BINOMIAL IDEALS

DAVID EISENBUD AND BERND STURMFELS

Introduction. It is notoriously difficult to deduce anything about the structure of an ideal or scheme by directly examining its defining polynomials. A notable exception is that of monomial ideals. Combined with techniques for making flat degenerations of arbitrary ideals into monomial ideals (typically, using Gröbner bases), the theory of monomial ideals becomes a useful tool for studying general ideals. Any monomial ideal defines a scheme whose components are coordinate planes. These objects have provided a useful medium for exchanging information between commutative algebra, algebraic geometry, and combinatorics.

This paper initiates the study of a larger class of ideals whose structure can still be interpreted directly from their generators: binomial ideals. By a *binomial* in a polynomial ring $S = k[x_1, \ldots, x_n]$, we mean a polynomial with at most two terms, say $ax^\alpha + bx^\beta$, where $a, b \in k$ and $\alpha, \beta \in \mathbf{Z}_+^n$. We define a *binomial ideal* to be an ideal of S generated by binomials, and a *binomial scheme* (or *binomial variety*, or *binomial algebra*) to be a scheme (or variety or algebra) defined by a binomial ideal. For example, it is well known that the ideal of algebraic relations on a set of monomials is a prime binomial ideal (Corollary 1.3). In Corollary 2.6 we shall see that every binomial prime ideal has essentially this form.

A first hint that there is something special about binomial ideals is given by the following result, a weak form of what is proved below (see Corollary 2.6 and Theorem 6.1).

THEOREM. *The components (isolated and embedded) of any binomial scheme in affine or projective space over an algebraically closed field are rational varieties.*

By contrast, every scheme may be defined by trinomials, that is, polynomials with at most three terms. The trick is to introduce $n - 3$ new variables z_i for each equation $a_1 x^{m_1} + \cdots + a_n x^{m_n} = 0$ and replace this equation by the system of $n - 2$ new equations

$$z_1 + a_1 x^{m_1} + a_2 x^{m_2} = -z_1 + z_2 + a_3 x^{m_3} = -z_2 + z_3 + a_4 x^{m_4} = \cdots$$

$$\cdots = -z_{n-4} + z_{n-3} + a_{n-2} x^{m_{n-2}} = -z_{n-3} + a_{n-1} x^{m_{n-1}} + a_n x^{m_n} = 0.$$

Our study of binomial ideals is partly motivated by the frequency with which they occur in interesting contexts. For instance, varieties of minimal degree in projective spaces are defined by binomial equations in a suitable system of coordinates. More generally, any toric variety is defined by binomials. (Throughout this paper, we use the term "toric variety" to include also toric varieties that are not normal.) We shall see that the binomial ideals that are prime are precisely the defining ideals of toric varieties. Sections of toric varieties by linear subspaces defined by coordinates or differences of coordinates give interesting examples of binomial schemes. For varieties of minimal degree, such sections were studied by Xambó [X].

More general than coordinate rings of toric varieties are commutative semigroup algebras. An excellent general reference is Gilmer's 1984 book [Gi], which treats these algebras over arbitrary base rings. Gilmer shows in Theorem 7.13 that the semigroup algebras of commutative semigroups are precisely the homomorphic images of polynomial rings by ideals generated by *pure difference binomials*, that is, polynomials $x^\alpha - x^\beta$, where $\alpha, \beta \in \mathbf{Z}_+^n$. In fact, the Zariski closure of any subsemigroup of k^n, regarded as a semigroup by pointwise multiplication, or any of its translates is defined by binomials (see Proposition 2.3 and the remark following). Generalizing in a different direction, we show that an algebra over a field k is defined by binomial equations if and only if the algebra admits a grading by a semigroup such that each graded component has dimension $\leqslant 1$ over k; see Proposition 1.11. An interesting special case that has been studied intensively is given by the *Algebras of type A* studied by Arnold [A], Korkina [Kor], [KPR], and others. It may be possible to shed some light on their structure using the techniques developed here.

Further examples generalizing toric varieties are the *face rings of polyhedral complexes* introduced by Stanley [Sta]. Geometrically, they are obtained by gluing toric varieties along orbits in a nice way. They all have binomial presentations (see Example 4.7). Some of them and their binomial sections are geometrically interesting, for example as degenerations of special embeddings of abelian varieties, and have played a role in the investigations of the Horrocks-Mumford bundle by Decker, Manolache, and Schreyer [DMS].

Gröbner basis techniques using a total monomial order on a polynomial ring allow the flat degeneration of an arbitrary algebra to an algebra defined by monomial equations. Using orders that are somewhat less strict, we sometimes get degenerations to algebras defined by binomial equations. In particular, the subalgebra bases of Robbiano and Sweedler [RS] allow one to do this in a systematic way. The resulting degenerate varieties may be better models of the original varieties than those produced by a further degeneration to varieties defined by monomials.

Complexity issues in computational algebraic geometry provide another motivation for the study of binomial ideals. The main examples known to attain worst case complexity for various classical problems are binomial: these are the constructions of Mayr-Meyer [MM] and Yap [Y] for ideal membership, Bayer-

Stillman [BS] for syzygies, and Brownawell [Br] and Kollár [K] for the effective Nullstellensatz. It has long been believed that the Mayr-Meyer schemes are so bad because of the form of their primary decompositions. The theory developed here provides tools for a systematic investigation of such schemes.

Binomial prime ideals arise naturally in a variety of settings in applied mathematics, including dynamical systems (see, e.g., Hoveijn [H]), integer programming (see Conti-Traverso [CT] and Thomas [T]), and computational statistics (see Diaconis-Sturmfels [DS]). Within computer algebra, they arise in the extension of Gröbner basis theory to canonical subalgebra bases suggested by Robbiano-Sweedler [RS], where the role of a single S-pair is played by an entire binomial ideal. For real-world problems in these domains, it may be computationally prohibitive to work with the binomial prime ideal that solves the problem exactly, in which case one has to content oneself with proper subideals that give approximate solutions. Those subideals are binomial but usually not prime, so the theory developed here may be relevant.

We now describe the content of this paper. To simplify the exposition, we assume that k is an algebraically closed field. Fundamental to our treatment is the observation that every reduced Gröbner basis of a binomial ideal consists of binomials. It follows, for example, that the intersection of a binomial ideal and a monomial ideal is binomial, and any projection of a binomial scheme into a coordinate subspace has binomial closure. Such facts are collected in Section 1 and are used frequently in what follows. We prove in Corollary 1.9 that the blowup algebra, symmetric algebra, Rees algebra, and associated graded algebra of a binomial algebra with respect to a monomial ideal are binomial algebras. This generalizes the remark that toric blowups of toric varieties are toric.

The first step in our analysis of binomial schemes in an affine space k^n is to decompose k^n into the 2^n algebraic tori interior to the coordinate planes, and study the intersection with each of these. In algebraic terms, we choose a subset $\mathscr{E} \subseteq \{1, \ldots, n\}$ and consider the binomial ideals in the ring of Laurent polynomials

$$k[\mathscr{E}^{\pm}] := k[\{x_i, x_i^{-1}\}_{i \in \mathscr{E}}] = k[x_1, \ldots, x_n][\{x_i^{-1}\}_{i \in \mathscr{E}}]/(\{x_i\}_{i \notin \mathscr{E}}),$$

corresponding to the torus

$$(k^*)^{\mathscr{E}} := \{(p_1, \ldots, p_n) \in k^n \mid p_i \neq 0 \text{ for } i \in \mathscr{E}, \, p_i = 0 \text{ for } i \notin \mathscr{E}\}.$$

In Section 2 we show that any binomial ideal in $k[\mathscr{E}^{\pm}]$ is a complete intersection. In characteristic zero, every such "Laurent binomial ideal" is equal to its own radical, and the algebraic set it defines consists of several conjugate torus orbits. In characteristic $p > 0$, binomial ideals may fail to be radical, as for example $(x^p - 1) = (x - 1)^p \subset k[x, x^{-1}]$, but this failure is easy to control. We establish a one-to-one correspondence between Laurent binomial ideals and *partial characters*

on the lattice $\mathbf{Z}^{\mathscr{E}}$ of monomials in $k[\mathscr{E}^{\pm}]$, where we define a partial character ρ to be a group homomorphism from a subgroup $L_\rho \subseteq \mathbf{Z}^{\mathscr{E}}$ to the multiplicative group k^*. Properties of Laurent binomial ideals can be deduced from arithmetic properties of the associated partial characters. For example, the lattice L_ρ is saturated if and only if the corresponding Laurent binomial ideal is prime.

