Many associated primes of powers of primes
Jesse Kim and Irena Swanson
Department of Mathematics, UCSD, La Jolla, CA 92093-0112
Reed College, 3203 SE Woodstock Boulevard, Portland, OR 97202
jvkim@ucsd.edu, iswanson@reed.edu

Abstract. We construct families of prime ideals in polynomial rings for which the number of associated primes of the second power (or higher powers) is exponential in the number of variables in the ring.

Keywords and phrases: primary decomposition, powers of ideals, Rees algebra, extended Rees algebra, Rees-like algebra, polynomial rings.

2010 Mathematics Subject Classification. Primary 13A30, 13B25.

An inspiration for this work came from McCullough-Peeva’s paper [11] in which they constructed families of counterexamples to the Eisenbud-Goto conjecture via new constructions of step-by-step homogenizations and Rees-like algebras. McCullough and Peeva applied these constructions in particular to the Mayr-Meyer ideals from [10]. Mayr-Meyer ideals are computationally hard in the sense that they have large Castelnuovo-Mumford regularity (Bayer and Stillman [2]) and large ideal-membership coefficient degrees (Mayr and Meyer [10]). Another class of computationally hard ideals are permanental ideals ([17]). Papers [7], [8], [12], [14], [15] indicate that perhaps computational hardness is related to the large numbers of associated primes, but McCullough and Peeva showed that even prime ideals — so ideals with only one associated prime — can be computationally hard, namely that they can have very large Castelnuovo-Mumford regularity. This paper is a result of trying to understand why McCullough and Peeva’s Rees-like algebras and step-by-step homogenizations generate such “hard” prime ideals, and trying to determine whether the primes defining Rees-like algebras have large numbers of associated primes. While initially we worked with Rees-like algebras, we got tighter results with extended Rees algebras.

We construct classes of prime ideals $P$ in polynomial rings over fields such that the number of associated primes of $P^2$ is not bounded by any polynomial function in the number of variables. In Theorem 4.1 we construct a family of almost complete intersection prime ideals $P$ of height $n−1$ in $3n$ variables for which all $P^e$ with $e \geq 2$ have exactly $3^n$ embedded primes. These $P$ are generated by elements of degrees up to 3 (or by quasi-homogeneous elements of degrees up to 10). In Theorem 4.3 we construct for odd $n$ a family of prime ideals $P$ of height $\frac{n+1}{2}$ in $3n$ variables for which $P^2$ has at least $3^n + 3^{(n+7)/2}$ embedded primes. We know of no other class of ideals with such large numbers of associated prime ideals. The second author proved in [15] that there is an upper bound on the number of associated prime ideals of the Mayr-Meyer ideals that is doubly exponential in the number of variables, but it is not known whether the number of associated primes is in fact doubly
or even singly exponential.

Hermann [5] was the first to consider upper bounds on the numbers and degrees of primary components of ideals in polynomial rings over a field. Seidenberg proved in [13, Point 65] that there exists a primitive recursive function $B(n, d)$ that is at least doubly exponential in $n$ such that any ideal $I$ in a polynomial ring in $n$ variables over a field with generators of degree at most $d$ has at most $B(n, d)$ associated primes. Our Theorem 4.1 shows that $B(n, d) \geq 3^{n/3}$ for all $d \geq 3$. More recent proofs of upper bounds on the numbers of primary components are in the paper [18] by van den Vries and Schmidt and in the paper [1] by Ananyan and Hochster. The bound $E(m, d)$ given by Ananyan and Hochster depends on the upper bound $m$ on the generators of $I$ and on the upper bound $d$ of the degrees of the generators, and it does not depend on the number of variables. (Note that $B(n, d)$, while not explicitly invoking $m$, does get a free upper bound $\binom{n+d}{d}$ on $m$.) In Theorem 4.1 we construct a family of $(n+1)$-generated almost complete intersection prime ideals $P$ in $3n$ variables for which all $P^e$ with $e \geq 2$ have exactly $3^n$ embedded primes. Thus $P^2$ has at most $m = (n+2)(n+1)/2 \leq (n+2)^2/2$ generators, which shows that $E(m, d) \geq 3\sqrt[3]{2m-1}$.

We develop two new methods for generating ideals with large numbers of primary components: splitting, which is a generalization of the step-by-step homogenization, and spreading. Section 1 develops some basic properties of splitting. We show that splitting increases the number of associated primes in a controlled way; the number is bounded above by a polynomial in the number of variables in the new ring, and the polynomial is of degree that is equal to the largest number of variables contained in an associated prime of the original ideal. Splitting does not increase the number of variables in the associated primes; it increases the numbers of associated primes. With the goal of increasing the numbers of variables in associated primes we introduce in Section 2 the new notion of spreading. We determine the presenting ideal of the Rees algebra, of the extended Rees algebra, or of the Rees-like algebra of the spreading of an ideal $I$ from the presenting ideal of the same type of Rees algebra of $I$.

In Section 3 we compute the presenting ideal $P$ of the extended Rees algebra of a specific five-generated monomial ideal. The spreading of monomial ideals is easy to understand. In Section 4 we apply spreading and splitting to this $P$ to get the exponential results.

All rings in this paper are commutative with identity, and most are Noetherian.

Acknowledgements. We are grateful to the two anonymous referees for substantially improving the presentation and the proofs, in particular of Theorem 1.2 and of Lemmas 1.3 and 1.6. The paper is now greatly streamlined due to their comments, and the main results are stated without reliance on calculations by Macaulay2.
1 Splitting, flatness, primary decompositions

In this section we define splittings, we prove that they are faithfully flat maps, and we show that under splitting the number of associated primes increases. We give a lower bound for the number of associated primes, and we show that the bound is achieved when all exponents of variables in the splitting are equal to 1.

**Definition 1.1** Let $A$ be a ring. An **$A$-splitting** is an $A$-algebra homomorphism $\varphi : A[z] \rightarrow A[u_1, \ldots, u_n]$ given by $\varphi(z) = u_1^{p_1} \cdots u_n^{p_n}$, where $n, p_1, \ldots, p_n$ are positive integers and $z, u_1, \ldots, u_n$ are variables over $A$. We refer to this map as the $A$-splitting $z \mapsto u_1^{p_1} \cdots u_n^{p_n}$.

Step-by-step homogenization of McCullough-Peeva [11] is a special case of splitting with $n = 2$, $p_1 = 1$ and $p_2$ chosen carefully depending on the gradings. In this paper the splittings ignore any gradings.

The composition of splittings is a splitting. If we restrict the splittings to those for which at least one (resp. each) $p_i$ equals 1, then again the composition of two such splittings is of the same type.

**Theorem 1.2** Splitting is a free and thus a faithfully flat map.

Proof. Note that the $A$-splitting $z \mapsto u_1^{p_1} \cdots u_n^{p_n}$ is a composition of the $A$-splitting $A[z] \rightarrow A[u_1^{p_1}, \ldots, u_n^{p_n}]$ with the inclusion into the free extension $A[u_1, \ldots, u_n]$. So it suffices to prove that the $A$-splitting $A[z] \rightarrow A[u_1^{p_1}, \ldots, u_n^{p_n}]$ is free. But $u_1^{p_1}, \ldots, u_n^{p_n}$ are variables over $A$, so by possibly renaming them, it remains to prove that the splitting $z \mapsto u_1^{r_1} \cdots u_n^{r_n}$ is free. But $A[u_1, \ldots, u_n]$ is free over $A[u_1, \ldots, u_n] \cong A[z]$ with basis consisting of monomials $u_1^{i_1} u_2^{i_2} \cdots u_n^{i_n}$ with $i_1, i_2, \ldots, i_n$ non-negative integers of which at least one equals 0.

**Lemma 1.3** (This is a generalization of [3, Exercise 10.4].) Let $a, b$ be a regular sequence in a ring $R$ and let $u$ be a variable over $R$. Then $a$ is a non-zerodivisor on $R[u] / (au - b)R[u]$. If the zero ideal in $R$ is prime (resp. primary), then $(au - b)R[u]$ is a prime (resp. primary) ideal in $R[u]$.

