ (including the coefficients $r_1, \dots, r_n$ (and -1 for $j = 3, 5, \dots$)) (so each g_j is a linear combination of the generators of $x^2(b^2, x^2)^{n-1}R$), and H_e is the $n+1$ by $n+1$ coefficient matrix, which is obtained (much as in (4.1.3)) by crossing out columns $3, 5, \dots, 2n+1$ from the $n+1$ by $2n+1$ matrix whose first row is $-1\ r_1\ r_2\ \dots\ r_n$ followed by n zeros, and whose i th row ($i = 2, \dots, n+1$) is obtained by adjoining a leading 0 to the $i-1$-st row and deleting the last zero from the $i-1$-st row.

Then, since $r_1, \dots, r_{n-2}, r_n$ are in M, H_e modulo M is the matrix

$$\overline{H_e} = \begin{pmatrix} -1 & 0 & 0 & 0 & \dots & 0 & \overline{r}_{n-1} & 0 & \dots & 0 & 0 \\ 0 & -1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & \overline{r}_{n-1} & \dots & 0 & 0 \\ 0 & 0 & -1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & -1 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & \overline{r}_{n-1} & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & -1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \overline{r}_{n-1} \end{pmatrix}$$

(where the overbar denotes residue class modulo M). By rearranging the rows of this matrix it is readily seen that its determinant is $\pm \overline{r}_{n-1}{}^{n/2} \neq 0$ (by the hypothesis on the coefficients $r_1, \dots, r_n$). Therefore the determinant of the coefficient matrix H_e is a unit in R, so it follows (much as in the next to last paragraph of the proof of (4.1)) that $(b, x)^{2n} R = x^2 (b^2, x^2)^{n-1} R$, so (4.7.1) holds.

The proof of (4.7.2) is similar, using the $n+1$ by $n+1$ matrix

$$\overline{H_o} = \begin{pmatrix} -1 & 0 & 0 & 0 & \dots & 0 & \overline{r}_n & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & \overline{r}_n & 0 & \dots & 0 \\ 0 & 0 & -1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \overline{r}_n & \dots & 0 \\ 0 & 0 & 0 & -1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & \overline{r}_n \\ 0 & 0 & 0 & 0 & \dots & 0 & -1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

(whose determinant is $\pm \overline{r}_n{}^{(n-1)/2} \neq 0$). □

We now prove a converse of (4.4). (Two additional converses of (4.4) are given in (6.3) and (6.8).)

(4.8) Theorem. *Let I be a regular ideal in a local ring (R, M) and assume that there exist positive integers g, n, and $k \geq \binom{n+g}{g}$ such that I has a basis $\beta_1, \dots, \beta_g, x$ such that $I^{kn} = ({\beta_1}^k, \dots, {\beta_g}^k, x^k)^n R$. Then $a(I) = 1$.*

Proof. Note first that, since I is generated by $g+1$ elements, it follows that $I^{[k]n} = ({\beta_1}^k, \dots, {\beta_g}^k, x^k)^n R$ can be generated by $\binom{n+g}{g}$ elements. Also, if $a(I) = a$, then I^{kn} needs at least $\binom{kn+a-1}{a-1}$ generators. Therefore, if $k \geq \binom{n+g}{g}$ and $I^{kn} = I^{[k]n}$, then it follows that $a = 1$, so $a(I) = 1$. □

(4.9) Corollary. *Let (R, M) be a local ring such that $char(R/M) = 0$ and let $I = (b_1, \dots, b_g, x)R$ be a regular ideal in R. Then $a(I) = 1$ if and only if there exists a positive integer n such that for all positive integers k there exists a basis $\beta_1, \dots, \beta_g, x$ of I such that $I^{jn} = ({\beta_1}^j, \dots, {\beta_g}^j, x^j)^n R$ for $j = 1, \dots, k$.*

Proof. This follows immediately from (4.4) and (4.8). □

5. Some results concerning bracket powers, prenormal ideals, and Ratliff-Rush closure

In this section we prove several useful results concerning ideals of the form $I^{[k]}$, as defined in (3.1.6), and relate these ideals to prenormal ideals and to the Ratliff-Rush closure of I. We begin by fixing some notation.

(5.1) Notation. *The following notation is fixed for this section:* R is a Noetherian ring, I is a regular ideal of R, $b_1, \dots, b_g$ $(g \geq 1)$ are regular elements of R that generate I, and if k is a positive integer, then $I^{[k]} = ({b_1}^k, \dots, {b_g}^k)R$. (Note that it is *not* assumed that $b_1, \dots, b_g$ is a minimal generating set for I; however, see (5.6.2) and the comment following (5.6).)

(5.2) Definition. (5.2.1). I is **normal** in case $I^k = (I^k)_a$ for all positive integers k, and I is **prenormal** in case $I^k = (I^k)_a$ for all large integers k.
(5.2.2) $v(I)$ denotes the smallest number of elements that generate I.
(5.2.3) The **Ratliff-Rush closure** I' of I is the ideal $\bigcup\{I^{k+1} : I^k;\ k \geq 1\}$, so I' $= I^{k+1} : I^k$ for all large integers k. (A nice summary of results concerning these ideals is given in [HJLS].)

(5.3) Remark. (5.3.1). Concerning (5.2.1), it is clear that every normal ideal is prenormal, and it is shown in [M, (11.15)] that I is prenormal if and only if $I^n = (I^n)_a$ for infinitely many positive integers n.

(5.3.2) Concerning (5.2.3), it readily follows from [RR1, (2.1) and (2.2)] that if J is another ideal in R, then: (*) $J' = I'$ if and only if $J^k = I^k$ for all large integers k. Moreover, I' is the largest ideal J such that $J^k = I^k$ for all large integers k, by [RR1, (2.1)]. (It follows from (*) that the conclusion of (4.4) can be viewed as saying that I^j and $I^{[j]}$ have the same Ratliff-Rush closure for $j = 1, \dots, k$. And a similar statement can be made concerning (4.1) and (4.7) (using (*) together with (5.6.1)).)

In (5.4) we prove two easy facts concerning prenormal ideals that will be useful below.

(5.4) Lemma. (5.4.1) *If $I^{[k]}$ is prenormal for some integer $k > 1$ and if m is a positive integer that divides k, then $I^{[m]}$ is prenormal. (In particular, I is prenormal.)*
(5.4.2) *If $I^{[k]}$ is prenormal for some integer $k > 1$, then $I^{[k]n} = I^{kn}$ for all large integers n, so $I^{[k]}$ and I^k have the same Ratliff-Rush closure.*

Proof. For (5.4.1) assume that $I^{[k]}$ is prenormal and let $k = mq$. Then for all large integers n it holds that $I^{[m]qn} \supseteq I^{[k]n} = (I^{[k]n})_a = (I^{kn})_a$ (by (3.2.1)) $= (I^{mqn})_a \supseteq (I^{[m]qn})_a \supseteq I^{[m]qn}$. Therefore $I^{[m]qn} = (I^{[m]qn})_a$ for all large integers n, so $I^{[m]}$ is prenormal by (5.3.1).