The next step in our theory is the study of reduced binomial schemes. The central result in Section 3 says that the radical of any binomial ideal is again binomial. We prove a corresponding result for the "k-radical"—that is, for the ideal of the Zariski closure of a binomial algebraic set in k^n even when k is not algebraically closed.

In Section 4 we apply our result on radicals to characterize when the intersection of prime binomial ideals is binomial. In other words, we determine which unions of toric varieties are defined by binomial equations.

A serious obstacle on our road to binomial primary decomposition lies in the fact that if B is a binomial ideal and b is a binomial, then the ideal quotient $(B : b)$ is generally not binomial. This problem is confronted in Section 5. A mainspring of our theory (Theorem 5.2) is the description of a delicate class of instances where these quotients are binomial.

In Section 6 we prove that the associated primes of a binomial ideal are binomial. Before undertaking a primary decomposition, we pass to a "cellular decomposition," in which the components are intersections of primary components having generic points in a given cell $(k^*)^{\mathscr{E}}$. We then decompose the cellular binomial ideals further: Theorem 6.4 states that the (uniquely defined) minimal primary components are still binomial. More generally, we prove that localizations of cellular binomial ideals at binomial primes intersect the polynomial ring in binomial ideals.

In Section 7 we prove that every binomial ideal has a primary decomposition, all of whose primary components are binomial. The form of the decomposition is curiously different in characteristic zero from that in positive characteristic.

Section 8 contains a number of auxiliary results, among them an alternative decomposition of a binomial ideal and a condition under which the cellular components are primary. Perhaps most interesting, we give a systematic way of finding a close approximation to a binomial prime ideal, the associated *circuit* ideal.

In Section 9 we present some algorithms for decomposing binomial ideals that emerge from the general theory. These differ markedly from the known algorithms for primary decomposition in that they maintain extreme sparseness of the polynomials involved.

Having learned that the operations of primary decomposition, radicals, projections, etc. described above take binomial ideals to binomial ideals, the reader may think that binomiality is preserved by many common ideal-theoretic constructions. This is not the case; in fact, the set of "binomial-friendly" operations is quite limited. This is what makes the main results of this paper difficult. Here are some cautionary examples.

If B is a binomial ideal and m is a monomial, then the ideal quotient $(B : m)$ is binomial (Corollary 1.7). However, the monomial m cannot be replaced by a monomial ideal. Even an ideal $(B : (x_i, x_j))$ need not be binomial (Examples 1.8 and 4.6). Similarly, ideals $(B : b)$ for a binomial ideal B and a binomial b need not be binomial (Example 5.1).

Another difficulty is that very few intersections of binomial ideals are binomial. For example, a radical binomial ideal can have several components, each of which must be binomial, as stated above, but such that only certain subsets intersect in binomial ideals. The simplest case, in one variable, is given by the ideal

$$(x^d - 1) = \bigcap_{\zeta \in k, \zeta^d = 1} (x - \zeta^m).$$

Here the intersections of components that are again binomial are precisely the ideals

$$(x^{d/e} - 1) = \bigcap_{\zeta \in k, \zeta^e = 1} (x - \zeta^m)$$

where e divides d. Our characterization of binomial algebraic sets gives rise to examples (such as Example 4.6) where the intersection of the primes of maximal dimension containing a radical binomial ideal need not be binomial. Given such waywardness, it still seems to us something of a miracle that binomial ideals have binomial primary decompositions.

1. Gröbner basis arguments. Throughout this paper, k denotes a field and $S := k[x_1, \ldots, x_n]$ the polynomial ring in n variables over k. In this section, we present some elementary facts about binomial ideals which are proved using Gröbner bases. The facts will be used frequently later on. For Gröbner basics, the reader may consult Buchberger [Bu], Cox, Little, and O'Shea [CLO], or Eisenbud [E]. Recall that a *term* is by definition a scalar times a monomial $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$.

PROPOSITION 1.1. *Let $<$ be a monomial order on S, and let $I \subset S$ be a binomial ideal.*
   (a) *The reduced Gröbner basis $\mathscr{G}$ of I with respect to $<$ consists of binomials.*
   (b) *The normal form with respect to $<$ of any term modulo $\mathscr{G}$ is again a term.*

Proof. (a) If we start with a binomial generating set for I, then the new Gröbner basis elements produced by a step in the Buchberger algorithm are binomials. (b) Each step of the division algorithm modulo a set of binomials takes a term to another term. □

One immediate application is a test for binomiality. (Note that we are work-

ing with a fixed coordinate system. We do not know how to test efficiently whether an ideal can be made binomial by a linear change of coordinates.)

COROLLARY 1.2.   *Let $<$ be a monomial order on S. An ideal $I \subset S$ is binomial if and only if some (equivalently, every) reduced Gröbner basis for I consists of binomials. In particular, an ideal $I \subset S$ is binomial if and only if, for some field extension k' of k, the ideal $k'I$ in $k'[x_1, \ldots, x_n]$ is binomial.*

Proof.   This follows from Proposition 1.1(a) and the uniqueness of the reduced Gröbner basis with respect to a fixed monomial order "$<$".   □

A binomial ideal in $k'[x]$ may have a nonbinomial contraction to $k[x]$. For example, take $I = (x - c) \subset k'[x]$, where $c \in k'$ is algebraic over k but not a root of an element of k.

The following consequence of Proposition 1.1 shows that coordinate projections of binomial schemes are binomial.

COROLLARY 1.3.   *If $I \subseteq k[x_1, \ldots, x_n]$ is a binomial ideal, then the elimination ideal $I \cap k[x_1, \ldots, x_r]$ is a binomial ideal for every $r \leqslant n$.*

Proof.   The intersection is generated by a subset of the reduced Gröbner basis of I with respect to the lexicographic order.   □

The projective closure is also well behaved.

COROLLARY 1.4.   *If X is an affine scheme in k^n defined by an ideal I in S, then the ideal in $S[x_0]$ defining the projective closure of X is binomial if and only if I is binomial.*

Proof.   The ideal of the projective closure is generated by the homogenizations of the elements in the reduced Gröbner basis for I with respect to the total degree order.   □

As we have already mentioned, an intersection of binomial ideals is rarely binomial. But when all but one of the ideals is generated by monomials, or even generated by monomials modulo a common binomial ideal, then everything is simple.

COROLLARY 1.5.   *If $I, I', J_1, \ldots, J_s$ are ideals in $S = k[x_1, \ldots, x_n]$ such that I and I' are generated by binomials and $J_1, \ldots, J_s$ are generated by monomials, then*

$$(I + I') \cap (I + J_1) \cap (I + J_2) \cap \cdots \cap (I + J_s)$$

is generated by binomials.

Proof.   Suppose first that $s = 1$. In the larger polynomial ring $k[x_1, \ldots, x_n, t]$, consider the binomial ideal L generated by $I + tI' + (1 - t)J_1$. The claim follows from Corollary 1.3 and the formula $(I + I') \cap (I + J_1) = L \cap k[x_1, \ldots, x_n]$. For the general case, use induction on s.   □

A slightly more subtle argument shows that there is a good theory of mono-mial ideals modulo a binomial ideal. (See Proposition 3.4 for a further result in this direction.)