Proof. Let $r \in (au - b) : a$. Then $ra = s(au - b)$ for some $s \in R[u]$. Since $a, b$ is a regular sequence in $R[u]$, this means that there exists $s' \in R[u]$ such that $r - su = s'b$ and $s = -s'a$. Hence $r = su + s'b = -s'(au - b) \in (au - b)$. This proves the first statement.

Let $B = R[u] / (au - b)R[u]$. Since $a$ is a non-zerodivisor on $B$ and on $R$, we can form localizations $R_a$ and $B_a$ at the multiplicatively closed set $\{1, a, a^2, \ldots\}$. Then $B$ injects into $B_a = R_a[u] / (u - b/a)R_a[u] \cong R_a$. Since the zero ideal in $R$ is prime (resp. primary), it is prime (resp. primary) in $R_a$ and hence also in $B_a$ and in its subring $B$. This says that $(au - b)R[u]$ is a prime (resp. primary) ideal in $R[u]$.

\[\square\]
Remark 1.4 It is not true in general with the set-up as in the lemma that for an integer $p > 1$, $(a u^p - b)A[u]$ is prime or primary. For example, if $a = c^p, b = d^p$ is a regular sequence for some $c, d \in R$, then $a u^p - b$ factors.

Lemma 1.5 Let $A$ be a ring and let $\varphi : A[z] \to A[u_1, \ldots, u_n]$ be the splitting map $z \mapsto u_1 \cdots u_n$. Let $q$ be a prime (resp. primary) ideal in $A[z]$ such that $z$ is not in the radical of $q$. Then $\varphi(q)A[u_1, \ldots, u_n]$ is prime (resp. primary) of the same height as $q$, and the $u_i$ are non-zerodivisors on $A[u_1, \ldots, u_n]/\varphi(q)A[u_1, \ldots, u_n]$.

Proof. Let $U$ stand for $u_1, \ldots, u_n$. Set $R = (A[z]/q)[U]$. By assumption, $u_2 \cdots u_n, z$ is a regular sequence on $R$. Since $u_1$ is a variable in $R$ over the obvious subring, we may apply Lemma 1.3 with $b = z, a = u_2 \cdots u_n, u = u_1$. Then by lifting we get that $qA[z][U] + (z - u_1 \cdots u_n)$ is a prime (resp. primary) ideal in $A[z][U]$, so that $\varphi(q)A[U] = (qA[z][U] + (z - u_1 \cdots u_n)) \cap A[U]$ is a prime (resp. primary) ideal in $A[U]$. Lemma 1.3 also says that the $u_i$ are non-zerodivisors on $R/(z - u_1 \cdots u_n)$, which by contraction means that they are non-zerodivisors on $A[U]/\varphi(q)A[U]$.

The height claim follows from faithful flatness of splittings. □

Lemma 1.6 Let $A$ be a Noetherian ring and let $\varphi : A[z] \to A[U] = A[u_1, \ldots, u_n]$ be the splitting map $z \mapsto u_1 \cdots u_n$. Let $q$ be a primary ideal in $A[z]$ that contains a power of $z$. Then

$$\varphi(q)A[U] = \bigcap_{i=1}^n \left( \varphi(q)A[U] : (u_1 \cdots u_{i-1} u_{i+1} \cdots u_n)_{\infty} \right)$$

is an irredundant primary decomposition. (Exponent $\infty$ stands for a very large integer; the colon ideals are independent of the large integer because the ring is Noetherian.)

The radical of $q$ can be written as $JA[z] + (z)$ with $J$ a prime ideal in $A$. Then the associated primes of $\varphi(q)A[U]$ are $JA[U] + (u_1), \ldots, JA[U] + (u_n)$. In particular, the heights of $q$ and $\varphi(q)A[U]$ are the same.

Proof. Let $Q$ be $\sqrt{q}$. Then $Q$ is a prime ideal in $A[z]$ containing $z$, so we can write it as $JA[z] + (z)$ for some prime ideal $J \subseteq A$. Then $\varphi(Q)A[U] = JA[U] + (u_1 \cdots u_n)$. Set $Q_i = JA[U] + (u_i)$. These are the prime ideals in $A[U]$ minimal over $\varphi(Q)A[U]$ and

$$\bigcap_{i=1}^n Q_i = JA[U] + (u_1 \cdots u_n) = \varphi(Q)A[U]$$

is an irredundant primary decomposition. Since $\varphi$ is flat by Theorem 1.2, an application of [9, Theorem 23.2] says that the associated primes of $qA[U]$ are precisely $Q_1, \ldots, Q_n$. Since $u_j \in Q_j \setminus Q_i$ for all distinct $i, j$, we get that the $Q_i$-primary component component of $\varphi(q)A[U]$ is $\varphi(q)A[U] : (u_1 \cdots u_{i-1} u_{i+1} \cdots u_n)_{\infty}$. □

It should be noted that splitting does not increase the numbers of variables in the associated primes.
Theorem 1.7 Let $A$ be a Noetherian ring, $m, n_1, \ldots, n_m$ positive integers, and let $A[Z] = A[z_1, \ldots, z_m]$ and $A[U] = A[u_{ij} : i = 1, \ldots, m; j = 1, \ldots, n_i]$ be polynomial rings over $A$. Let $\varphi : A[Z] \rightarrow A[U]$ be the $A$-algebra homomorphism with $z_i \mapsto u_{i1}^{p_{i1}} \cdots u_{in_i}^{p_{in_i}}$ for some positive integers $p_{ij}$. Let $I$ be an ideal in $A[Z]$ with an irredundant primary decomposition $I = q_1 \cap q_2 \cap \cdots \cap q_s$. Then the following statements hold.

1. The height of $\varphi(I)A[u_1, \ldots, u_n]$ equals the height of $I$.
2. The number of primary components of $\varphi(I)A[U]$ is the sum of the numbers of primary components of the $\varphi(q_i)A[U]$.
3. Let $I$ be a primary ideal in $A$. For $i = 1, \ldots, m$ let $\epsilon_i$ be 1 if $I$ contains a power of $z_i$ and let $\epsilon_i$ be 0 otherwise. Then $\varphi(I)A[U]$ has at least $n_1^{\epsilon_1} \cdots n_m^{\epsilon_m}$ primary components. If $p_{ij} = 1$ for all $(i, j)$ with $\epsilon_i = 1$, then $\varphi(I)A[U]$ has exactly $n_1^{\epsilon_1} \cdots n_m^{\epsilon_m}$ primary components. The counted corresponding associated prime ideals are of the form $\sqrt{I} \cap A + (u_{ij} : \epsilon_i > 0, j = 1, \ldots, n_i)$.

Proof. The homomorphism $\varphi$ is a composition of the $A$-algebra homomorphisms where each $z_i$ is split separately. By Theorem 1.2, $\varphi$ is faithfully flat, so that (1) holds. Also, flatness and [9, Theorem 23.2] say that an irredundant primary decomposition of $\varphi(I)A[U]$ equals the intersection of irredundant primary decompositions of the $\varphi(q_i)A[U]$. This proves (2).

Suppose that (3) holds in case all $p_{ij} = 1$. Then $I' = IA[z_i, u_{ij}^{p_{ij}} : i, j]/(z_i - u_{i1}^{p_{i1}} \cdots u_{in_i}^{p_{in_i}} : i)$ has the stated associated primes. But $A[z_i, u_{ij}^{p_{ij}} : i, j]/(z_i - u_{i1}^{p_{i1}} \cdots u_{in_i}^{p_{in_i}} : i) \cong A[z_i, u_{ij} : i, j]/(z_i - u_{i1}^{p_{i1}} \cdots u_{in_i}^{p_{in_i}} : i)$ is a free extension, so that an irredundant primary decomposition of $\varphi(I)A[U]$ contracts to a possibly redundant primary decomposition of $I'$. This means that the number of associated primes of $\varphi(I)A[U]$ is at least the number of primary components of $I'$. Thus it suffices to prove (3) in case all $p_{ij}$ equal 1. The case $m = 1$ follows from the previous two lemmas.