For the parenthetical part of (5.4.1), by taking $m = 1$ (so $I^{[1]} = I$ and $q = k$) in the string of containments in the preceding paragraph it follows that $I^{kn} = (I^{kn})_a$ for all large integers n, so it follows from (5.3.1) that I is prenormal.

For (5.4.2), if $I^{[k]}$ is prenormal, then for all large integers n it holds that $I^{[k]n} = (I^{[k]n})_a = (I^{kn})_a$ (by (3.2.1)) $= I^{kn}$ (by (5.4.1)), so $I^{[k]n} = I^{kn}$ for all large integers n. Therefore $I^{[k]}$ and I^k have the same Ratliff-Rush closure by (5.3.2)(*). □

Because of (5.4.2), in (5.5)–(5.9) we note a few useful facts concerning the equality $I^{[k]n} = I^{kn}$; because of (5.3.2), each of these concerns the Ratliff-Rush closure of an ideal.

(5.5) Remark. (5.5.1). If $I = (b_1, \dots, b_g)R$ $(g > 1)$, if $b_1, \dots, b_g$ are analytically independent elements, and if $k > 1$ is an integer, then, for each positive integer n, $({b_1}^k, \dots, {b_g}^k)^n R \neq (b_1, \dots, b_g)^{kn} R$. (This follows by noting that the number of generators of $I^{[k]n}$ is $\binom{n+g-1}{g-1}$ while the number of generators of I^{kn} is $\binom{kn+g-1}{g-1}$.)
(5.5.2) If x, y are analytically independent in R, if 2 is a unit in R, and if $J = (x, y)R$, then $J = (x, x+y, y)R$ and $J^{[2]} = (x^2, (x+y)^2, y^2)R$ is such that $J^{[2]n} = J^{2n}$ for all positive integers n. (Note that this example also shows that $v(J^{[k]}) > v(J)$ is possible (see (5.2.2)); however, it is always true that $I^{[k]}$ is generated by the g elements ${b_1}^k, \dots, {b_g}^k$, where $I = (b_1, \dots, b_g)R$.)

(5.6) Lemma. *If $I^{[k]n} = I^{kn}$ for some integers $k \geq 2$ and $n \geq 1$, then:*
(5.6.1) *$I^{[k]i} = I^{ki}$ for all integers $i \geq max\{n, k(g-1)+1\}$.*
(5.6.2) *If K is the ideal generated by the k-th powers of the elements in I, and if J is an ideal such that $I^{[k]} \subseteq J \subseteq K$, then $J^n = I^{kn}$ for all large integers n. In particular, if $c_1, \dots, c_f \in I$, then we may choose $J = ({b_1}^k, \dots, {b_g}^k, {c_1}^k, \dots, {c_f}^k)R$.*
(5.6.3) *If m is a positive integer that divides k, then $I^{[m]n} = I^{mn}$ for all large integers n.*
(5.6.4) *$R[I/b] = R[I^{[k]}/b^k]$ for each regular element $b \in I$.*

(5.6.5) *If J is an ideal in R, then $\overline{I^{[k]n}} = \bar{I}^{[k]n} = \bar{I}^{kn} = \overline{I^{kn}}$, where the "bar" denotes residue class modulo J.*
(5.6.6) *If A is an extension ring of R, then $I^{[k]n}A = (IA)^{[k]n} = (IA)^{kn} = I^{kn}A$.*
(5.6.7) *If S ($0 \notin S$) is a multiplicatively closed set in R such that $IR_S \neq R_S$, then $I^{[k]n}R_S = (IR_S)^{[k]n} = (IR_S)^{kn} = I^{kn}R_S$.*

Proof. For (5.6.1), note first that if $I^{[k]n} = I^{kn}$, then $I^{[k]nq} = I^{knq}$ for all positive integers q, so $I^{[k]n} = I^{kn}$ for infinitely many positive integers n.

Now let X be a reduction of $I^{[k]}$ (possibly $X = I^{[k]}$), so X is a reduction of I^k, by (3.2.1) (and the transitivity property of reductions), so there exists a positive integer m such that $XI^{[k]n} = I^{[k](n+1)}$ and $XI^{kn} = I^{k(n+1)}$ for all integers $n \geq m$. (Note that if $X = I^{[k]}$, then m can be taken to be $k(g-1)+1$.) By the preceding paragraph fix $n \geq m$ such that $I^{[k]n} = I^{kn}$. Then $I^{[k](n+j)} = X^jI^{[k]n} = X^jI^{kn} = I^{k(n+j)}$ for all positive integers j; hence $I^{[k]i} = I^{ki}$ for all integers $i \geq max\{n, k(g-1)+1\}$.

For (5.6.2), it follows from the hypothesis and (5.6.1) that if n is a large integer, then $I^{kn} = I^{[k]n} \subseteq J^n \subseteq K^n \subseteq I^{kn}$, so $J^n = I^{kn}$. For the last statement, if $c_1, \ldots, c_f \in I$, then it is clear that $I^{[k]} \subseteq ({b_1}^k, \ldots, {b_g}^k, {c_1}^k, \ldots, {c_f}^k)R \subseteq K$.

For (5.6.3) let $k = mq$. Then $I^{[m]qn} \supseteq I^{[mq]n} = I^{[k]n} = I^{kn} = I^{mqn} \supseteq I^{[m]qn}$, so $I^{[m]h} = I^{mh}$ for $h = qn$; hence $I^{[m]n} = I^{mn}$ for all large integers n by (5.6.1).

For (5.6.4) fix a regular element b in I. If $I^{[k]n} = I^{kn}$ for some positive integer n, then $R[I/b] \supseteq R[I^{[k]}/b^k] \supseteq R[I^{[k]n}/b^{kn}] = R[I^{kn}/b^{kn}] = R[I/b]$, the last equality since $b^{kn-1}b_i \in I^{kn}$ for $i = 1, \ldots, g$, so $R[I/b] = R[I^{[k]}/b^k]$.

The proof of each of (5.6.5)–(5.6.7) is straightforward, so the proofs will be omitted. □

Perhaps two comments concerning (5.6) should be given here. First, it follows from (5.6.2) that we could replace $I^{[k]}$ with K, which has the advantage that K is independent of the basis $b_1, \ldots, b_g$ of I. However, this replacement has the disadvantage that K does not behave nicely when passing to related rings and when considering different exponents k.

And, second, it follows from (5.6.5)–(5.6.7) that, when working with the hypothesis $I^{[k]n} = I^{kn}$, it can often be assumed that R is an integrally closed complete local domain with an infinite residue field.

Theorem 5.7 is related to (5.6.4) and it characterizes when the ideal $I^{\langle k \rangle} = (\{b^k;\ b \in I\})R$ has the property that $I^{\langle k \rangle n} = I^{kn}$ for some positive integer n. (We do not know if the hypothesis that R/M is infinite is necessary in (5.7).)