COROLLARY 1.6. *Let I be a binomial ideal and let $J_1, \ldots, J_s$ be monomial ideals in S.*

(a) *The intersection $(I + J_1) \cap \cdots \cap (I + J_s)$ is generated by monomials modulo I.*

(b) *Any monomial in the sum $I + J_1 + \cdots + J_s$ lies in one of the ideals $I + J_j$. In particular, if $m, m_1, \ldots, m_s$ are monomials and $m \in I + (m_1, \ldots, m_s)$, then $m \in I + (m_i)$ for some i.*

Proof. Choose a monomial order on S, and let $\mathcal{M}$ be the set of monomials not in the initial ideal $\mathrm{in}(I)$ of I with respect to this order; these monomials are called *standard monomials* mod I. The image $\bar{\mathcal{M}}$ of $\mathcal{M}$ in S/I is a vector space basis. Let $\bar{J}_j$ be the image of J_j in S/I. By Proposition 1.1 (b), each $\bar{J}_j$ has a vector space basis that is a subset of $\bar{\mathcal{M}}$. It follows that the intersection of these bases is a basis for $\cap_j \bar{J}_j$, which is thus spanned by monomials. Similarly, the union of these bases is a basis for $\sum_j \bar{J}_j$. Using Proposition 1.1(b) again, we see that if m is a monomial in $\sum_j (I + J_j)$ then $\bar{m} \in S/I$ is represented by a standard monomial in $\sum_j \bar{J}_j$, and thus belongs to one of the $\bar{J}_j$, whence $m \in I + J_j$ as required. The last statement is a special case. $\square$

Here is a central result that serves as a bridge to connect the theory of binomial ideals in a polynomial ring with that of Laurent binomial ideals developed in the next section. If I, J are ideals in a ring R, then we set $(I : J) := \{ f \in R \mid fJ \subset I \}$, and $(I : J^\infty) := \{ f \in R \mid fJ^m \subset I \text{ for } m \gg 0 \}$. If $g \in R$, we abbreviate $(I : (g))$ to $(I : g)$.

COROLLARY 1.7. *Let $I \subset S$ be a binomial ideal, $m_1, \ldots, m_t$ monomials, and $f_1, \ldots, f_t$ polynomials such that $\sum_i f_i m_i \in I$. Let $f_{i,j}$ denote the terms of f_i. For each term $f_{i,j}$, either $f_{i,j} m_i \in I$ or there is a term $f_{i',j'}$, distinct from $f_{i,j}$, and a scalar $a \in k$ such that $f_{i,j} m_i + a f_{i',j'} m_{i'} \in I$. In particular:*

(a) *For any monomial m the ideal quotients $(I : m)$ and $(I : m^\infty)$ are binomial.*

(b) *The first syzygies of monomials modulo a binomial ideal are generated by binomial syzygies.*

Proof. Choose a monomial order $>$ on S. By Proposition 1.1(b) the normal form of $f_{i,j} m_i$ modulo I is either zero or a term m. If it is zero, we have $f_{i,j} m_i \in I$. Otherwise, m must cancel against a sum of terms in the normal forms of some $f_{i'} m_{i'}$. By Proposition 1.1(b), these are the normal forms of terms $f_{i',j'} m_{i'}$. The first statement follows.

To prove (a), suppose that $f \in (I : m)$, that is, $fm \in I$. By the first part of the corollary, with $t = 1$, we may write f as a sum of binomials in $(I : m)$. Thus, $(I : m)$ is generated by binomials. Since $(I : m^\infty) = \bigcup_s (I : m^s)$, the second statement follows from the first. Part (b) follows similarly. $\square$

Corollary 1.7 shows that the ideal quotient of a binomial ideal by a single monomial is a binomial ideal. However, the quotient of a binomial ideal by a monomial ideal need not be a binomial ideal, even if the monomial ideal is generated by two variables.

Example 1.8 (Quotients of binomial ideals by monomial ideals are generally not binomial). Let $I = (ax_1 - ax_3, ax_2 - ax_4, bx_1 - bx_4, bx_2 - bx_3) \subseteq k[a, b, x_1, \dots, x_4]$. This ideal is the intersection of four binomial primes defining linear subspaces:

$$I = (a, b) \cap (a, x_1 - x_4, x_2 - x_3) \cap (b, x_1 - x_3, x_2 - x_4) \cap (x_2 - x_3, x_3 - x_4, x_1 - x_4).$$

The equidimensional part of I of codimension 3 is $(I : (a, b))$, which is the intersection of the last three of these primes. But the homogeneous ideal

$$(I : (a, b)) = (x_1 + x_2 - x_3 - x_4, a(x_2 - x_4), (x_2 - x_3)(x_2 - x_4), b(x_2 - x_3))$$

is not a binomial ideal. For example, it contains $x_1 + x_2 + x_3 + x_4$, but no other linear form. See also Example 4.6.

Corollaries 1.3 and 1.7 give us interesting sources of binomial algebras, for example, the following corollary.

COROLLARY 1.9. *Let B be a binomial ideal and M a monomial ideal in S. If we set $R = S/B$ and $I = (B + M)/B \subseteq R$, then each of the following five algebras is binomial: the symmetric algebras $\mathrm{Sym}_R I$ and $\mathrm{Sym}_{R/I} I/I^2$, the blowup algebra $R[zI] \subseteq R[z]$, the Rees algebra $R[z^{-1}, zI] \subseteq R[z^{-1}, z]$, and the associated graded algebra $gr_I R$.*

Proof. Let $M = (m_1, \dots, m_t)$. By Corollary 1.7, there are binomial syzygies $\sum_j f_{i,j} m_j \equiv 0 \pmod{B}$ that generate all the syzygies of I over R. The symmetric algebra $\mathrm{Sym}_R I$ may be represented as a polynomial algebra $R[y_1, \dots, y_t]$ modulo the relations $\sum_j f_{i,j} y_j = 0$. Each generator $\sum_i f_{i,j} y_i$ is a binomial, so we see that the symmetric algebra is binomial. It follows that $\mathrm{Sym}_{R/I} I/I^2 = \mathrm{Sym}_R(I)/ I \, \mathrm{Sym}_R(I)$ is binomial, too.

The blowup algebra $R[zI] \subseteq R[z]$ may be represented as $R[y_1, \dots, y_t]/J$, where J is the ideal of algebraic relations satisfied over R by the elements $m_i z \in R[z]$. The ideal J is the intersection of $R[y_1, \dots, y_t]$ with the ideal

$$J' = (y_1 - m_1 z, \dots, y_t - m_t z) \subseteq R[y_1, \dots, y_t, z].$$

Since J' is binomial, Corollary 1.3 shows that J is binomial. An analogous construction with two variables z and z', and an ideal $J' = (y_1 - m_1 z, \dots, y_t - m_t z, zz' - 1)$ proves the statement about the Rees algebra.

The case of the associated graded algebra follows from the cases above, since $gr_I R = R[zI]/IR[zI] = R[z^{-1}, zI]/z^{-1} R[z^{-1}, zI]$.

Here is another useful fact about monomial ideals modulo binomial ideals. The assertion is equivalent to the existence of the special Gröbner basis constructed in the proof.

PROPOSITION 1.10. *Let B be a binomial ideal and M a monomial ideal in S. If $f \in B + M$ and f' is the sum of those terms of f that are not individually contained in $B + M$, then $f' \in B$.*

Proof. We may harmlessly assume that $f = f'$, and we must show that $f \in B$. We shall construct a special Gröbner basis for $B + M$.