Now let $m > 1$. Let $\varphi_1$ be the splitting of $z_1$ and let $\varphi'$ be the splitting of $z_2, \ldots, z_m$ such that $\varphi = \varphi' \circ \varphi_1$. By the case $m = 1$, the number of primary components of $I' = \varphi_1(I)A[u_{11}, \ldots, u_{1n_1}]$ is $n_1^{\epsilon_1}$. By the previous two lemmas, for each $i > 1$ and for each primary component $q$ of $I'$, $q$ contains $z_i$ if and only if $I$ contains $z_i$. Thus by induction on $m$, the number of primary components of $\varphi'(q)A[U]$ is $n_2^{\epsilon_2} \cdots n_m^{\epsilon_m}$, with the stated form. By applying [9, Theorem 23.2] again due to faithful flatness, $\varphi(I)A[U] = \varphi'(I')A[U]$ has $n_1^{\epsilon_1} \cdots n_m^{\epsilon_m}$ primary components. The corresponding associated primes are in the stated form. \qed
2 Variable spreading

Splitting replaces one variable by a product of variables, it can be described by a homomorphism, and its effect is that after splitting an ideal, the number of associated prime ideals increases. By Theorem 1.7, the increase is limited by the number of variables in the associated primes of $I$, and it does not increase the number of variables in the associated primes. This section introduces a new method, which we call spreading, which adds more variables. A simple example is in Proposition 2.6, a more involved one in Theorem 2.9.

Here is an attempt at adding variables to associated primes. Let $P$ (resp. $Q$) be a prime ideal in a polynomial ring $k[x_1, \ldots, x_n]$ (resp. $k[y_1, \ldots, y_m]$) with the property that it contains no variables but all of its higher powers have embedded primes containing variables. (Such an example is in Example 3.1.) Suppose that $(P+Q)k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ is prime (say if $k$ is algebraically closed). Let $P^2 = P\cap p_1 \cap \cdots \cap p_r$ and $Q^2 = Q\cap q_1 \cap \cdots \cap q_s$ be primary decompositions. It turns out that the number of variables in the associated primes of $(P+Q)^2$ does not increase because $(P+Q)^2 = P^2 + PQ + Q^2$, with the algebraic closure assumption the ideals $p_i + Q$ and $P + q_j$ are primary, and the intersection of these primary ideals is $(P+Q)^2$ by using that $\otimes k[x]/P$ and $\otimes k[y]/Q$ are flat. Thus the associated primes of $(P+Q)^2$ are $P + Q$, $\sqrt{p_i + Q}$, $P + \sqrt{q_j}$, and thus the number of variables in any embedded prime of $(P+Q)^2$ is the same as such a number for $P^2$ and $Q^2$. However, by [16, Theorem 1.5], $\sqrt{p_i} + \sqrt{q_j}$ are associated to higher powers of $P + Q$, so that we can get an increase in the number of variables appearing in an associated prime of higher powers of $P + Q$.

**Definition 2.1** $(S_z, d_z, S_u, d_u, \varphi)$ is called an **A-spreading** if the following conditions are satisfied:

1. $S_z$ and $S_u$ are $A$-algebras.
2. $d_z, d_u$ are gradings on $S_z, S_u$, respectively, with degrees in possibly distinct commutative monoids $M_z, M_u$ that are submonoids of free $\mathbb{Z}$-modules.
3. $\varphi : S_u \to S_z$ is an $A$-algebra homomorphism that takes homogeneous components to homogeneous components; by abuse of notation we write $\varphi : M_u \to M_z$ so that for any homogeneous $f \in S_u$, $\varphi(d_u(f)) = d_z(\varphi(f))$.
4. If $f$ and $g$ are homogeneous elements in $S_u$, then the degree of $\varphi(fg)$ is the sum of the degrees of $\varphi(f)$ and $\varphi(g)$. In other words, $d_z(\varphi(fg)) = d_z(\varphi(f)) + d_z(\varphi(g))$.

With the abuse of notation from (3), this is saying that $d_z \circ \varphi$ is a monoid homomorphism.

Given such an A-spreading, the **spreading of a homogeneous ideal $I$ in $S_z$** is

$$\text{spr}(I) = \{ f \in S_u : f \text{ is homogeneous and } \varphi(f) \in I \}.$$
Example 2.2 Let $A = k[a, b]$ where $k$ is a field and $a$ and $b$ are variables over $k$. Let $S_z = A[c], S_u = A[c_1, \ldots, c_n], d_z$ and $d_u$ trivial on $A$, $d_z(c) = 1$, and $\varphi : S_u \to S_z$ given by $\varphi(c_i) = c$ for all $i$. Let $J = (a^2b^2c, b^4, ab^3, a^3b, a^4) \subseteq S_z$.

1. Let $d_u(c_j) = 1$ for all $j$. Then $\text{spr}(J) = (a^2b^2c_1, b^4, ab^3, a^3b, a^4, c_1 - c_2, \ldots, c_1 - c_n)$.
2. Let $d_u(c_j) = e_j$, where $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ has 1 in the $j$th entry. Then $\text{spr}(J) = (a^2b^2c_1, \ldots, a^2b^2c_n, b^4, ab^3, a^3b, a^4)$.

Note that $\varphi(c_1 - c_2) = 0 \in J$ regardless of the grading, but that $c_1 - c_2$ is not in $\text{spr}(J)$ when it is not homogeneous.

Remarks 2.3 Let $I \subseteq J$ be homogeneous ideals in $S_z$.

1. $\varphi(\text{spr}(I)) \subseteq I$. Equality need not hold: say if $S_z = A[z], S_u = A[u_1, \ldots, u_n]$ are polynomial rings over $A$ and $\varphi(u_i) = z^2$, then $\text{spr}(z) = (u_1, \ldots, u_n)$ and $\varphi(\text{spr}(z)) = \varphi(u_1, \ldots, u_n) = (z)^2 \subseteq (z)$.
2. If $I \subseteq J$, then $\text{spr}(I) \subseteq \text{spr}(J)$.
3. For all ideals $I, J$ in $S_z$, $\text{spr}(I) \text{spr}(J) \subseteq \text{spr}(IJ)$.

In general, $\text{spr}(I) \text{spr}(J)$ need not equal $\text{spr}(IJ)$ and $\text{spr}(I')$ need not equal $(\text{spr}(I))^r$.

For example, let $S_z = A[z], S_u = A[u_1, \ldots, u_n]$ and $\varphi$ take $u_i$ to $z$. First suppose that $d_u$ is the trivial (zero) grading. Then $\text{spr}(z^r) = (u_1^r, u_1 - u_2, \ldots, u_1 - u_n)$. The element $u_1 - u_2$ is thus not in any higher power of $\text{spr}(z)$ but it is in $\text{spr}(z^r)$ for every positive integer $r$.

If instead we choose the grading $d_u(u_i) = e_i$ for all $i$ and change $\varphi$ to $\varphi(u_i) = z^2$, then $\text{spr}(z) = \text{spr}(z^2) = (u_1, \ldots, u_n)$, so that spreading again does not commute with powers.

Here is another example: Let $S_z = A[z_1, z_2, \ldots, z_m]$ for some $m \geq 2, S_u = A[u_{ij} : i = 1, \ldots, m; j = 1, \ldots, u_n], \varphi(u_{ij}) = z_i$ and $d_u(u_{ij}) = e_j$. The spreading does not commute with powers as the spreading of every ideal contains $u_{11}u_{22} - u_{12}u_{21}$.

Lemma 2.4 Spreading commutes with radicals. The spreading of a radical (resp. prime, primary) ideal is radical (resp. prime, primary).