(5.7) Theorem. *Let R be a Noetherian ring, let I be a regular ideal of R, let $k \geq 2$ be an integer, and consider the following statements:*
(5.7.1) *$I^{\langle k \rangle n} = I^{kn}$ for all large integers n.*
(5.7.2) *$I^{\langle k \rangle n} = I^{kn}$ for some integer $n \geq 1$.*
(5.7.3) *$R[I/b] = R[I^{\langle k \rangle}/b^k]$ for each regular element $b \in I$.*

Then (5.7.1) ⇒ (5.7.2) ⇒ (5.7.3), and if R is local with an infinite residue field, then (5.7.3) ⇒ (5.7.1).

Proof. It is clear that (5.7.1) ⇒ (5.7.2).

For (5.7.2) ⇒ (5.7.3), since $I^{\langle k \rangle} = (\{b^k;\ b \in I\})R$, there exists a basis $b_1, \ldots, b_h$ for I such that $I^{\langle k \rangle} = ({b_1}^k, \ldots, {b_h}^k)R$. Fix a regular element b in I and note that $I^{\langle k \rangle n} = I^{kn}$ for some positive integer n, by (5.7.2). Therefore it follows that

$R[b_1/b, \dots, b_h/b] = R[I/b] \supseteq R[I^{\langle k \rangle}/b^k] \supseteq R[I^{\langle k \rangle n}/b^{kn}] = R[I^{kn}/b^{kn}] = R[I/b]$, the last equality since $b^{kn-1}b_i \in I^{kn}$ for $i = 1, \dots, h$, so $R[I/b] = R[I^{\langle k \rangle}/b^k]$. Therefore (5.7.2) $\Rightarrow$ (5.7.3).

Finally, assume that R is local with an infinite residue field and that (5.7.3) holds, and by (3.3) let b be a regular superficial element for I such that b^k is a regular superficial element for $I^{\langle k \rangle}$. Let $A = R[I/b]$, so $A = R[I^{\langle k \rangle}/b^k]$, by hypothesis. Then $b^{kn}A \cap R = I^{kn}$ and $b^{kn}A \cap R = I^{\langle k \rangle n}$ for all large integers n by (3.5). Therefore it follows that $I^{\langle k \rangle n} = I^{kn}$ for all large integers n, so (5.7.3) $\Rightarrow$ (5.7.1). □

The following lemma gives four computational rules concerning the operation $I \to I^{[k]}$.

(5.8) Lemma. *Let R and $I = (b_1, \dots, b_g)R$ be as in (5.1), and let m and k be positive integers. Then:*
(5.8.1) $I^{[k][m]} = I^{[km]}$.
(5.8.2) $I^{[k]m} = I^{m[k]}$.
(5.8.3) *If J is another ideal in R, then $(IJ)^{[k]} = I^{[k]}J^{[k]}$.*
(5.8.4) *If J is another ideal in R, if $I \subseteq J$, and if $char(R) = p$ is prime, then $I^{[p^e]} \subseteq J^{[p^e]}$ for all positive integers e. (Therefore $I^{[p^e]}$ is independent of the basis of I and is the ideal generated by the p^e-th powers of any set of basis elements of I.)*

Proof. For (5.8.1), $I^{[k][m]} = ((b_1{}^k, \dots, b_g{}^k)R)^{[m]} = (b_1{}^{km}, \dots, b_g{}^{km})R = I^{[km]}$.

For (5.8.2), $I^{[k]m}$ is generated by elements of the form $b_1{}^{ke_1} \cdots b_g{}^{ke_g}$, where $e_1 + \cdots + e_g = m$, and $I^{m[k]}$ is generated by elements of the form $(b_1{}^{e_1} \cdots b_g{}^{e_g})^k$, where $e_1 + \cdots + e_g = m$, so it follows that the ideals $I^{[k]m}$ and $I^{m[k]}$ have a common generating set.

For (5.8.3), if $J = (c_1, \dots, c_f)R$, then $(IJ)^{[k]}$ is generated by elements of the form $(b_ic_j)^k$ (with $i = 1, \dots, g$ and $j = 1, \dots, f$), and $I^{[k]}J^{[k]}$ is generated by elements of the form $b_i{}^k c_j{}^k$ (with $i = 1, \dots, g$ and $j = 1, \dots, f$), so it follows that the ideals $(IJ)^{[k]}$ and $I^{[k]}J^{[k]}$ have a common generating set.

Finally, for (5.8.4), let $J = (c_1, \dots, c_f)R$, assume that $I \subseteq J$, and let e be a positive integer. Then for $i = 1, \dots, g$ there exist elements $r_{i,j}$ in R such that $b_i = \sum_{j=1}{}^f r_{i,j}c_j$. Therefore $b_i{}^{p^e} = \sum_{j=1}{}^f r_{i,j}{}^{p^e} c_j{}^{p^e} \in J^{[p^e]}$, so it follows that $I^{[p^e]} \subseteq J^{[p^e]}$. The parenthetical statement readily follows from this. □

In (6.3.2) we show that if $char(R) = p$ is prime and I is a regular ideal such that $I^{[p]n} = I^{pn}$ for some positive integer n, then $a(IR_P) = 1$ for all prime ideals P in R that contain I. This is, of course, a converse of (4.4), and we believe something similar to this should hold in arbitrary characteristic (and the results in (5.8) might prove useful in this regard), but we have not been able to prove it. However, it follows from (5.5.2) that some caution must be used in stating the desired result, and we include the following example to show that the proof of the desired result is not completely trivial.

(5.9) Example. Assume that I is a regular ideal in a local ring (R, M) and assume that R/M is infinite. Then the following is an **incorrect** proof of the implication $I^{[k]n} = I^{kn}$ for some integers $k \geq 2$ and $n \geq 1$ implies that $a(I) = 1$. By (5.6.1), $I^{[k]n} = I^{kn}$ for all large integers n, so let $n = k^h$ with h a large integer. Then $I^{[k]k^h} = I^{k^{h+1}}$, so by (5.8.2) we have $I^{k^{h+1}} = (I^{k^h})^{[k]}$. Therefore $v(I^{k^{h+1}}) = v((I^{k^h})^{[k]}) \leq v(I^{k^h}) =$ (say) $h^\star$ (the inequality holds, since raising the elements in a basis

to their k-th power does not increase the number of elements). Iterating this it follows that $v((I^{k^h})^n) \leq h^\star$ for all positive integers n, so $v((I^{k^h})^{h^\star+1}) < h^\star + 1$. Therefore, [ES, Theorem], shows that $a(I^{k^h}) \leq 1$, so $a(I) \leq 1$; hence $a(I) = 1$ since I is regular. (The mistake in this "proof" is that, although the equality $I^{k^{h+1}} = (I^{k^h})^{[k]}$ does imply that $v(I^{k^{h+1}}) = v((I^{k^h})^{[k]})$, it is not necessarily true that $v((I^{k^h})^{[k]}) \leq v(I^{k^h})$; for example, $I = (X, X+Y, Y)$ in $Q[X,Y]_{(X,Y)}$ (Q is the rationals) has $I^{[2]} = I^2$, so $(I^{2^h})^{[2]} = I^{[2]2^h} = I^{2^{h+1}}$, but $v(I^{2^{h+1}}) > v(I^{2^h})$.)