Choose a monomial order on S. Let G be a Gröbner basis for B, and let M' be a set of generators for the ideal of all monomials contained in $B + M$. Clearly, $G \cup M'$ generates $B + M$. We claim that $G \cup M'$ is a Gröbner basis. By Buchberger's criterion, it is enough to check that all s-pairs made from $G \cup M'$ reduce to zero modulo $G \cup M'$. Now the s-pairs made from pairs of elements of G reduce to zero since G is a Gröbner basis. The s-pairs made from an element of G and an element of M' yield monomials that lie in $B + M$ and that therefore reduce to zero through generators of M'. The s-pairs made from two elements of M' yield zero to begin with. This shows that $G \cup M'$ is a Gröbner basis.

The normal form modulo $G \cup M'$ of a term t of f is, by Proposition 1.1, a monomial $m(t)$, and our assumption implies that $m(t)$ is nonzero. Consider the division process that reduces t to $m(t)$ by subtracting appropriate multiples of elements of $G \cup M'$. At each stage the remainder is a monomial. If this monomial were ever divisible by an element of M' then it would reduce to zero. Thus, the division process can use only elements from G. We conclude that f reduces to zero under division by G, and hence f lies in B. $\square$

An affine toric variety over k is a variety admitting an algebraic action by a finite product of copies of the multiplicative group $(G_m)^d$ with a dense orbit isomorphic to $(G_m)^d$. Such varieties may be characterized by saying that their coordinate rings are $\mathbf{Z}^d$-graded in such a way that each homogeneous component has dimension $\leqslant 1$. The following characterization of binomial algebras extends this.

PROPOSITION 1.11. *A finitely generated k-algebra R admits a presentation of the form $R = S/B$, where B is a binomial ideal, if and only if R can be graded by a commutative semigroup Σ with n generators in such a way that every homogeneous component of R has dimension $\leqslant 1$.*

Proof. First suppose that R admits a grading of the given type by the semigroup Σ. We may map S onto R by sending the variables x_i to nonzero elements of the one-dimensional spaces of homogeneous elements of degree corresponding to the n generators of Σ. The relations on these generators are generated by homogeneous relations, that is, by relations that are sums of monomials all with the same degree in Σ. But for any two monomials m, m' of S with the same degree in Σ, there is a scalar $a \in k$ such that the binomial $am - m' \in S$ goes to

zero in R. Thus, the ideal of all such binomials generates the kernel of the map $S \to R$.

Before proving the converse, a remark about semigroup gradings will be useful. Suppose that $R = S/B$ where B is *any* ideal. Let Σ be the set of all one-dimensional subspaces $\langle m \rangle$ of R generated by monomials m in the images of the x_i, together with the "formal" element $\langle 0 \rangle$. The set Σ is an (additive) semigroup, with operation $\langle m \rangle + \langle n \rangle = \langle mn \rangle$ (this is where the element $\langle 0 \rangle$ may be necessary) and neutral element $\langle 1 \rangle$. In order for R to be graded by Σ, it is necessary and sufficient that the natural map

$$\bigoplus_{\substack{\langle m \rangle \in \Sigma, \\ m \neq 0}} \langle m \rangle \to R$$

be an isomorphism of vector spaces. The map is clearly surjective, but it is not always injective.

If now B is a binomial ideal, and we choose a monomial order on S, then by Proposition 1.1 the normal form of a monomial modulo B is a term. This implies that if $\langle m \rangle$ is contained in the linear span of $\langle m_1 \rangle, \ldots, \langle m_t \rangle$ modulo B, then $\langle m \rangle$ is contained in one of the $\langle m_i \rangle$ modulo B, and proves that the $\langle m \rangle$ in Σ with $m \neq 0$ are linearly independent, as required. $\square$

2. Laurent binomial ideals and binomial primes.

Let k be a field. We consider the ring

$$k[x^{\pm}] := k[\mathbf{Z}^n] = k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$$

of Laurent polynomials with coefficients in k. A *binomial* in $k[x^{\pm}]$ is an element with at most two terms, say $ax^{\alpha} + bx^{\beta}$, where $a, b \in k$ and $\alpha, \beta \in \mathbf{Z}^n$. A *Laurent binomial ideal* is an ideal in $k[x^{\pm}]$ generated by binomials. Note that in $k[x^{\pm}]$ any nonzero binomial that is not a unit can be written in the form $x^m - c_m$ for some $m \in \mathbf{Z}^n$ and $c_m \in k^*$.

In this section, we analyze Laurent binomial ideals and their primary decompositions. We regard $k[x^{\pm}]$ as the coordinate ring of the algebraic torus $(k^*)^n = \text{Hom}(\mathbf{Z}^n, k^*)$, the group of *characters* of $\mathbf{Z}^n$. A *partial character* on $\mathbf{Z}^n$ is a homomorphism ρ from a sublattice L_ρ of $\mathbf{Z}^n$ to the multiplicative group k^*. Whenever we speak of a partial character ρ, we mean the pair consisting of the map ρ and its domain $L_\rho \subseteq \mathbf{Z}^n$. Given a partial character ρ, we define a Laurent binomial ideal

$$I(\rho) := (x^m - \rho(m) : m \in L_\rho).$$

We shall see that all Laurent binomial ideals are of this form.

THEOREM 2.1.   *Let $k[x^{\pm}]$ be a Laurent polynomial ring over a field k.*

(a) *For any proper Laurent binomial ideal $I \subseteq k[x^{\pm}]$ there is a unique partial character ρ on $\mathbf{Z}^n$ such that $I = I(\rho)$.*

(b) *If $m_1, \ldots, m_r$ is a basis of the lattice L_ρ, then the binomials*

$$x^{m_1} - \rho(m_1), \ldots, x^{m_r} - \rho(m_r)$$

generate $I(\rho)$ and form a regular sequence in $k[x^{\pm}]$. After a change of variables in $k[x^{\pm}]$, the ideal I may even be generated by a regular sequence of the form

$$x_1^{d_1} - c_1, \ldots, x_r^{d_r} - c_r.$$

In particular,

$$\operatorname{codim}(I(\rho)) = \operatorname{rank}(L_\rho).$$

Now assume that k is algebraically closed.

(c) *The ideal $I(\rho)$ is prime if and only if L_ρ is a direct summand of $\mathbf{Z}^n$.*

(d) *Let $\operatorname{char}(k) = p \geqslant 0$. Suppose that ρ is a partial character on $\mathbf{Z}^n$ and $L_\rho \subseteq L \subseteq \mathbf{Z}^n$ are lattices with L/L_ρ finite of order g. If g is relatively prime to p, then there are g distinct characters ρ' on L that are extensions of ρ on L_ρ, and*

$$I(\rho) = \bigcap_{\rho' \text{ extends } \rho \text{ to } L} I(\rho').$$

If g is a power of p, then there is a unique extension ρ' of ρ to L, and $k[x^{\pm}]/I(\rho)$ has a filtration by $k[x^{\pm}]$-modules

$$k[x^{\pm}]/I(\rho) = M_0 \supset M_1 \supset \cdots \supset M_g = 0$$

with successive quotients $M_i/M_{i+1} \cong k[x^{\pm}]/I(\rho')$.

Proof. (a) Any proper binomial ideal I in $k[x^{\pm}]$ is generated by its elements of the form $x^m - c_m$ for $m \in \mathbf{Z}^n$ and $c \in k^*$. Let L be the subset of $\mathbf{Z}^n$ consisting of those m that appear. Since I is proper, c_m is uniquely determined by m. From the basic formula

$$x^{m+m'} - cd = (x^m - c)x^{m'} + c(x^{m'} - d), \qquad (2.1)$$

we see that if $x^m - c_m$ and $x^{m'} - c_{m'}$ are in I, then so is $x^{m+m'} - c_m c_{m'}$, while if $x^{m+m'} - c_m c_{m'}$ and $x^m - c_m$ are in I, then so is $x^{m'} - c_{m'}$. Hence, L is a sublattice of $\mathbf{Z}^n$, the map $\rho: L \to k^*$ taking m to c_m is a character, and $I = I(\rho)$.