Proof. Let $I$ be a homogeneous ideal in $S_z$. Certainly $\sqrt{I}, \text{spr}(I)$ are homogeneous.

First suppose that $I$ is a radical ideal. Let $f \in S_u$ be in the radical of $\text{spr}(I)$. We want to prove that $f \in \text{spr}(I)$. It suffices to prove the result in case $f$ is homogeneous. For some large $N$, $f^N \in \text{spr}(I)$, so $(\varphi(f))^N = \varphi(f^N) \in I$. Since $I$ is radical, it follows that $\varphi(f) \in I$ and so $f \in \text{spr}(I)$. This proves that the spreading of a radical ideal is radical.

In general, $\text{spr}(I) \subseteq \text{spr}(\sqrt{I})$, so that the radical of $\text{spr}(I)$ is contained in the radical ideal $\text{spr}(\sqrt{I})$. We next prove the opposite inclusion. If $f$ in $\text{spr}(\sqrt{I})$ is homogeneous, then $\varphi(f) \in \sqrt{I}$, so that for some large integer $N$, $\varphi(f^N) = (\varphi(f))^N \in I$. Hence $f^N \in \text{spr}(I)$. This proves that the radical of $\text{spr}(I)$ equals $\text{spr}(\sqrt{I})$, so that spreading commutes with radicals.

Now let $f, g \in S_u$ be homogeneous such that $fg \in \text{spr}(I)$. Then $\varphi(f)\varphi(g) = \varphi(fg) \in I$.

If $I$ is prime, then either $\varphi(f)$ or $\varphi(g)$ is in $I$, so that either $f$ or $g$ is in $\text{spr}(I)$. Thus by homogeneity of ideals, $\text{spr}(I)$ is a prime ideal.
If $I$ is primary and $f \not\in \spr(I)$, then $\varphi(f) \not\in I$, so that $\varphi(g) \in \sqrt{I}$. But then $g \in \spr(\sqrt{I}) = \sqrt{\spr(I)}$. Thus $\spr(I)$ is primary. \hfill $\square$

**Lemma 2.5** Spreading commutes with intersections of homogeneous ideals. In particular, it commutes with (homogeneous) primary decompositions.

Surjective spreading takes irredundant primary decompositions to irredundant primary decompositions.

**Proof.** Let $I = q_1 \cap \cdots \cap q_r$ be an intersection of homogeneous ideals in $S_z$. Then $\spr(I) \subseteq \spr(q_1) \cap \cdots \cap \spr(q_r)$. To prove equality, let $f$ be a homogeneous element in $\spr(q_1) \cap \cdots \cap \spr(q_r)$. Then $\varphi(f) \in \varphi(\spr(q_1)) \cap \cdots \cap \varphi(\spr(q_r)) \subseteq q_1 \cap \cdots \cap q_r = I$, so that $f \in \spr(I)$. This proves that spreading commutes with intersections.

By Lemma 2.4, if $q_i$ is primary, so is $\spr(q_i)$, so that spreading commutes with primary decompositions.

Suppose that $\varphi$ is surjective and that $\spr(I) = \spr(q_2) \cap \cdots \cap \spr(q_r)$. Let $a \in q_2 \cap \cdots \cap q_r$. By surjectivity there exists $b \in \spr(q_2) \cap \cdots \cap q_r$ such that $a = \varphi(b)$. But then $b \in \spr(q_2) \cap \cdots \cap \spr(q_r) = \spr(I)$, so that $a = \varphi(b) \in I$, which says that $q_1$ was an irredundant primary component of $I$. This proves the lemma. \hfill $\square$

The following is a special case of spreading:

**Proposition 2.6** Let $z, z_1, \ldots, z_n$ be variables over a Noetherian ring $A$, let $I$ be an ideal in $A[z]$ and let $J = I + (z - z_1, \ldots, z - z_n)$ be an ideal in $R = A[z, z_1, \ldots, z_n]$. Then the following hold for a positive integer $e$.

1. If an associated prime ideal $P$ of $I^e$ contains $z$, then an associated prime ideal of $J^e$ contains $P$ and $n + 1$ variables $z, z_1, \ldots, z_n$.

2. If $z$ is not a zerodivisor on $A[z]/I^e$, then $J^e : z \subseteq I^e + (z - z_1, \ldots, z - z_n)$.

**Proof.** Set $S_z = A[z], S_u = R, d_u$ and $d_z$ both zero on $A$ and with value 1 on the variables. Let $\varphi : S_u \to S_z$ be the $A[z]$-algebra homomorphism that maps $z_i$ to $z$. Then $(S_z, d_z, S_u, d_u, \varphi)$ is a surjective $A$-spreading, and $J = \spr(I)$.

Let $P$ be an associated prime ideal of $I^e$ such that $z \in P$. By a characterization of associated primes, $P = I^e : a$ for some $a \in S_z \setminus I^e$. If $a \in J^e$ then $a = \varphi(a) \in \varphi(J^e) = I^e$, which is a contradiction. So $J^e : a$ is a proper ideal and so necessarily contained in some associated prime $Q$ of $J^e$. This $Q$ contains $z$ and also $z - z_1, \ldots, z - z_n$, hence it contains $z, z_1, \ldots, z_n$. (Note that Lemma 2.5 proves (1) in case $e = 1$ but not in case $e > 1$.)

Suppose that $z$ is not a zerodivisor on $S_z/I^e$. Let $b \in S_u$ such that $zb \in J^e$. Then $z\varphi(b) = \varphi(zb) \in \varphi(J^e) = I^e$. By assumption then $\varphi(b) \in I^e$, so that $b \in J^e + (z - z_1, \ldots, z - z_n) = I^e + (z - z_1, \ldots, z - z_n)$. \hfill $\square$

**Definition 2.7** An $A$-spreading $(S_z, d_z, S_u, d_u, \varphi)$ is called full if for any $d_u$-degree $\underline{a}$, $\varphi$ restricted to $(S_u)_{\underline{a}}$ is injective into $(S_z)_{\varphi(\underline{a})}$. 

Example 2.8 The following is an example of a non-injective full spreading. Let \( m, v_1, \ldots, v_m \) be positive integers, \( S_z = A[z_1, \ldots, z_m] \) and \( S_u = A[u_{ij} : i = 1, \ldots, m; j = 1, \ldots, v_i] \). Let \( \varphi(u_{ij}) = z_i \) and \( \varphi|_A = id \). Let \( d_z \) be the monomial \( \mathbb{N}^m \)-grading on \( S_z \) with \( d_z(A) = 0 \) and \( d_z(z_i) = e_i \), and let \( d_u \) be the monomial \( \mathbb{N}^N \)-grading on \( S_u \) with \( d_u(A) = 0 \) and \( d_u(u_{ij}) = e_{v_i+1} + v_{i+1} + \cdots + v_{i+1+j} \). The verification of the full property is straightforward since every homogeneous element in \( S_z \) (resp. \( S_u \)) is of the form \( am \) for some \( a \in A \) and some monomial \( m \) in the \( z_i \) (resp. in the \( u_{ij} \)).

Recall that for an ideal \( J \) in a ring \( A \), its Rees algebra is \( A[Jt] \), its extended Rees algebra is \( A[Jt, t^{-1}] \), and its Rees-like algebra is \( A[Jt, t^2] \), where \( t \) is a variable over \( A \). In the rest of this section we use the presenting ideal of a Rees algebra of an ideal \( J \) to construct the prime ideal presenting the same type of Rees algebra of a full spreading of \( J \).

Set-up: Let \((S_z, d_z, S_u, d_u, \varphi)\) be an \( A \)-spreading of Noetherian rings. Let \( a_1, \ldots, a_m \) be homogeneous elements in \( S_z \) and let \( J = (a_1, \ldots, a_m) \). Let \( \text{spr}(J) \) have \( m' \) homogeneous generators. Let \( t, \sigma, Z = Z_1, \ldots, Z_m, U_1, \ldots, U_{m'} \) be variables over \( S_z \) and \( S_u \).