6. A property that implies analytic spread one in characteristic p

In this section we prove a strong converse of (4.4) when $char(R) = p$ is prime, and another strong converse when (R, M) is local and $char(R/M)$ is prime. For the first of these we need the following result, which is of some interest in itself.

(6.1) Proposition. *Let $A \subseteq B = A[x_1, \ldots, x_g] \subseteq C$ be rings and assume that $char(A) = p$ is prime and that $B = A[{x_1}^{e_1}, \ldots, {x_g}^{e_g}]$, where each e_i is of the form $p^k > 1$. Then:*

(6.1.1) *$B = A[{x_1}^{p^i}, \ldots, {x_g}^{p^i}]$ for all integers $i \geq 1$.*

(6.1.2) *If $y_1, \ldots, y_m$ are elements in C such that $B = A[y_1, \ldots, y_m]$, then $B = A[{y_1}^{p^i}, \ldots, {y_m}^{p^i}]$ for all integers $i \geq 1$.*

Proof. For (6.1.1), $B = A[{x_1}^{e_1}, \ldots, {x_g}^{e_g}] \subseteq A[{x_1}^p, \ldots, {x_g}^p] \subseteq B$, so we have $B = A[{x_1}^p, \ldots, {x_g}^p]$. Therefore for $j = 1, \ldots, g$ there exists a polynomial $P_j(X_1, \ldots, X_g)$ with coefficients in A such that $x_j = P_j({x_1}^p, \ldots, {x_g}^p)$. Let $k \geq 1$ and assume it has been shown that $B = A[{x_1}^{p^k}, \ldots, {x_g}^{p^k}]$. Then

$$ {x_j}^{p^k} = (P_j({x_1}^p, \ldots, {x_g}^p))^{p^k} \in A[{x_1}^{p^{k+1}}, \ldots, {x_g}^{p^{k+1}}]. $$

It therefore follows that $A[{x_1}^{p^k}, \ldots, {x_g}^{p^k}] \subseteq A[{x_1}^{p^{k+1}}, \ldots, {x_g}^{p^{k+1}}]$, and it then follows that $B = A[{x_1}^{p^{k+1}}, \ldots, {x_g}^{p^{k+1}}]$. Therefore $B = A[{x_1}^{p^i}, \ldots, {x_g}^{p^i}]$ for all positive integers i, so (6.1.1) holds.

For (6.1.2), if $A[x_1, \ldots, x_g] = B = A[y_1, \ldots, y_m]$, then for $j = 1, \ldots, g$ there exists a polynomial $Q_j(X_1, \ldots, X_m)$ with coefficients in A such that $x_j = Q_j(y_1, \ldots, y_m)$. Then ${x_j}^p = (Q_j(y_1, \ldots, y_m))^p \in A[{y_1}^p, \ldots, {y_m}^p]$, so it follows that $A[{x_1}^p, \ldots, {x_g}^p] \subseteq A[{y_1}^p, \ldots, {y_m}^p]$. But $B = A[{x_1}^p, \ldots, {x_g}^p]$, by (6.1.1), and $A[{y_1}^p, \ldots, {y_m}^p] \subseteq B$, so it follows that $A[y_1, \ldots, y_m] = A[{y_1}^p, \ldots, {y_m}^p]$. Therefore the conclusion follows from (6.1.1). □

(6.2) Remark. Let A and B be as in (6.1) and let $P \in Spec(B)$. Then the P-residue classes of the x_i are algebraic over $A/(P \cap A)$.

Proof. $B/P = R[y_1, \ldots, y_g] = R[{y_1}^p, \ldots, {y_g}^p]$, where $R = A/(P \cap A)$ and $y_i = x_i + P$ for $i = 1, \ldots, g$. Therefore $F(y_1, \ldots, y_g) = F({y_1}^p, \ldots, {y_g}^p)$, where F is the quotient field of R, so each y_i is algebraic over F, by (6.6) below, so each y_i is algebraic over R. □

(6.3) gives a strong converse of (4.4) when $char(R)$ is prime.

(6.3) Theorem. *Let R be a Noetherian ring, let $I = (b_1, \ldots, b_g)R$ be an ideal in R, and assume that $char(R) = p$ is prime and that $I^{[mp^e]n} = I^{mp^e n}$ for some positive integers m, e, and n. Then the following hold for each prime ideal P in R that contains I:*

(6.3.1) $(IR_P)^{[p^f]h} = (IR_P)^{p^f h}$ *for all positive integers* f *and for all large integers* h.
(6.3.2) $a(IR_P) = 1$.

Proof. Note first that by (5.6.3) it may be assumed that $m = 1$.

Fix a prime ideal P in R that contains I. Then $char(R_P) = p$ and $(IR_P)^{[p^e]n} = (IR_P)^{p^e n}$, by (5.6.7). If R_P/PR_P is finite, then let X be an indeterminate and let $L = R_P(X) = R_P[X]_{PR_P[X]}$ and $M = PL$, so $char(L) = p$, $(IL)^{[p^e]n} = (IL)^{p^e n}$, by (5.6.6), and L/M is infinite. Also, $a(IR_P) = a(IL)$, so to prove both statements it may be assumed to begin with that R is local with maximal ideal P and that R/P is infinite.

Now fix a positive integer f. Then, since $char(R) = p$, it is readily checked that $I^{[p^f]} = K_{p^f}$, where K_{p^f} is the ideal generated by the p^f-th powers of the elements in I. Therefore by (3.3) there exists a regular superficial element x for I such that x^{p^f} is a regular superficial element for $I^{[p^f]}$. Let $A = R[I/x]$, so $A = R[I^{[p^e]}/x^{p^e}]$, by hypothesis and (5.6.4); hence $A = R[I^{[p^f]}/x^{p^f}]$ by (6.1.1). Therefore it follows from (3.5) that, for all large integers n, we have $x^{p^f n}A \cap R = I^{p^f n}$ (since $A = R[I/x]$), and $x^{p^f n}A \cap R = I^{[p^f]n}$ (since $A = R[I^{[p^f]}/x^{p^f}]$), so it follows that $I^{[p^f]n} = I^{p^f n}$ for all positive integers f and for all large integers n, so (6.3.1) holds.