For the uniqueness part of (a), we shall show that if a binomial $x^u - c_u$ lies in $I(\rho)$, then $u \in L_\rho$ and $c_u = \rho(u)$. We write $k[x^{\pm}]$ as the quotient of the poly-

nomial ring $T := k[y_1, \ldots, y_n, z_1, \ldots, z_n]$ modulo the binomial ideal $(y_i z_i - 1 : i = 1, \ldots, n)$. If $I'(\rho)$ denotes the preimage of $I(\rho)$ in T, then $I'(\rho)$ is generated by the set

$$\{y^a z^b - \rho(a - b - c + d) \cdot y^c z^d : a, b, c, d \in \mathbf{N}^n, \ a - b \equiv c - d \ (\mathrm{mod} \ L_\rho)\}. \quad (2.2)$$

By Buchberger's criterion, this set is a Gröbner basis for $I'(\rho)$ with respect to any monomial order on T, since the condition $a - b \equiv c - d \ (\mathrm{mod} \ L_\rho)$ on exponents is preserved by the formation of s-pairs. If $x^u - c_u$ lies in $I(\rho)$, and we write u_+, u_- for the positive and negative parts of u, so that $u = u_+ - u_-$, then the normal form of $y^{u_+} z^{u_-}$ modulo this Gröbner basis is the constant c_u. Each polynomial in the reduction sequence is a term of the form $\rho(a - b - c + d) \cdot y^{u_+ - a + c} z^{u_- - b + d}$ where $a - b - c + d \in L_\rho$. This proves that $u \in L_\rho$ and $\rho(u) = c_u$.

(b) Formula (2.1) shows that any set of additive generators $\{m_i\}$ of L_ρ gives rise to a set of generators $x^{m_i} - \rho(m_i)$ of the ideal $I(\rho)$. Diagonalizing a matrix representing the inclusion $L_\rho \subseteq \mathbf{Z}^n$, we see that $I(\rho)$ can be generated by a sequence of elements of the form $x_1^{d_1} - c_1, \ldots, x_r^{d_r} - c_r$ as claimed. Since this is obviously a regular sequence, we see at once that the codimension of $I(\rho)$ is r.

If $m_1, \ldots, m_r$ are linearly independent elements that span L_ρ, it remains to show that

$$x^{m_1} - \rho(m_1), \ldots, x^{m_r} - \rho(m_r)$$

is a regular sequence. By induction on r, we may suppose that the first $r - 1$ binomials form a regular sequence. In particular, all the associated primes of the ideal they generate have codimension $r - 1$. Since $I(\rho)$ has codimension r, the last binomial is not in any of these associated primes, and we are done.

(c) From the expression $I(\rho) = (x_1^{d_1} - c_1, \ldots, x_r^{d_r} - c_r)$, as in part (b), it is clear that $I(\rho)$ is prime if and only if all the d_i are equal to 1. This holds if and only if L_ρ is a direct summand, as claimed.

(d) Both statements reduce to the case where L/L_ρ is a cyclic group of prime order q. Diagonalizing a matrix for the inclusion $L_\rho \subset L$, we may choose a basis $m_1, \ldots, m_r$ of L such that L_ρ has the basis $m_1, \ldots, m_{r-1}, q m_r$. For any extension ρ' of ρ to L, the element $\rho'(m_r)$ is a qth root of $\rho(q m_r)$. If $c \in k^*$ is one such qth root and we let

$$J = (x^{m_1} - \rho(m_1), \ldots, x^{m_{r-1}} - \rho(m_{r-1})),$$

then each of the ideals $I(\rho')$ has the form $I(\rho') = J + (x^{m_r} - \zeta c)$ for some qth root of unity ζ, while $I(\rho) = J + (x^{q m_r} - c^q)$.

If $q \neq p$, then there are q distinct qth roots of unity in k. If ζ and ζ' are two of them, then $I(\rho') = J + (x^{m_r} - \zeta c)$ and $I(\rho') = J + (x^{m_r} - \zeta' c)$ together generate the unit ideal. Thus, in the ring $R := k[x^\pm]/J$ the intersection of these ideals is

equal to their product, and we get

$$I(\rho)/J = (x^{qm_r} - c^q)R = \prod_\zeta (x^{m_r} - \zeta c)R = \bigcap_\zeta (x^{m_r} - \zeta c)R = \bigcap_{\rho'} I(\rho')/J.$$

It follows that $I(\rho) = \bigcap_{\rho'} I(\rho')$ as required.

On the other hand, if $q = p$, then $\zeta = 1$ and $x^{qm_r} - c^q = (x^{m_r} - c)^q$. By part (b), the element $x^{m_r} - c$ is a nonzerodivisor modulo J. Therefore, in the filtration

$$k[x^\pm] \supset I(\rho') = J + (x^{m_r} - c) \supset J + (x^{m_r} - c)^2 \supset \cdots \supset J + (x^{m_r} - c)^p = I(\rho),$$

the successive quotients are isomorphic to $k[x^\pm]/I(\rho')$. Reducing modulo $I(\rho)$, we get a filtration of $k[x^\pm]/I(\rho)$ with the desired properties. $\square$

Using Theorem 2.1 we can describe the primary decomposition and radical of a Laurent binomial ideal in terms of operations on integer lattices. If L is a sublattice of $\mathbf{Z}^n$, then the *saturation* of L is the lattice

$$\mathrm{Sat}(L) := \{m \in \mathbf{Z}^n \mid dm \in L \text{ for some } d \in \mathbf{Z}\}.$$

The group $\mathrm{Sat}(L)/L$ is finite. We say that L is *saturated* if $L = \mathrm{Sat}(L)$. If p is a prime number, we further define $\mathrm{Sat}_p(L)$ and $\mathrm{Sat}'_p(L)$ to be the largest sublattices of $\mathrm{Sat}(L)$ such that $\mathrm{Sat}_p(L)/L$ has order a power of p and $\mathrm{Sat}'_p(L)/L$ has order relatively prime to p. (These can be computed by diagonalizing a matrix representing the inclusion of L in $\mathbf{Z}^n$.) We adopt the convention that if $p = 0$, then $\mathrm{Sat}_p(L) = L$ and $\mathrm{Sat}'_p(L) = \mathrm{Sat}(L)$.

If ρ is a partial character, we define the *saturations* of ρ to be the characters ρ' of $\mathrm{Sat}(L_\rho)$ that restrict to ρ on L_ρ, and we say that ρ is saturated if L_ρ is saturated.

COROLLARY 2.2. *Let k be an algebraically closed field of characteristic $p \geqslant 0$. Let ρ be a partial character. Write g for the order of $\mathrm{Sat}'_p(L_\rho)/L_\rho$. There are g distinct characters $\rho_1, \ldots, \rho_g$ of $\mathrm{Sat}'_p(L_\rho)$ extending ρ and for each j a unique character ρ'_j of $\mathrm{Sat}(L_\rho)$ extending ρ_j. There is a unique partial character ρ' of $\mathrm{Sat}_p(L_\rho)$ extending ρ. The radical, associated primes, and minimal primary decomposition of $I(\rho) \subseteq k[x^\pm]$ are*

$$\sqrt{I(\rho)} = I(\rho')$$

$$\mathrm{Ass}(S/I(\rho)) = \{I(\rho'_j) \mid j = 1, \ldots, g\}$$

$$I(\rho) = \bigcap_{j=1}^{g} I(\rho_j),$$

and $I(\rho_j)$ is $I(\rho'_j)$-primary. In particular, if $p = \mathrm{char}(k) = 0$, then $I(\rho)$ is a radical

ideal. The associated primes $I(\rho_j')$ *of* $I(\rho)$ *are all minimal and have the same co-dimension* rank(L_ρ). *The geometric multiplicity of each primary component* $I(\rho_j)$ *is the order of the group* $\mathrm{Sat}_p(L_\rho)/L_\rho$.