Let \( \tilde{\varphi} : S_u[t, t^{-1}] \to S_z[t, t^{-1}] \) be the \( A \)-algebra homomorphism that agrees with \( \varphi \) on \( S_u \) and such that \( \varphi(t^\pm 1) = t^\pm 1 \). The grading on \( S_z[t, t^{-1}] \) is as follows: the degree of a homogeneous element \( s \in S_z \subseteq S_z[t, t^{-1}] \) is \((d_z(s), 0)\) and the degree of \( t^\pm 1 \) is \((0, \pm 1)\). The grading on \( S_u[t, t^{-1}] \) is defined similarly.

All three types of Rees algebras of \( J \) are subrings of \( S_z[t, t^{-1}] \). Let \( \psi_z : S_z[Z, T] \to S_z[t, t^{-1}] \) be the \( S_z \)-algebra homomorphism which takes \( Z_i \) to \( a_it \), and which takes \( T \) to one of \( 0, t^{-1}, t^2 \), depending on whether we are using Rees algebra, extended Rees algebra, or the Rees-like algebra. The image of \( \psi_z \) is the chosen type of the Rees algebra of \( J \). To make this map graded, we impose the grading \( d_Z \) on \( S_z[Z, T] \) as follows: \( d_Z(s) = (d_z(s), 0) \) for all \( s \in S_z \), \( d_Z(Z_i) = (d_z(a_i), 1) \) for all \( i = 1, \ldots, m \), and the degree of \( T \) is \( \infty \), \((0, -1)\), or \((0, 2)\) depending on the type of the Rees algebra. (Instead of \( d_Z(T) = \infty \) in case of a Rees algebra we can simply not adjoin \( T \).)

Analogously we define the grading \( d_U \) on \( S_u[U, T] \), and we let \( \psi_u : S_u[U, T] \to S_u[t, t^{-1}] \) be a graded \( S_u \)-algebra homomorphism whose image is a Rees algebra of \( \text{spr}(J) \), this Rees algebra being of the same type as the constructed algebra for \( J \). With this we have the following commutative diagram:

\[
\begin{array}{ccc}
J \subseteq S_z & \subseteq & S_z[Z, T] \xrightarrow{\psi_z} \text{Rees algebra of } J \subseteq S_z[t, t^{-1}] \\
\uparrow \varphi & & \uparrow \tilde{\varphi} \\
\text{spr}(J) \subseteq S_u & \subseteq & S_u[U, T] \xrightarrow{\psi_u} \text{Rees algebra of } \text{spr}(J) \subseteq S_u[t, t^{-1}]
\end{array}
\]

Note that \( \tilde{\varphi} \) takes the Rees algebra of \( \text{spr}(J) \) to the Rees algebra of \( J \). Let \( \Phi \) be the restriction map of \( \tilde{\varphi} \). We next define \( \Phi : S_u[U, T] \to S_z[Z, T] \) as \( \Phi|_S = \varphi \), \( \Phi(T) = T \), and \( \Phi(U_i) = f_i \) where \( f_i \) is a homogeneous element of \( S_z[Z, T] \) such that \( \psi_z(f_i) = \tilde{\varphi}(\psi_u(U_i)) \).
Then the following diagram commutes:

\[
\begin{array}{ccc}
J \subseteq S_z & \subseteq & S_z[Z,T] \\
\uparrow \varphi & \uparrow \Phi & \uparrow \tilde{\varphi} \\
\text{Rees algebra of } J & \subseteq & S_z[t,t^{-1}] \\
\end{array}
\]

\[
\begin{array}{ccc}
\text{spr}(J) \subseteq S_u & \subseteq & S_u[U,T] \\
\uparrow \psi_u & \uparrow \hat{\psi}_u & \uparrow \tilde{\psi}_u \\
\text{Rees algebra of } \text{spr}(J) & \subseteq & S_u[t,t^{-1}] \\
\end{array}
\]

**Theorem 2.9** \((S_z[Z,T], d_z, S_u[U,T], d_U, \Phi)\) is an \(A\)-spreading.

1. If \(\varphi\) is surjective, then there exists a surjective \(\hat{\Phi}\).
2. \(\ker(\psi_u) \subseteq \text{spr}(\ker(\psi_z))\).
3. If \(\varphi\) is full, then \(\text{spr}(\ker(\psi_z)) = \ker(\psi_u)\). In other words, when \(\varphi\) is full then the spreading of the presenting ideal of a type of Rees algebra of \(J\) equals the presenting ideal of the same type of Rees algebra of the spreading of \(J\).

**Proof.** The set-up makes \((S_z[Z,T], d_z, S_u[U,T], d_U, \Phi)\) a spreading.

Suppose that \(\varphi\) is surjective. Then \(\tilde{\varphi}\) and \(\hat{\varphi}\) are surjective as well. We may order a generating set of \(\text{spr}(J)\) so that the image under \(\varphi\) of the \(i\)th generator is \(a_i\) for \(i \leq m\). We then set \(\Phi(U_i) = Z_i\) for \(i \leq m\), which makes \(\Phi\) surjective.

Let \(f \in \ker(\psi_u)\). Since \(\psi_u\) is a graded homomorphism, every homogeneous component of \(f\) is in \(\ker(\psi_u)\), so that to prove that \(f \in \text{spr}(\ker(\psi_z))\) without loss of generality we may assume that \(f\) is homogeneous. Then \(\psi_z \circ \Phi(f) = \hat{\varphi} \circ \psi_u(f) = 0\), so that \(\Phi(f) \in \ker(\psi_z)\). Thus \(f \in \text{spr}(\ker(\psi_z))\).

Now let \(\varphi\) be full and let \(f \in \text{spr}(\ker(\psi_z))\) be homogeneous. Then \(\Phi(f) \in \ker(\psi_z)\), so that \(0 = \psi_z \circ \Phi(f) = \hat{\varphi} \circ \psi_u(f)\). Since \(\varphi\) is injective on homogeneous components, so are \(\tilde{\varphi}\) and \(\hat{\varphi}\), so that \(\psi_u(f) = 0\). Thus \(f \in \ker(\psi_u)\).

\(\square\)

### 3 Examples

This section provides a few examples of prime ideals whose powers have embedded primes that contain variables. These examples are used in Section 4 as a base for generating prime ideals whose powers have many associated primes containing many variables.

The first example below treats all powers of a prime ideal, whereas the second example is about the second power only.

**Example 3.1** Let \(P\) be the kernel of the \(k\)-algebra homomorphism \(k[x, y, z] \to k[t^3, t^4, t^5]\) taking \(x\) to \(t^3\), \(y\) to \(t^4\), \(z\) to \(t^5\). Then \(P\) is a prime ideal of height two, it contains no variables, and by [6], \((x, y, z)\) is associated to \(P^e\) for all \(e \geq 2\), and \(\bigcup_{e=1}^{\infty} \text{Ass}(k[x, y, z]/P^e) = \{P, (x_1, y, z)\}\).
Proposition 3.2 In any polynomial ring in nine variables over an arbitrary field there exists a binomial prime ideal $P$ of height 5 containing no variables such that $P^2$ has exactly two embedded associated prime ideals: one of the two is a monomial ideal generated by eight variables and the other is the maximal ideal generated by the nine variables.

Proof. Let $k$ be a field, $a, b, c, Z_1, \ldots, Z_5, t, T$ variables over $k$, let $A = k[a, b, c]$, $J = (a^2b^2c, b^4, ab^3, a^3b, a^4)$, and $R = k[a, b, c, Z_1, Z_2, Z_3, Z_4, Z_5, T]$. Let $B = A[t, t^{-1}] \subseteq A[t, t^{-1}]$ be the extended Rees algebra of $J$. There is a natural surjective $A$-algebra map $R \to B$, with $Z_i$ mapping onto $t$ times the $i$th listed generator of $J$, and with $T$ mapping to $t^{-1}$. Let $P$ be the kernel of this map.