Finally, (5.8.4) shows that $v(I^{[p^f]}) = v(I)$, so it follows from $I^{[p^f]n} = I^{p^f n}$ that $v(I^{p^f n}) \leq v(I^n) \leq \binom{n+v(I)-1}{v(I)-1}$ for each large integer n and for all integers $f \geq 1$ (see (5.2.2)). Since the number of generators of I^n is a polynomial, and since $\binom{n+v(I)-1}{v(I)-1}$ is independent of f, it follows that this polynomial has degree zero, so $a(I^n) \leq 1$. Therefore $a(I^n) = 1$, since I is regular, so $a(I) = a(I^n) = 1$, so (6.3.2) holds. □

(6.4) Corollary. *Let* I *be a regular ideal in a Noetherian ring* R. *Assume that* $char(R) = p \neq 0$ *and that there exists a generating set* $b_1, \ldots, , b_g$ *of* I *such that there exist positive integers* m, e *such that* $({b_1}^{mp^e}, \ldots, {b_g}^{mp^e})R$ *and* I^{mp^e} *have the same Ratliff-Rush closure. Then* $a(IR_P) = 1$ *for all prime ideals* P *in* R *that contain* I *and* $height(P) = 1$ *for each minimal prime divisor* P *of* I. *Moreover, if* xR *is a minimal reduction of* I, *if* b *is a regular element in* I, *and if* $A = R[I/b]$, *then* A *is the localization* $B[x/b]$ *of* $B = R[I/x]$.

Proof. It is noted in (5.8.4) that $I^{[p^e]}$ is independent of the basis for I, so the hypothesis is that $I^{[mp^e]}$ and I^{mp^e} have the same Ratliff-Rush closure. Also, by (5.6.3) it may be assumed that $m = 1 = e$, so $I^{[p]}$ and I^p have the same Ratliff-Rush closure; hence $I^{[p]n} = I^{pn}$ for all large integers n, by (5.3.2). Therefore it follows from (6.3) that if $I \subseteq P \in Spec(R)$, then $a(IR_P) = 1$ (so if P is a minimal prime divisor of I, then IR_P is open and $a(IR_P) = 1$, so it follows that $height(P) = altitude(R_P) = 1$).

Now assume that xR is a minimal reduction of I, so $xR \subseteq I \subseteq (xR)_a$. Therefore x is a regular nonunit, since I is a regular ideal; hence $B = R[I/x] \subseteq R'$. Also, if b is a regular element in I, then $b/x \in B \subseteq R' \subseteq A'$, where $A = R[I/b]$, and $x/b \in A$. Therefore it follows that $b/x \in A$, so $A = R[I/b] = R[I/b, b/x] = R[I/x, x/b] = B[x/b]$; hence $A = B[x/b]$ is a localization of B. □

(6.5) Corollary. *Let* R *and* I *be as in (6.4) and assume that* $height(I) > 1$. *Then for all prime ideals* P *in* R *that contain* I *it holds that* $(IR_P)^{[p]}$ *and* $(IR_P)^p$ *do not have the same Ratliff-Rush closure.*

Proof. If $I \subseteq P \in Spec(R)$ and if $(IR_P)^{[p]}$ and $(IR_P)^p$ have the same Ratliff-Rush closure, then $height(IR_P) = 1$ by (6.4), so $height(I) = 1$. Therefore, if $height(I) > 1$, then $(IR_P)^{[p]}$ and $(IR_P)^p$ do not have the same Ratliff-Rush closure. □

In (6.8) we prove another converse of (4.4). For (6.8) we need the following result (which is a slight extension of a result of R. Gilmer). (6.6) is a useful extension of [ZS1, Corollary, p. 70], where it is shown that if F is a field of characteristic $p \neq 0$ and y is algebraic over F, then $F(y) = F(y^p)$ if and only if y is separable over F.

(6.6) Proposition. *Let $G \subseteq F \subseteq E$ be fields of characteristic $p \neq 0$ and assume that $y_1, \ldots, y_g$ are elements in E such that $G({y_1}^{p^i}, ..., {y_g}^{p^i}) = F(y_1, ..., y_g)$ for some positive integer i. Then each y_i is algebraic over G.*

Proof. If $G({y_1}^{p^i}, ..., {y_g}^{p^i}) = F(y_1, ..., y_g)$, then it readily follows that $G({y_1}^{p^i}, ..., {y_g}^{p^i}) = G(y_1, ..., y_g)$, so it may be assumed to begin with that $G = F$.

Now let $\{y_1, \ldots, y_n\}$ be a transcendence basis for $L = F(y_1, \ldots, y_g)$ over F. Then L is a finite algebraic extension field of $K = F({y_1}^{p^i}, \ldots, {y_n}^{p^i})$, and $L = F({y_1}^{p^i}, \ldots, {y_g}^{p^i})$, by hypothesis. Also, $K(L^p) = L$, since

$$K(L^p) = F({y_1}^p, \ldots, {y_n}^p, {y_{n+1}}^p, \ldots, {y_g}^p) \supseteq F({y_1}^{p^i}, \ldots, {y_g}^{p^i}) = L \supseteq K(L^p),$$

so L is separable over K, by [ZS1, Theorem 8, p. 69]. But this implies that $n = 0$, for otherwise $y_1 \in L - K$ is purely inseparable over K; hence each y_i is algebraic over F. □

Unfortunately, when $char(F) = 0$, it is possible for $F(y_1, \ldots, y_g)$ to be equal to $F({y_1}^n, \ldots, {y_g}^n)$ for all positive integers n and with each y_i transcendental over F, as the following example of Gilmer shows.

(6.7) Example. Let F be a field of characteristic zero and let X be an indeterminate. Then there exist $Y, Z \in F(X) - F$ such that $F(Y, Z) = F(X) = F(Y^n, Z^n)$ for all positive integers n.

Proof. Let $f(X)$ and $g(X)$ in $F[X]$. Then $F(f(X)) \subseteq F(f(X), g(X)) \subseteq F(X)$ and $F(g(X)) \subseteq F(f(X), g(X)) \subseteq F(X)$. Therefore $[F(X) : F(f(X), g(X))]$ divides both $[F(X) : F(f(X))] = deg(f(X))$ and $[F(X) : F(g(X))] = deg(g(X))$, so if $deg(f(X))$ and $deg(g(X))$ are relatively prime, then it follows that $F(f(X), g(X)) = F(X)$. Therefore let $a, b \in F$, let $f(X) = X^2 + a$ and $g(X) = X^2 + X - b$, and let $Y = f(X)$ and $Z = g(X)$. Then Y and Z are transcendental over F, and $F(Y, Z) = F(X) = F(Y^n, Z^n)$ for all positive integers n (since $F(Y^n, Z^n) = F(Y^n, Y^n - Z^n)$ and the degrees of Y^n and $Y^n - Z^n$ are relatively prime). □

The next result is closely related to (6.3), and is another converse of (4.4).

(6.8) Theorem. *Let (R, M) be a local ring, let I be a regular ideal in R, and let $b_1, \ldots, b_g$ be regular elements in R that generate I. Assume that $char(R/M) = p$ is prime and that there exist positive integers e, m, n such that $I^{[mp^e]n} = I^{mp^e n}$. Then $a(I) = 1$.*

Proof. Note first that by (5.6.3) it may be assumed that $m = 1 = e$.