Proof. For every prime $q \neq p$ and every integer $d \geqslant 0$, the subgroup of k^* of elements of order q^d is cyclic of order q^d, while the subgroup of k^* of elements of order p^d is trivial. This implies that there is a unique extension ρ' of ρ to $\mathrm{Sat}_p(L_\rho)$, exactly g extensions ρ_j of ρ to $\mathrm{Sat}_p'(L_\rho)$, and a unique extension ρ_j' of ρ_j to $\mathrm{Sat}(L_\rho)$. Since $\mathrm{Sat}(L_\rho)/L_\rho$ is finite, the rank of $\mathrm{Sat}(L_\rho)$ is the same as that of L_ρ.

By Theorem 2.1(b) and (c), each $I(\rho_j')$ is a prime ideal of codimension $=$ rank(L_ρ). By the first part of Theorem 2.1(d), we have $I(\rho') = \cap_j I(\rho_j')$, so $I(\rho')$ is a radical ideal. The second part of Theorem 2.1(d) shows that $k[x^\pm]/I(\rho)$ has a finite filtration whose factors are isomorphic to $k[x^\pm]/I(\rho')$, so that $I(\rho')$ is nilpotent mod $I(\rho)$. This shows that $I(\rho')$ is the radical of $I(\rho)$.

The equality $I(\rho) = \bigcap_{j=1}^{g} I(\rho_j)$ follows directly from the first part of Theorem 2.1(d). Thus, to establish the assertions about associated primes and primary decomposition, it suffices to show that each $I(\rho_j)$ is $I(\rho_j')$-primary of geometric multiplicity card($\mathrm{Sat}_p(L_\rho)/L_\rho$). Applying the second part of Theorem 2.1(d), we see that $k[x^\pm]/I(\rho_j)$ has a filtration of length g whose successive quotients are all isomorphic to $k[x^\pm]/I(\rho_j')$. Both the fact that $I(\rho_j)$ is primary and the assertion about the geometric multiplicity follow.   □

We next characterize the algebraic sets corresponding to Laurent binomial ideals: They are the translates of algebraic subgroups of $(k^*)^n$. It turns out that the Zariski closure of any subsemigroup of the group $(k^*)^n$ has this form. In the statement below we identify $(k^*)^n$ with the group of characters $\mathrm{Hom}(\mathbf{Z}^n, k^*)$, so that $k[\mathbf{Z}^n]$ is naturally the coordinate ring of $(k^*)^n$.

PROPOSITION 2.3. *Let k be any field.*

(a) *The ideal of polynomials vanishing on any translate of a submonoid of* $(k^*)^n$ *is generated by binomials, and thus has the form* $I(\rho)$ *for some partial character* ρ *on* $\mathbf{Z}^n$.

(b) *The algebraic set* $Z(I(\rho))$ *of points in* $(k^*)^n = \mathrm{Hom}(\mathbf{Z}^n, k^*)$ *where all the elements of* $I(\rho)$ *vanish is the set of characters* $\tilde{\rho}$ *of* $\mathbf{Z}^n$ *that are extensions of* ρ. *If it is nonempty, it is the translate of the subgroup*

$$\mathrm{Hom}(\mathbf{Z}^n/L_\rho, k^*) \subseteq \mathrm{Hom}(\mathbf{Z}^n, k^*)$$

by any such $\tilde{\rho}$.

Proof. (a) Let Γ be a subsemigroup of $(k^*)^n$, and let $\tau \in (k^*)^n$ be any element. We must show that the ideal of Laurent polynomials vanishing on $\tau\Gamma$ is generated by binomials. First suppose that τ is trivial. Each monomial in $k[\mathbf{Z}^n]$ acts as a character on Γ. A Laurent polynomial that vanishes on Γ is thus a linear dependence relation on characters of Γ. Artin's theorem (see, for example, Lang

[L, VIII.4.7]) says that distinct characters are linearly independent, so the dependence relations are generated by the differences of pairs of characters that are equal on Γ, that is, by pure difference binomials.

A function $p: (k^*)^n \to k$ vanishes on $\tau\Gamma$ if and only if the function $(\tau \cdot p)(x) := p(\tau \cdot x)$ vanishes on Γ. Thus, if the ideal of Γ is $I(\sigma)$, where σ is the trivial character on the lattice L_σ, then the ideal of $\tau\Gamma$ is $I(\tau|_{L_\sigma})$.

(b) The assertion is immediate from the identification of points of $(k^*)^n$ with characters of $\mathbf{Z}^n$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Remark. The same argument shows that the ideal of polynomials vanishing on a translate of a subsemigroup of k^n, regarded as a semigroup by component-wise multiplication, is generated by binomials. A variant of this proof shows that any subsemigroup-scheme of $\mathbf{A}^n$ is defined by a binomial ideal. The point is the following version of Artin's theorem: If A is an algebra over a field k with an algebra map $\Delta: A \to A \otimes A$ and $m_1, ..., m_r \in A$ are distinct nonzero elements that are primitive in the sense that $\Delta(m_i) = m_i \otimes m_i$, then $m_1, \ldots, m_r$ are linearly independent in A.

Recall that the *k-radical* $\sqrt[k]{I_\rho}$ of an ideal I in an affine k-algebra A is the ideal of functions vanishing at all the k-rational points of the variety associated to I; that is, it is the intersection of all the maximal ideals of A with residue class field k. We next show that the k-radical of a Laurent binomial ideal is again generated by binomials. In Section 3 we shall use this result to prove the same statement for ideals in a polynomial ring. This question was suggested to us by J. Gamboa.

COROLLARY 2.4. *Let k be any field. If I is a binomial ideal in $k[x^{\pm}]$, then the k-radical of I is generated by binomials.*

Proof. By Proposition 2.3(b) the algebraic set defined by I is a translate of a subgroup, and by Proposition 2.3(a) the ideal of polynomials vanishing on such a set is binomial. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Here is an explicit formula for the radical of a Laurent binomial ideal:

$$\sqrt[k]{I_\rho} = \begin{cases} (1) & \text{if the partial character } \rho: L_\rho \to k^* \text{ has no extension } \mathrm{Sat}(L_\rho) \to k^* \\ I_{\rho'} & \text{where } L' \text{ is the largest sublattice of } \mathrm{Sat}(L_\rho) \text{ on which all} \\ & \text{extensions of } \rho \text{ to } \mathrm{Sat}(L_\rho) \text{ agree and } \rho': L' \to k^* \text{ is their} \\ & \text{common restriction.} \end{cases}$$

The results of Theorem 2.1 can be transferred to certain affine binomial ideals. As in the proof of Theorem 2.1(a), we let $m_+, m_- \in \mathbf{Z}^n_+$ denote the *positive part* and *negative part* of a vector $m \in \mathbf{Z}^n$. Given a partial character ρ on $\mathbf{Z}^n$, we define the ideal

$$I_+(\rho) := (\{x^{m_+} - \rho(m)x^{m_-} : m \in L_\rho\}) \quad \text{in } S = k[x_1, \ldots, x_n]. \qquad (2.3)$$

COROLLARY 2.5. *If I is a binomial ideal in $S = k[x_1, \ldots, x_n]$ not containing any monomial, then there is a unique partial character ρ on $\mathbf{Z}^n$ such that*