Then $P$ is a prime ideal that contains no variables. As the dimension of the Rees algebra is 4, the height of $P$ is 5. Rees algebras of monomial ideals are generated by binomials.

It is easy to verify that the following elements are in $P$: $f_1 = a^4 - Z_5T$, $f_2 = aZ_2 - bZ_3$, $f_3 = aZ_4 - bZ_5$, $f_4 = ab^3 - Z_3T$, $f_5 = a^3Z_3 - b^3Z_5$, $f_6 = a^4Z_2 - b^4Z_5$, $f_7 = a^2Z_1 - b^2cZ_5$, $f_8 = a^2b^2c - Z_1T$, $f_9 = Z_1Z_5 - cZ_4^2$, $f_{10} = Z_1Z_2 - cZ_2^2$, $f_{11} = aZ_1 - bcZ_4$, $f_{12} = Z_1^2 - c^2Z_3Z_4$, $f_{13} = Z_2T - b^4$, $f_{14} = Z_2^2Z_4 - Z_3^4$, $f_{15} = Z_2^3Z_5 - Z_3^4$, $f_{16} = acZ_3 - bZ_1$, $f_{17} = a^3b - Z_4T$, $f_{18} = a^2Z_3 - b^2Z_4$. We do not claim that these elements generate $P$.

Consider $\alpha = a^4Z_2 - a^3bZ_3 - ab^3Z_4 + b^4Z_5 - Z_2Z_5T + Z_3Z_4T$. If $\alpha \in P^2$, then under the lexicographic order $a > b > c > Z_1 > Z_2 > \cdots > Z_5 > T$, the leading monomial $a^4Z_2$ must be a product of two leading terms of elements of $P$. By the structure of the kernels of monomial maps, neither $a^3$ nor $Z_2$ can be multiples of leading terms of elements of $P$, which means that $\alpha$ is not in $P^2$. One can verify that

$$aa = a^5Z_2 - a^4bZ_3 - a^2b^3Z_4 + ab^4Z_5 - aZ_2Z_5T + aZ_3Z_4T = f_1f_2 - f_3f_4 \in P^2.$$ 

Since $a \not\in P$, this proves that $P^2$ has an embedded prime ideal which contains $P^2 : \alpha$ and thus $a$. If we invert $c$ or set $c = 1$, then the resulting $\alpha$ is still not in $P^2$ but $aa \in P^2$. This proves that $c$ is not in the radical of $P^2 : \alpha$, so that at least one of the embedded prime ideals of $P^2$ does not contain $c$.

After inverting $a$, the ideal $(f_1, f_3, f_5, f_6, f_7)$ equals $(a^{-4}Z_5T - 1, Z_4 - bZ_5/a, Z_3 - b^3Z_5/a^3, Z_2 - b^4Z_5/a^4, Z_1 - b^2cZ_5/a^2)$, which is a prime ideal in $R_a$ of height 5 and contained in $P_b$. By the height consideration, $P_b$ must equal this five-generated ideal. Similarly, after inverting $Z_1$, $P$ is the complete intersection prime ideal $(f_8, f_9, f_{10}, f_{11}, f_{12})Z_1 = (T - a^2b^2cZ_1^{-1}, Z_5 - cZ_4^2Z_1^{-1}, Z_2 - cZ_4^2Z_1^{-1}, a - bcZ_4Z_1^{-1}, 1 - c^2Z_3Z_4Z_1^{-1})$, after inverting $Z_2$, $P$ is the complete intersection prime ideal $(f_2, f_{10}, f_{13}, f_{14}, f_{15})Z_2 = (a - bZ_2Z_1^{-1}, Z_1 - cZ_3Z_2^{-1}, T - b^4Z_2^{-1}, Z_4 - Z_3^3Z_2^{-2}, Z_5 - Z_3^4Z_2^{-3})$, and after inverting $Z_3$, $P$ is the complete intersection prime ideal $(f_2, f_4, f_{10}, f_{14}, f_{15})Z_3 = (b - aZ_2Z_3^{-1}, T - ab^3Z_3^{-1}, c - Z_1Z_2Z_3^{-2}, Z_5 - Z_3^4Z_3^{-3}, 1 - Z_2Z_4Z_3^{-1})$. Furthermore, after localization at $T$, $P_T$ is generated by the variables $Z_1 - a^2b^2cT^{-1}$, $Z_2 - b^4T^{-1}$, $Z_3 - ab^3T^{-1}$, $Z_4 - a^3bT^{-1}$, $Z_5 - a^4T^{-1}$. Whenever an ideal in a Cohen-Macaulay ring is generated by a regular sequence, its powers have no embedded primes. So we just proved that $a, Z_1, Z_2$ and $Z_3, T$ must be contained in
every embedded prime of every power of $P$. By symmetry, $a, b, Z_1, Z_2, Z_3, Z_4, Z_5, T$ must be contained in all the embedded primes of powers of $P$.

Thus we have proved that $P^2$ has an embedded associated prime ideal and that each embedded prime ideal contains $(a, b, Z_1, Z_2, Z_3, Z_4, Z_5, T)$. By multihomogeneity of $J$ and of the extended Rees algebra, then the only possible associated primes of $P^2$ are $Q_1 = (a, b, Z_1, Z_2, Z_3, Z_4, Z_5, T)$ and $Q_2 = (a, b, c, Z_1, Z_2, Z_3, Z_4, Z_5, T)$. Since we proved that at least one embedded prime ideal does not contain $c$, we get that $Q_1$ is associated to $P^2$.

We next prove that $Q_2$ is also associated to $P^2$. Consider $\beta = a^5 Z_3 - 2a^3 b^2 Z_4 + a^2 b^3 Z_5 - aZ_3 Z_5 T + bZ_4^2 T$. If $\beta \in P^2$, then under the lexicographic order $a > b > c > Z_1 > Z_2 > \cdots > Z_5 > T$, the leading monomial $a^5 Z_3$ must be a product of the leading terms of two elements of $P$. By the structure of the kernels of monomial maps, neither $a^3$ nor $aZ_3$ can be multiples of leading terms of elements of $P$, which means that $\beta \notin P^2$. However,

$$c\beta = a^5 cZ_3 - 2a^3 b^2 cZ_4 + a^2 b^3 cZ_5 - acZ_3 Z_5 T + bcZ_4^2 T = f_1 f_{16} + f_{11} f_{17} - f_8 f_{18}.$$ 

This proves that $Q_2$ is associated to $P^2$.

The proof shows more:

**Proposition 3.3** Let $k$ be an arbitrary field, let $a, b, c, Z_1, \ldots, Z_5, T$ be variables over $k$, let $R = k[a, b, c, Z_1, \ldots, Z_5, T]$, and let $P$ be the kernel of the $k[a, b, c]$-algebra surjection from $R$ to the extended Rees algebra of the monomial ideal $(a^2 b^2 c, b^4, ab^3, a^3 b, a^4) \subseteq k[a, b, c]$, where $Z_i$ maps to the $i$th listed generator of $J$ and $T$ maps to $t^{-1}$. Then there exist $\alpha, \beta \in k[a, b, Z_2, Z_3, Z_4, Z_5, T]$ such that $(a, b, Z_1, \ldots, Z_5, T)$ is the radical of $P^2 : \alpha$ and such that the maximal ideal $(a, b, c, Z_1, \ldots, Z_5, T)$ is the radical of $P^2 : \beta$. (We emphasize: no variables $c$ and $Z_1$ appear in $\alpha$ and $\beta$.)

**Proof.** Proposition 3.2 shows that $P^2 = P^{(2)} \cap J_1 \cap J_2$, where $J_1$ is primary to $(a, b, Z_1, \ldots, Z_5, T)$ and $J_2$ is primary to $(a, b, c, Z_1, \ldots, Z_5, T)$.