Let $a(I) = d$ and let $altitude(R) = h$, so $d \leq h$, and $d \geq 1$ (since I is regular). Let $\mathbf{R} = R[u, tI]$, so by the definition of the analytic spread of an ideal it suffices to show that $d = altitude(\mathbf{R}/(u, M)\mathbf{R}) = 1$.

For this, let P_0 be a (minimal) prime divisor of $(u, M)\mathbf{R}$ such that $depth(P_0) = d$ and let $\mathbf{M} = (u, M, tI)\mathbf{R}$, so $P_0 \subset \mathbf{M}$. We now show that $depth(P_0) = 1$ (so $a(I) = 1$).

For this, since $P_0 \subset \mathbf{M}$, by resubscripting the b_j, if necessary, it may be assumed that $tb_g \notin P_0$. Therefore let $B = R[b_1/b_g, \ldots, b_{g-1}/b_g]$ and let $\mathbf{S} = \mathbf{R}[1/tb_g]$. Then $\mathbf{S} = B[tb_g, 1/tb_g]$, $u\mathbf{S} = b_g\mathbf{S}$, and $(u, M)\mathbf{S} = M\mathbf{S}$ (since $b_g \in MB \subseteq M\mathbf{S}) \subseteq P_0\mathbf{S}$. Also, since $\mathbf{S} = B[tb_g, 1/tb_g]$ and tb_g is transcendental over B, it follows that $P_0\mathbf{S} = p_0\mathbf{S}$, where $p_0 = P_0\mathbf{S} \cap B$.

Assume it is known that B/p_0 is a field. Then $depth(p_0) = 0$, so since $\mathbf{S}$ is the localization $B[tb_g, 1/tb_g]$ of the pure transcendental extension $B[tb_g]$ of B, it follows that $depth(p_0\mathbf{S}) = 1$, so $depth(P_0\mathbf{S}) = 1$ (since $P_0\mathbf{S} = p_0\mathbf{S}$). Also, $\mathbf{S}/P_0\mathbf{S}$ and $\mathbf{R}/P_0$ are finitely generated integral domains over the field $F = R/M$, so it follows that $trd((\mathbf{S}/P_0\mathbf{S})/F) = altitude(\mathbf{S}/P_0\mathbf{S}) = depth(P_0\mathbf{S}) = 1$ and $trd((\mathbf{R}/P_0)/F) = depth(P_0)$. Further $\mathbf{S}/P_0\mathbf{S}$ is the localization $(\mathbf{R}/P_0)[1/\overline{tb_g}]$ of $\mathbf{R}/P_0$, so it follows that $altitude(\mathbf{R}/P_0) = altitude(\mathbf{S}/P_0\mathbf{S})$, so $altitude(\mathbf{R}/P_0) = 1$. Therefore $a(I) = depth(P_0) = altitude(\mathbf{R}/P_0) = 1$, as desired, so it remains to show that B/p_0 is a field.

For this, let $x_j = b_j/b_g$ for $j = 1, \ldots, g-1$ and note that by hypothesis and (5.6.4) (and the first paragraph of this proof) it follows that $B = R[x_1{}^p, \ldots, x_{g-1}{}^p]$. Let $C = B/p_0$, and for $j = 1, \ldots, g-1$ set $y_j = x_j + p_0$ in C, so $C = F[y_1, \ldots, y_{g-1}] = F[y_1{}^p, \ldots, y_{g-1}{}^p]$. Therefore it follows that $F(y_1, \ldots, y_{g-1}) = F(y_1{}^p, \ldots, y_{g-1}{}^p)$. Therefore, since $char(F) = p$, by hypothesis, it follows from (6.6) that each y_i is algebraic over F, and it then follows that C is a field; hence $a(I) = 1$ by the preceding paragraph. □

7. An application to imbedded prime divisors

The main result in this section, (7.2), uses (6.5) to show that if R is a Noetherian ring such that $char(R) = p$ is prime, if I is a regular ideal of height at least two in R, if $\mathbf{S}$ is the set of prime ideals in R that contain I, and if W is an arbitrary finite subset of $\mathbf{S}$ that contains the essential prime divisors of I (see (7.1.3)), then there exists an ideal J in R that is closely related to I such that $Ass(R/J^k) = W$ for all positive integers k. This result is related to the results in [MR], where there are given a number of sufficient conditions on the ideals in W for this conclusion to hold. The results in [MR] apply to all regular ideals of R (instead of restricting attention to ideals of height at least two in Noetherian rings of prime characteristic), but the inclusion of ideals of height one in all Noetherian rings came at the price of imposing some restrictions on the ideals in W. (For example, the result holds for a (regular) principal ideal bR if and only if bR_P is not integrally closed for all minimal prime divisors P of bR.)

To prove (7.2) we need the following four definitions.

(7.1) Definition. If I is an ideal in a Noetherian ring R, then:
(7.1.1) $A^\star(I)$ is the set of **persistent prime divisors** of I, so $A^\star(I) = \{P;\ P \in Ass(R/I^k)$ for all large integers $k\}$.
(7.1.2) $\hat{A}^\star(I)$ denotes the set of **asymptotic prime divisors** of I, so $\hat{A}^\star(I) = \{P;\ P \in Ass(R/(I^k)_a)$ for some positive integer $k\}$.
(7.1.3) $\mathbf{E}(I)$ denotes the set of **essential prime divisors** of I, so $\mathbf{E}(I) = \{P;\ P = p \cap R$, where $p \in Ass(\mathbf{R}(R, I)/u\mathbf{R}(R, I))$ and the completion of $\mathbf{R}(R, I)_p$ contains a depth one prime divisor of zero$\}$. (Concerning $\mathbf{R}(R, I)$, see (3.1.3).)

(7.1.4) If J is another ideal in R, then J is **projectively equivalent** to I in case $(J^j)_a = (I^i)_a$ for some positive integers i and j.

Concerning (7.1.1)–(7.1.3), it is shown in [KR, (2.5.7) and (2.3.3)] that $\hat{A}^\star(I) \subseteq \mathbf{E}(I) \subseteq A^\star(I)$, and it is shown in [M, (1.5)] that $A^\star(I)$ is a finite set.

With these definitions in mind, we can now prove the main result in this section.

(7.2) Theorem. *Let R be a Noetherian ring such that $char(R) = p \neq 0$, let I be a regular ideal in R such that $height(I) > 1$, and let $\mathbf{S} = \{P \in Spec(R);\ I \subseteq P\}$. Then for every finite subset W of $\mathbf{S}$ there exists an ideal J in R such that:*
(7.2.1) *J is projectively equivalent (see (7.1.4)) to I.*
(7.2.2) *$A^\star(J) = Ass(R/J^k) = W \cup \mathbf{E}(I)$ for all positive integers k.*

Proof. It is shown in [MR, (1.10)] that there exist a positive integer m and an ideal H between I^m and $(I^m)_a$ such that $A^\star(H) = W \cup \mathbf{E}(I)$, if for each prime ideal P of R that contains I it holds that either $P \in \hat{A}^\star(I)$ or IR_P is not prenormal. Also, it is shown in [M, (1.5)] that $Ass(R/H^k) = A^\star(H)$ for all large integers k. We will now apply these results to $I^{[p]}$ to construct the desired ideal J.