$(I: (x_1 \cdots x_n)^\infty) = I_+(\rho)$. *The generators of $I_+(\rho)$ given in (2.3) form a Gröbner basis for any monomial order on S. The binomial ideals of the form $I_+(\rho)$ are precisely those whose associated points are off the coordinate hyperplanes. If k is algebraically closed, then all the statements of Corollary 2.2 continue to hold if we replace each $I(-)$ by $I_+(-)$.*

Proof. The ideal $(I: (x_1 \cdots x_n)^\infty)$ is equal to $I \cdot k[x^\pm] \cap S$, the contraction from the Laurent polynomial ring. By Theorem 2.1(a), there exists a unique partial character ρ such that $I \cdot k[x^\pm] = I(\rho) \cdot k[x^\pm]$. The map $S \to k[x^\pm]$ may be factored through the ring T as in the proof of Theorem 2.1(a). With $I'(\rho)$ defined as in that proof, we have $I \cdot k[x^\pm] \cap S = I'(\rho) \cap S$. Since the elements in the set (2.2) form a Gröbner basis with respect to any monomial order on T, the elements in this set not involving the variables y_i form a Gröbner basis of $I \cdot k[x^\pm] \cap S$. These are exactly the given generators of $I_+(\rho)$.

The third statement holds because an ideal in S whose associated points are off the coordinate hyperplanes is contracted from $k[x^\pm]$. The fourth statement follows at once.   □

Consider a k-algebra homomorphism from $S = k[x_1, \ldots, x_n]$ to the Laurent polynomial ring $k[t^\pm] := k[t_1, t_1^{-1}, \ldots, t_r, t_r^{-1}]$ which sends each variable x_i to a monomial $c_i t^{a_i}$. Its kernel P is a prime ideal, which is generated by binomials. The variety defined by P in k^n is a (not necessarily normal) affine toric variety. For details on toric varieties and their ideals, see Fulton [F], Sturmfels [Stu1], and the references given there. Corollary 2.2 implies that over an algebraically closed field *toric ideals* are the same as binomial prime ideals.

COROLLARY 2.6.   *Let k be an algebraically closed field, and let P be a binomial ideal in $S = k[x_1, \ldots, x_n]$. Set $\{y_1, \ldots, y_s\} := \{x_1, \ldots, x_n\} \cap P$ and let $\{z_1, \ldots, z_t\} := \{x_1, \ldots, x_n\} \backslash P$. The ideal P is prime if and only if*

$$P = (y_1, \ldots, y_s) + I_+(\rho)$$

for a saturated partial character ρ in the lattice $\mathbf{Z}^t$ corresponding to $z_1, \ldots, z_t$. In this case, the prime P is the kernel of a ring homomorphism

$$k[y_1, \ldots, y_s, z_1, \ldots, z_t] \to k[t^\pm], \quad y_i \mapsto 0, \quad z^m \mapsto \tilde{\rho}(m)t^{\bar{m}}, \qquad (2.4)$$

where $\bar{m} \in \mathbf{Z}^t/L_\rho$ denotes the image of $m \in \mathbf{Z}^t$, the group algebra of $\mathbf{Z}^t/L_\rho$ is identified with a Laurent polynomial ring $k[t^\pm]$, and $\tilde{\rho}$ is any extension of ρ to $\mathbf{Z}^t$.

Proof. We must prove the "only if" direction. Given a binomial prime P, consider the binomial prime $P/(y_1, \ldots, y_s)$ in $k[z_1, \ldots, z_t]$. Modulo this prime each z_j is a nonzerodivisor. By Corollary 2.2, we may write $P/(y_1, \ldots, y_s) = I_+(\rho)$. Since $Pk[z^\pm] = I(\rho)$ is prime, Theorem 2.1(c) shows that ρ is saturated. For the proof of the second statement, consider the surjective homomorphism $k[z^\pm] \to k[t^\pm]$, $z^m \mapsto \tilde{\rho}(m)t^{\bar{m}}$. Its kernel obviously contains $Pk[z^\pm]$, and since $Pk[z^\pm]$ is a prime of codimension $\text{rank}(L_\rho) = \dim(k[z^\pm]) - \dim(k[t^\pm])$, the kernel

is precisely P. Since P is the preimage of $Pk[z^{\pm}]$ in S, we conclude that P is the kernel of the composite map $S \to k[z^{\pm}] \to k[t^{\pm}]$, which coincides with (2.4). $\qquad\square$

3. The radical of a binomial ideal. The radical of an ideal I in $S = k[x_1, \ldots, x_n]$ is $\sqrt{I} := \{f \in S \mid f^d \in I \text{ for } d \gg 0\}$. In this section, we show that the family of binomial ideals is closed under taking radicals. We also prove the analogous theorem for the k-radical (defined in the Section 2).

THEOREM 3.1. *Let k be a field, and let $I \subseteq S = k[x_1, \ldots, x_n]$ be an ideal. If I is binomial then the radical and k-radical of I are binomial.*

In the special case where I is generated by pure difference binomials (monomial minus monomial), the result on the ordinary radical was proved using different methods by Robert Gilmer [Gi, Section 9]. Gilmer shows that the radical is again generated by pure difference binomials (something that can also be deduced from the argument below), and he proves a similar statement for the case of an arbitrary base ring. An algorithmic and refined version of Theorem 3.1 for the real radical was given by Becker, Grobe, and Niermann [BGN].

Our proof works by an induction on the number of variables and an application of the Laurent case treated in Corollaries 2.2 (for the ordinary radical) and 2.4 (for the k-radical). For this we use the following lemma.

LEMMA 3.2. *Let R be any commutative ring, and let $x_1, \ldots, x_n \in R$. If I is any ideal in R, then the radical of I satisfies the relation*

$$\sqrt{I} = \sqrt{(I : (x_1 \cdots x_n)^{\infty})} \cap \sqrt{I + (x_1)} \cap \cdots \cap \sqrt{I + (x_n)}. \qquad (3.1)$$

For the k-radical we have the relation

$$\sqrt[k]{I} = \left(\sqrt[k]{Ik[x^{\pm}]} \cap S\right) \cap \sqrt[k]{I + (x_1)} \cap \cdots \cap \sqrt[k]{I + (x_n)}. \qquad (3.2)$$

Proof. The right-hand side clearly contains $\sqrt{I}$. It suffices to show that every prime P containing I contains one of the ideals on the right-hand side. If $(I : (x_1 \cdots x_n)^{\infty})) \subseteq P$ we are done. Otherwise, $f \cdot (x_1 \cdots x_n)^d \in I \subset P$ for some integer d and some $f \in R \backslash P$. This implies $x_i \in P$ for some i. Thus, P contains $I + (x_i)$ as required.

To prove formula (3.2), note that the k-radical of I is the intersection of all the maximal ideals P containing I such that $k[x]/P = k$. Such a maximal ideal P either contains $\sqrt[k]{Ik[x^{\pm}]} \cap S$ or it contains one of the variables x_i. $\qquad\square$

The rest of the arguments we need are identical in the case of the ordinary radical or the k-radical. Thus, for the rest of this section, we use the word "radical" and the symbol $\sqrt{(\ )}$ to denote either the ordinary radical or the k-radical.

LEMMA 3.3. *Let I be a binomial ideal in $S = k[x_1, \ldots, x_n]$. Set $S' = k[x_1, \ldots, x_{n-1}]$. If $I' = I \cap S'$, then $I + (x_n)$ is the sum of $I'S + (x_n)$ and an ideal generated by monomials in S'.*

Proof. Every binomial that involves x_n is either contained in (x_n) or is congruent modulo (x_n) to a monomial in S'. Thus, all generators of I which are not in I' may be replaced by monomials in S' when forming a generating set for $I + (x_n)$. $\square$

PROPOSITION 3.4. *Let I be a radical binomial ideal in S. If M is a monomial ideal, then $\sqrt{I + M} = I + M_1$ for some monomial ideal M_1.*

Remark. Once we have established Theorem 3.1, we can drop the hypothesis that I is radical in Proposition 3.4 and change the conclusion to $\sqrt{I + M} = \sqrt{I} + M_1$.