We take $\alpha, \beta$ as in the proof of Proposition 3.2. Since $aa \in P^2$ and since $a$ is a non-zero divisor on $R/P^{(2)}$, it follows that $\alpha \in P^{(2)}$. Thus $P^2 : \alpha = (J_1 : \alpha) \cap (J_2 : \alpha) \neq R$. Since $c$ is not in the radical of $P^2 : \alpha$ (see the proof of Proposition 3.2), necessarily $J_1 : \alpha \neq R$. Thus the radical of $P^2 : \alpha$ is $(a, b, Z_1, \ldots, Z_5, T)$.

Since $c\beta \in P^2$ and since $c$ is a non-zero divisor on $R/P^{(2)}$ and on $R/J_1$, it follows that $\beta \in P^{(2)} \cap J_1$. Thus $P^2 : \beta = J_2 : \beta \neq R$ must be primary to the maximal ideal.

**Remark 3.4** Work similar to that in the proof of Proposition 3.2 shows that if $P$ is the presenting ideal of the Rees algebra $A[Jt]$ of $J$, then $P$ is a prime ideal of height 4 in a polynomial ring in eight variables, that $(a, b, Z_1, Z_2, Z_3, Z_4, Z_5)$ is associated to $P^2$ and that the only other candidate for an embedded associated prime of $P^2$ is $(a, b, c, Z_1, Z_2, Z_3, Z_4, Z_5)$. Macaulay2 [4] computes that the latter ideal is not associated to $P^2$.

If $P$ is the presenting ideal of the Rees-like algebra $A[Jt, t^2]$ of $J$, then we can similarly show that $P$ is a prime ideal of height 5 in a polynomial ring in nine variables, that either
We get that either $Q$ or $(a, b, Z_1, Z_2, Z_3, Z_4, Z_5)$ or $(a, b, Z_1, Z_2, Z_3, Z_4, Z_5, T)$ is associated to $P^2$ and that the only other candidates for embedded associated primes of $P^2$ are $(a, b, c, Z_1, Z_2, Z_3, Z_4, Z_5)$ and $(a, b, c, Z_1, Z_2, Z_3, Z_4, Z_5, T)$. Macaulay2 [4] computes that only the first and the third prime ideals on this list are associated to $P^2$.

4 Prime ideals whose powers have many associated prime ideals

We exploit splitting and spreading to generate prime ideals whose specific powers have arbitrarily many associated prime ideals.

Theorem 4.1 Let $k$ be an arbitrary field, and let $m \geq 3$ and $v_1, \ldots, v_m$ be any positive integers. Then there exists a polynomial ring $R$ in $\sum v_i$ variables over $k$ with an $m$-generated prime ideal $P$ of height $m - 1$ with generators of degree at most 3 (or with quasi-homogeneous generators of degree at most 10) such that for all integers $e \geq 2$, $P^e$ has $\prod v_i$ embedded primes, all of which have height $m$.

In case all $v_i$ equal $v$, this says that there exists a polynomial ring in $mv$ variables over a field $k$ with an $m$-generated prime ideal $P$ of height $m - 1$ such that $P^e$ has $v^m$ embedded primes if $e \geq 2$. The number $v^m = (\sqrt[v]{v})^{mv}$ is exponential in the number $mv$ of variables if we think of $v$ as fixed.

Proof. Let $x, y, z, z_1, \ldots, z_{m-3}$ be variables over $k$. Let $I = (x^3 - yz, y^2 - xz, z^2 - x^2y) \subseteq k[x, y, z]$ be the prime ideal as in Example 3.1. Set $R_m = k[x, y, z, z_1, \ldots, z_{m-3}]$ and $I_m = (x^3 - yz, y^2 - xz, z^2 - x^2y, z_1 - z, \ldots, z_{m-3} - z)$. Then $R_m$ is a polynomial ring in $m$ variables over $k$ and $I_m$ is a prime ideal in $R_m$ of height $m - 1$. By Proposition 2.6, $I_m$ is a spreading of $I$. By Example 3.1, for all integers $e \geq 2$, $I^e$ has exactly one embedded prime ideal, namely $(x, y, z)$. Then by Proposition 2.6, the maximal ideal $J = (x, y, z, z_1, \ldots, z_{m-3})$ in $R_m$ is an associated prime ideal of $I^e_m$. Suppose that $Q$ is associated to $I^e_m$. Since $I_m$ has height $m - 1$, the height of $Q$ is either $m - 1$ or $m$, so that by quasi-homogeneity of $I_m$ we get that either $Q = I_m$ or $Q = J$. This proves that for all integers $e \geq 2$, the set of associated primes of $I^e_m$ consists of $I_m$ and $J$.

Let $\varphi : R_m \to A$ be the splitting which for $i = 1, \ldots, m$ splits the $i$th variable into $v_i$ variables. Set $P = \varphi(I_m)A$. Then by Theorem 1.7, $A$ is a polynomial ring in $\sum v_i$ variables over $k$, $P$ is a prime ideal of height $m - 1$, and $P^e$ has $1 + v_1 \cdots v_m$ primary components for all $e \geq 2$. Each of the embedded components is the splitting of $J$ and is thus generated by $m$ variables.

The number of generators of $P$ is at most the number of generators $m$ of $I_m$. Since the height of $P$ is $m - 1$, the number of generators is at least $m - 1$, and since higher powers of $P$ have embedded primes, $P$ cannot be a complete intersection, so that the number of generators of $P$ is exactly $m$. \qed
Corollary 4.2 Let $M$ and $d$ be positive integers and let $E(M, d)$ the Ananyan-Hochster bound from [1], namely the constant such that for any ideal $I$ in any polynomial ring over a field, if $I$ has at most $M$ generators all of which have degree at most $d$, then $I$ has at most $E(M, d)$ associated primes. Then $E(M, d) \geq 1 + 3^{2M - 1}$.

Proof. Let $m \geq 3$, $v = 3$, $P$ be as in Theorem 4.1. Then the number $M$ of generators of $P^2$ is at most $\frac{m(m+1)}{2} \leq \frac{(m+1)^2}{2}$, and the number of associated primes of $P^2$ is

$$1 + 3^m \geq 1 + 3^{2M - 1}. \quad \square$$

Theorem 4.3 For every field $k$, for every odd integer $m = 2n + 7 \geq 9$ and for all positive integers $v_1, \ldots, v_m$ there exists a polynomial ring in $\sum_{i=1}^m v_i$ variables over $k$ with a prime ideal $P$ of height $\frac{m+1}{2} = n + 4$ such that $P^2$ has at least $\prod_{i=1}^m v_i + v_1v_2 \prod_{i=n+3}^m v_i$ embedded primes.

If all $v_i$ equal $v$, this says that there exists a prime ideal $P$ of height $\frac{m+1}{2} = n + 4$ in a polynomial ring in $mv$ variables such that $P^2$ has at least $v^m + v^{m+7} = v^{2n+7} + v^{n+7}$ embedded primes. The number $v^m = (\sqrt{v})^{mv}$ is exponential in the number $mv$ of variables if we think of $v$ as fixed.

Proof. We use the set-up as in Example 2.2 (2): $A = k[a, b]$, $S_z = A[c]$, $S_u = A[c_1, \ldots, c_n]$, $J = (a^2b^2c, b^4, ab^3, a^3b, a^4) \subseteq S_z$, $d_z$ and $d_u$ trivial gradings on $A$, and $d_z(c) = 1$, $d_u(c_j) = e_j$, where $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ has 1 in the $j$th entry. Then the $A$-module homomorphism $\varphi : S_u \rightarrow S_z$ taking $c_j$ to $c$ is a spreading, and it is surjective and full. Furthermore, spr$(J) = (a^2b^2c_1, \ldots, a^2b^2c_n, b^4, ab^3, a^3b, a^4)$.