For this, since $height(I) > 1$, it follows from (6.5) and (5.4.2) that $I^{[p]}R_P = (IR_P)^{[p]}$ is not prenormal for all $P \in Spec(R)$ that contain I. Therefore by applying [MR, (1.10)] to $I^{[p]}$ it follows that there exist a positive integer m and an ideal K between $I^{[p]m}$ and $(I^{[p]m})_a$ such that $A^\star(K) = W \cup \mathbf{E}(I^{[p]})$. Then since $I^{[p]}$ and I are projectively equivalent (by (3.2.1) and (7.1.4)), [KR, (2.5.6)] shows that $\mathbf{E}(I^{[p]}) = \mathbf{E}(I)$, so $A^\star(K) = W \cup \mathbf{E}(I)$, so [M, (1.5)] shows that if k is a large integer, then (7.2.2) holds for $J = K^k$. Finally, $(I^{[p]})_a = (I^p)_a$, by (3.2.1), so $I^{[p]}$ is projectively equivalent to I, and it is readily checked that K is projectively equivalent to $I^{[p]}$ and then that J is projectively equivalent to K. Therefore, since projective equivalence is transitive, it follows that J is projectively equivalent to I, so (7.2.1) holds. □

(7.3) Corollary. *Let $Q_1, \ldots, Q_g$ be primary ideals of height at least two in a Noetherian ring R, assume that $char(R) = p$ is prime, and let W be a finite set of prime ideals of R that contain $Q_1 \cdots Q_g$. Then there exists an ideal J in R such that:*
(7.3.1) *J is projectively equivalent to $Q_1 \cdots Q_g$.*
(7.3.2) *$A^\star(J) = Ass(R/J^k) = W \cup \mathbf{E}(Q_1 \cdots Q_g)$ for all integers $k \geq 1$.*

Proof. The hypothesis implies that $height(Q_1 \cdots Q_g) > 1$, so this follows immediately from (7.2). □

(7.4) Remark. With the notation of (7.2):
(7.4.1) The reason for wanting the ideal J of (7.2) to be projectively equivalent to I is that projectively equivalent ideals have many of the same properties. So in many ways the change from I to J is a small one, but (7.2) shows that the change from $A^\star(I)$ to $A^\star(J)$ can be almost arbitrarily bad (or, good).
(7.4.2) As noted in the proof of (7.2), it is shown in [KR, (2.5.6)] that $\mathbf{E}(H) = \mathbf{E}(I)$ whenever H and I are projectively equivalent ideals, so the conclusion of (7.2.2) can be restated as $A^\star(J) = Ass(R/J^k) = W \cup \mathbf{E}(J)$ for all integers $k \geq 1$. This (together with the fact that $\mathbf{E}(H) \subseteq A^\star(H)$) shows that if H is any ideal that is projectively equivalent to I, then $\mathbf{E}(I) \subseteq A^\star(H)$.
(7.4.3) If W is the empty set, then (7.2.2) shows that $Ass(R/J^k) = \mathbf{E}(I)$ for all integers $k \geq 1$. This is the main result in [KMOR], but the result in [KMOR] applies to all regular ideals (not just those of height at least two).

8. Related results

In this section we give some further results concerning the equality $I^{[k]n} = I^{kn}$ and some additional characterizations of when $a(I) = 1$.

The conclusion of the first result in this section is similar to the conclusion of (4.4). However, we are only able to prove (8.1) for the case when $altitude(R) = 1$.

(8.1) Proposition. *Let (R, M) be a local ring such that $altitude(R) = 1$, let H be a regular ideal in R, and let f be an integer such that $I = H^f$ has a reduction generated by one element, say x. Let $I = (b_1, \dots, b_g, x)R$ and fix a positive integer k. Then there exists a positive integer q such that $I^{[kqh]n} = I^{[kq]hn}$ for all positive integers h and for all large integers n. (In particular, if we let $J = I^{[kq]}$, then $J^{[h]n} = J^{hn}$ for all positive integers h and for all large integers n.)*

Proof. Since $altitude(R) = 1$ and I is regular, it follows that $a(I) = 1$. Therefore, since $x \in I \subseteq (xR)_a$, (3.7) shows that x (resp., x^k) is a regular superficial element for I (resp., $I^{[k]}$).

For each positive integer q let $A_q = R[I^{[kq]}/x^{kq}]$, so if m is a positive integer that divides q, then $A_q \subseteq A_m$ (and $A_m \subseteq A_1 = R[I^{[k]}/x^k]$). Also, $x^{kqn}A_q \cap R = I^{[kq]n}$ and $x^{kmn}A_m \cap R = I^{[km]n}$ for all large integers n, by (3.5).

Now there exists a positive integer i such that $x^iA_1 \subseteq R$ (since $A_1 = R[I^{[k]}/x^k]$ is a finite R-module (since xR is a reduction of I)) and R/x^iA_1 is an Artinian local ring (since xR is M-primary (since x is regular and $altitude(R) = 1$)). Therefore for any rings C and B such that $R \subseteq C \subseteq B \subseteq A_1$ we have $x^iA_1 \subseteq R \subseteq C \subseteq B$, so it follows that $C/x^iA_1 = B/x^iA_1$ if and only if $C = B$. Also, A_1/x^iA_1 is a finite module over the Artinian ring R/x^iA_1, so the rings between R/x^iA_1 and A_1/x^iA_1 satisfy the descending chain condition. It therefore follows that there exists a positive integer q such that $A_{qh} = A_q$ for all positive integers h. And it follows from the preceding paragraph that $x^{kqhn}A_{qh} \cap R = I^{[kqh]n}$ and $x^{kqhn}A_q \cap R = I^{[kq]hn}$ for all large integers n, so the conclusion follows since $A_{qh} = A_q$ for all positive integers h. The parenthetical statement follows from this and (5.8.1). □

(8.2) Remark. By using (5.8), it is tempting to use the conclusion of (8.1) to say that $H^{[kqh]fn} = (H^f)^{[kqh]n} = (H^f)^{[kq]hn} = H^{[kq]hfn}$ for all positive integers h and for all large integers n. However, when passing from H to $I = H^f$, we had to introduce the regular superficial element x as part of the basis of I, so $H^{[kq]f} \neq H^{f[kq]}$ because $H^{[kq]}$ is the bracket power of a given basis (say $c_1, \dots, c_m$) for H, while $H^{f[mq]}$ is the bracket power of H^f with a different basis than the basis $\{{c_1}^{e_1} \cdots {c_m}^{e_m};\ e_1 + \cdots + e_m = f\}$.