The extended Rees algebra of $J$ is a natural homomorphic image of the polynomial ring $S_Z = S_z[Z_1, \ldots, Z_5, T]$, and the extended Rees algebra of spr$(J)$ is a natural homomorphic image of the polynomial ring $S_U = S_u[U_1, \ldots, U_n, U'_1, U'_3, U'_4, U'_5, T]$. Let $P_Z$ (resp. $P_U$) be the kernels of these homomorphisms. By Theorem 2.9, there exists a surjective spreading $(S_Z, d_Z, S_U, d_U, \Phi)$ such that spr$(P_Z) = P_U$. We may take $\varphi(U_i) = Z_1$ and $\varphi(U'_i) = Z_i$ for all $i$. Without loss of generality we may identify each $U'_i$ with $Z_i$, so that in the sequel we write $S_U = S_u[U_1, \ldots, U_n, Z_2, Z_3, Z_4, Z_5, T]$.

Note that $S_U$ is a polynomial ring in $m = 2n + 7$ variables over $k$. Since $S_u$ has dimension $n + 2$, the extended Rees algebra of spr$(J)$ has dimension $n + 3$, so that the height of $P_U$ is $(2n + 7) - (n + 3) = n + 4 = \frac{m+1}{2}$.

Let $M_Z$ (resp. $M_U$) be the maximal homogeneous ideal in $S_Z$ (resp. $S_U$). We show that $M_U$ is associated to $P^2_U$. Note that $P_Z$ is as in Proposition 3.3, and so $M_Z$ is associated to $P^2_Z$ and $M_Z$ is the radical of $P^2_Z : f$ for some $f \in k[a, b, Z_2, Z_3, Z_4, Z_5, T]$. Since $\Phi(f) = f \notin P^2_Z = \Phi(P^2_U)$, it follows that $f \notin P^2_U$. Let $x$ be any variable in $S_U$. Then for some large integer $p$, $\Phi(x^p) = \Phi(x)^p f \in P^2_Z = \Phi(P^2_U)$. We use a lexicographic order that places all $c_1, \ldots, c_n$ and $U_1, \ldots, U_n$ at the top of the order, and if $x$ is one of these variables, then $x$ is the least in the order. Then by Gröbner bases theory there exists an equation that writes $\Phi(x^p)$ as an element of $P^2_Z$ using only the variables $\Phi(x), a, b, Z_2, Z_3, Z_4, Z_5, T$. If in that
equation we replace each occurrence of $\Phi(x)$ with $x$, then by the definition of spreading we get that $x^p f \in P_U^2$. This proves that $M_U$ is associated to $P_U^2$.

Set $Q_Z = (a, b, Z_1, \ldots, Z_5, T)$, and $Q'_U = (a, b, U_1, \ldots, U_n, Z_2, \ldots, Z_5, T)$. By Proposition 3.3, $Q_Z$ is associated to $P_Z^2$ and $Q_Z$ is the radical of $P_Z^2 : g$ for some $g \in k[a, b, Z_2, Z_3, Z_4, Z_5, T]$. As in the proof in the previous paragraph, $g \notin P_U^2$ and a power of $Q'_U$ is contained in $P_U^2 : g$. If a power of $c_i$ is in $P_U^2 : g$ then a power of $c = \Phi(c_i)$ is in $P_Z^2 : g$, which is a contradiction. Thus no power of $c_i$ is in $P_U^2 : g$. Thus there exists a prime ideal $Q_U$ associated to $P_U^2$ that contains $Q'_U$ and that is different from $M_U$. Thus $Q_U$ contains at least the $n + 7 = \frac{m-7}{2}$ variables from $Q'_U$.

If we split the $i$th variable in $S_U$ into a product of $v_i$ distinct new variables, as $i$ varies from 1 to $m$, then by Theorem 1.7, the image $P$ of $P_U$ is a prime ideal of height $\frac{m+1}{2}$, and $P^2$ has at least $\prod_{i=1}^n v_i$ embedded primes coming from $M_U$ and at least $v_1 v_2 \prod_{i=n+3}^m v_i$ embedded primes coming from $Q_U$.

**Remark 4.4** The proof shows that one of the associated prime ideals of $P_U^2$ is the maximal ideal of $S_U$ and that another associated prime ideal has at least $n + 7$ variables. We do not determine the exact number of variables in this second associated prime.

**Examples 4.5** All rings below are polynomial rings over an arbitrary field.

1. By Theorem 4.1 there exists a prime ideal $P$ of height 4 in $2 + 2 + 5 + 5 + 5 = 19$ variables such that $P^e$ has exactly $500 = 2^2 \cdot 5^3$ embedded primes for all $e \geq 2$.
2. By Theorem 4.3 there exists a prime ideal $P$ of height 5 in $2 + 2 + 1 + 1 + 1 + 5 + 5 + 5 = 23$ variables such that $P^2$ has at least $2^2 \cdot 1^4 \cdot 5^3 + 2^2 \cdot 1^3 \cdot 5^3 = 1000$ embedded primes.
3. By Theorem 4.1, there exists a prime ideal $P$ of height 5 in $6 \cdot 3 = 18$ variables such that $P^e$ has exactly $3^6 = 729$ embedded primes for all $e \geq 2$.
4. By Theorem 4.3, there exists a prime ideal $P$ of height 5 in $9 \cdot 2 = 18$ variables such that $P^2$ has at least $2^9 + 2^8 = 768$ embedded primes.
5. By Theorem 4.1, there exists a prime ideal $P$ of height 10 in $11 \cdot 2 = 22$ variables such that $P^e$ has exactly $2^{11} = 2048$ embedded primes for all $e \geq 2$.
6. By Theorem 4.3, there exists a prime ideal $P$ of height 6 in $11 \cdot 2 = 22$ variables such that $P^2$ has at least $2^{11} + 2^9 = 2560$ embedded primes.

**References**

1. T. Ananyan and M. Hochster, Small subalgebras of polynomial rings and Stillman’s conjecture, arXiv:math.AC/1610.09268.
2. D. Bayer and M. Stillman, On the complexity of computing syzygies, J. Symbolic Comput., 6 (1988), 135-147.
3. D. Eisenbud, *Commutative Algebra with a View toward Algebraic Geometry*, Springer-Verlag, 1994.
4. D. Grayson and M. Stillman, Macaulay2, a software system for research in algebraic geometry, available at http://www.math.uiuc.edu/Macaulay2.
5. G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.* 95 (1926), 736–788.
6. C. Huneke, The primary components of and integral closures of ideals in 3-dimensional regular local rings, *Math. Ann.* 275 (1986), 617–635.
7. G. A. Kirkup, Minimal primes over permanental ideals, *Trans. Amer. Math. Soc.* 360 (2008), 3751–3770.
8. R. C. Laubenbacher and I. Swanson, Permanental ideals, *J. Symbolic Comput.* 30 (2000), 195–205.
9. H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, 1986.
10. E. Mayr and A. Meyer, The complexity of the word problems for commutative semigroups and polynomial ideals, *Adv. Math.*, 46 (1982), 305-329.
11. J. McCullough and I. Peeva, Counterexamples to the regularity conjecture, *J. Amer. Math. Soc.* 31 (2018), 473–496.
12. J. Porcino and I. Swanson, 2 x 2 permanental ideals of hypermatrices, *Comm. Alg.* 43 (2015), 84–101.
13. A. Seidenberg, Constructions in algebra, *Trans. Amer. Math. Soc.* 197 (1974), 273–313.
14. I. Swanson, The minimal components of the Mayr-Meyer ideals, *J. Algebra* 267 (2003), 127–155.
15. I. Swanson, On the embedded primes of the Mayr-Meyer ideals, *J. Algebra* 275 (2004), 143-190.
16. I. Swanson and R. M. Walker, Tensor-Multinomial Sums of Ideals: Primary Decompositions and Persistence of Associated Primes, arXiv:1806.03545.
17. L. G. Valiant, The complexity of computing the permanent, *Theoret. Comp. Sci.* 8 (1979), 189–201.
18. L. van den Dries and K. Schmidt, Bounds in the theory of polynomial rings over fields. A non-standard approach, *Invent. Math.* 76 (1984), 77–91.
19. R. M. Walker, Uniform symbolic topologies via multinomial expansions, arXiv:math.AC/1703.04530.