We close this paper with one more theorem that characterizes regular ideals of analytic spread one. This result also strengthens and expands the last conclusion of (6.4).

(8.3) Theorem. *Let I be an ideal generated by regular elements $b_1, \dots, b_g$ in a local ring (R, M), assume that R/M is infinite, let $\mathbf{R} = \mathbf{R}(R, I)$, and for $i = 1, \dots, g$ let $A_i = R[I/b_i]$. Then the following are equivalent:*

(8.3.1) $a(I) = 1$.

(8.3.2) *There exists a regular element $b \in I$ such that b/b_i is a unit in A_i for $i = 1, \dots, g$.*

(8.3.3) *There exists a regular element $b \in I$ such that $A = R[b_1/b, \ldots, b_g/b] \subseteq A_i$ for $i = 1, \ldots, g$.*
(8.3.4) *There exists a regular element $b \in I$ such that $tI\mathbf{R} \subseteq Rad(tb\mathbf{R})$.*
(8.3.5) *There exist a regular element $b \in I$ and a positive integer k such that $I^{[k]} \subseteq bI^{k-1}$.*

Proof. Assume that (8.3.1) holds. Then since R/M is infinite, there exist a regular element $b \in I$ and a positive integer n such that $bI^{n-1} = I^n$. Therefore ${b_i}^n \in bI^{n-1}$ for $i = 1, \ldots, g$, so by dividing both sides of ${b_i}^n \in bI^{n-1}$ by ${b_i}^n$ it follows that $1 \in (b/b_i)(I^{n-1}/{b_i}^{n-1}) \subseteq (b/b_i)A_i$. Therefore b/b_i is a unit in A_i for $i = 1, \ldots, g$, so (8.3.1) $\Rightarrow$ (8.3.2).

Assume that (8.3.2) holds and fix $i \in \{1, \ldots, g\}$. Then $b_j/b = (b_j/b_i)(b_i/b) \in A_i$ for $j = 1, \ldots, g$, so $A \subseteq A_i$, so (8.3.2) $\Rightarrow$ (8.3.3). And if (8.3.3) holds, then $b_i/b \in A_i$ for $i = 1, \ldots, g$, so b/b_i is a unit in A_i; hence (8.3.3) $\Rightarrow$ (8.3.2).

Assume that (8.3.2) holds, fix $i \in \{1, \ldots, g\}$, and let $\mathbf{S} = A_i[tb_i, 1/tb_i]$, so $\mathbf{S} = \mathbf{R}[1/tb_i]$. Also, $u\mathbf{S} = b_i\mathbf{S} = b\mathbf{S}$ (since tb_i and b/b_i are units in $\mathbf{S}$), so it follows that $tb\mathbf{S} = b\mathbf{S} : u\mathbf{S} = \mathbf{S}$, so tb is a unit in $\mathbf{S}$. Therefore $(tb_i)^n \in tb\mathbf{R}$ for some integer $n \geq 1$ (since $\mathbf{S} = \mathbf{R}_S$ with $S = \{(tb_i)^n;\ n \geq 0\}$). Since this holds for $i = 1, \ldots, g$, it follows that $tI\mathbf{R} \subseteq Rad(tb\mathbf{R})$, so (8.3.2) $\Rightarrow$ (8.3.4).

Assume that (8.3.4) holds, so there exists a positive integer k such that $(tI)^k\mathbf{R} \subseteq tb\mathbf{R}$. Therefore by considering the homogeneous elements of degree k in the two homogeneous ideals $(tI)^k\mathbf{R}$ and $tb\mathbf{R}$ it follows that $I^k \subseteq bI^{k-1}$, and it is clear that $I^{[k]} \subseteq I^k$, so (8.3.4) $\Rightarrow$ (8.3.5).

Finally, assume that (8.3.5) holds. Then since $b \in I$ it follows that $I^{[k]} \subseteq bI^{k-1} \subseteq I^k$. Also, $I^{[k]}$ is a reduction of I^k, by (3.2.1), so bI^{k-1} is a reduction of I^k. Therefore it follows that $(I^k)^{n+1} = bI^{k-1}(I^k)^n = bI^{kn+k-1}$ for all large integers n, so bR is a reduction of I. Therefore $a(I) \leq 1$, and $a(I) \geq 1$ (since I is a regular ideal); hence $a(I) = 1$, so (8.3.5) $\Rightarrow$ (8.3.1). □

References

[ES] P. Eakin and A. Sathaye, *Prestable ideals*, J. Algebra **41** (1976), 439-454. MR **54:**7449

[HJLS] W. Heinzer, B. Johnston, D. Lantz, and K. Shah, *The Ratliff-Rush ideal in a Noetherian ring: A survey*, Methods In Module Theory, Lecture Notes in Pure and Applied Math, No. 140, 1993. MR **93k:**13004

[KMOR] D. Katz, S. McAdam, J. Okon, and L. J. Ratliff, Jr., *Essential prime divisors and projectively equivalent ideals*, J. Algebra **109** (1987), 468-478. MR **88i:**13016

[KR] D. Katz and L. J. Ratliff, Jr., *U-essential prime divisors and sequences over an ideal*, Nagoya Math. J. **103** (1986), 39-66. MR **87j:**13002

[M] S. McAdam, *Asymptotic Prime Divisors*, LNM vol 1023, Springer-Verlag, 1983. MR **85f:**13018

[MR] S. McAdam and L. J. Ratliff, Jr., *Persistent primes and projective extensions of ideals*, Comm. Algebra **16** (1988), 1141-1185. MR **89i:**13003

[N] M. Nagata, *Local Rings*, Interscience Tracts In Pure and Applied Math. No. 13, Interscience, New York, NY, 1962. MR **27:**5790

[NR] D. G. Northcott and D. Rees, *Reductions of ideals in local rings*, Math. Proc. Cambridge Philos. Soc. **50** (1954), 145-158. MR **15:**59a

[RR1] L. J. Ratliff, Jr. and David E. Rush, *Two notes on reductions of ideals*, Indiana Univ. Math. J. **27** (1978), 929-934. MR **58:**22034

[RR2] L. J. Ratliff, Jr. and David E. Rush, *Triangular powers of integers from determinants of binomial coefficient matrices*, Linear Algebra and Appl. (to appear).

[ZS1] O. Zariski and P. Samuel, *Commutative Algebra, Vol. I*, D. Van Nostrand Co., Inc., Princeton, NJ, 1958. MR **52:**5641

[ZS2] O. Zariski and P. Samuel, *Commutative Algebra, Vol. II*, D. Van Nostrand Co., Inc., Princeton, NJ, 1960. MR **52:**10706

Department of Mathematics, University of California, Riverside, California 92521
E-mail address: ratliff@math.ucr.edu

Department of Mathematics, University of California, Riverside, California 92521
E-mail address: rush@math.ucr.edu