Proof. We apply Lemma 3.2 to the ideal $I + M$. If $M = (0)$ there is nothing to prove, so we may assume that M actually contains a monomial. In this case $((I + M): (x_1 \cdots x_n)^\infty) = S$, and Lemma 3.2 yields $\sqrt{I + M} = \bigcap_{i=1}^{n} \sqrt{I + M + (x_i)}$. By Corollary 1.5, it suffices to show that the radical of $I + M + (x_i)$ is the sum of I and a monomial ideal.

For simplicity, let $i = n$ and write $S' = k[x_1, \ldots, x_{n-1}]$. Since I is radical, the ideal $I' = I \cap S'$ is radical as well. By Lemma 3.3, $I + M + (x_n) = I'S + M'S + (x_n)$ where M' is a monomial ideal in S'. By induction on n, the radical of $I' + M'$ in S' has the form $I' + M_1'$, where M_1' is a monomial ideal of S'. Putting this together, we get

$$\sqrt{I + M + (x_n)} = \sqrt{I'S + M'S + (x_n)}$$

$$= I'S + M_1'S + (x_n)$$

$$\subseteq I + M_1'S + (x_n)$$

$$\subseteq \sqrt{I + M + (x_n)},$$

so $\sqrt{I + M + (x_n)} = I + M_1'S + (x_n)$ is I plus a monomial ideal, as required. $\square$

Proof of Theorem 3.1. We proceed by induction on n, the result being trivial for $n = 0$. Let I be a binomial ideal in S. Let $I_j := I \cap S_j$ where $S_j = k[x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n]$. By induction we may assume that the radical of each I_j is binomial. Adding these binomial ideals to I, we may assume that each I_j is radical to begin with.

We shall use formula (3.1) for $\sqrt{I}$ and formula (3.2) for $\sqrt[k]{I}$. Either of the ideals $\sqrt{(I: (x_1 \cdots x_n)^\infty)}$ or $(\sqrt[k]{Ik[x^{\pm}]} \cap S)$ is binomial by Corollaries 1.7, 2.2, and 2.4 or 2.5, and we can write it as $I + I'$ for some binomial ideal I'. By Corollary 1.5 the intersection in formula (3.1) or (3.2) is binomial if $\sqrt{I + (x_j)}$ is the sum of I and a monomial ideal. By Lemma 3.3, we can write $I + (x_j) = I_jS + JS + (x_j)$, where J is a monomial ideal in S_j. Since I_j is radical, the ideal I_jS is radical, so we can apply Proposition 3.4 with $M = JS + (x_i)$ to see that there exists a monomial ideal

M_1 in S such that

$$\sqrt{I + (x_j)} = \sqrt{I_j S + J S + (x_j)} = I_j S + M_1.$$

It follows that $\sqrt{I + (x_j)} = I + M_1$ has the desired form.   □

Example 3.5. Permanental ideals. We do not know how to tell whether a binomial ideal is radical just from the shape of a generating set. As an example, consider the ideal $P_{m,n}$ generated by the 2×2-subpermanents $x_{ij}x_{kl} + x_{il}x_{kj}$ of an $m \times n$-matrix (x_{ij}) of indeterminates over a field k with char$(k) \neq 2$. If $m \leqslant 2$ or $n \leqslant 2$, then $P_{m,n}$ is a radical ideal. (This can be shown using the technique in Proposition 4.8.) For instance, we have

$$P_{2,3} = (x_{11}, x_{12}, x_{13}) \cap (x_{21}, x_{22}, x_{23}) \cap (x_{11}x_{22} + x_{12}x_{21}, x_{13}, x_{23})$$

$$\cap (x_{11}x_{23} + x_{13}x_{21}, x_{12}, x_{22}) \cap (x_{12}x_{23} + x_{13}x_{22}, x_{11}, x_{21}).$$

However, if $m, n \geqslant 3$, then $P_{m,n}$ is not radical: $x_{11}^2 x_{22} x_{33} \in P_{m,n}$ but $x_{11}x_{22}x_{33} \notin P_{m,n}$. Of course, if the plus signs in the generators of $P_{m,n}$ are changed to minus signs, we get a determinantal ideal that is prime for every m and n.

Example 3.6. k'-radicals. We may interpolate between the ordinary radical and the k-radical as follows: If k' is a field containing k, define the k'-radical of I to be the intersection of those maximal ideals of S that contain I and have residue class fields that are k-subalgebras of the given field k'. However, the k'-radical of a binomial ideal is not in general binomial. Consider, for example, the ideal I in the polynomial ring $k[x]$ in one variable generated by the binomial

$$b := x^8 - a^8 = (x^2 - a^2)(x^2 + a^2)(x^4 + a^2 x^2 + a^4)$$

over a field k that contains a^2. Let ζ be a primitive eighth root of unity, and set $k' := k[\zeta a]$. The k'-radical of I is generated by the product of those irreducible factors of b that have a root in k'. Suppose that $k[a]$ and $k[\zeta]$ are linearly disjoint over k, of degrees 2 and 4, respectively. It follows that $k' := k[\zeta a]$ has degree 4 over k, so the factor $(x^4 + a^2 x^2 + a^4)$ is irreducible and has a root in k'.

The roots of $(x^2 - a^2)$ are a and $-a$. If either of these were contained in k', then we would have $k' = k[\zeta, a]$; since the field $k[\zeta, a]$ has degree 8 over k, this is a contradiction. A similar argument shows that neither root of $(x^2 + a^2)$ is in k'. Thus the k'-radical of I is generated by $(x^4 + a^2 x^2 + a^4)$, which is not a binomial.

4. Binomial algebraic sets. We next characterize intersections of prime binomial ideals that are generated by binomials. The result is best stated geometrically. For this purpose, we define an algebraic set to be a reduced affine algebraic scheme over k. (Alternately, one may work with ordinary algebraic sets defined by equations with coefficients in k but having points with coordinates in some fixed algebraic closure of k, or one may simply restrict to the case where k is algebraically closed.) By Theorem 3.1, an algebraic set is cut out by binomials

set-theoretically, if and only if its ideal is generated by binomials. Such a set is called a *binomial algebraic set.*

We decompose affine n-space k^n into tori corresponding to the 2^n coordinate flats

$$(k^*)^{\mathscr{E}} := \{(p_1, \ldots, p_n) \in k^n \mid p_i \neq 0 \text{ for } i \in \mathscr{E}, \, p_i = 0 \text{ for } i \notin \mathscr{E}\}, \qquad (4.1)$$

where $\mathscr{E}$ runs over all subsets of $\{1, \ldots, n\}$. We shall refer to the tori $(k^*)^{\mathscr{E}}$ as *coordinate cells.* The closure of a coordinate cell $(k^*)^{\mathscr{E}}$ in k^n is defined by the ideal

$$M(\mathscr{E}) := (\{x_i \mid i \notin \mathscr{E}\}) \quad \text{in } S = k[x_1, \ldots, x_n].$$

The coordinate ring of $(k^*)^{\mathscr{E}}$ is the Laurent polynomial ring

$$k[\mathscr{E}^{\pm}] := k\left[\{x_i, x_i^{-1}\}_{i \in \mathscr{E}}\right].$$

There is a *coordinate projection* $(k^*)^{\mathscr{E}'} \to (k^*)^{\mathscr{E}}$ whenever $\mathscr{E} \subseteq \mathscr{E}' \subseteq \{1, \ldots, n\}$. It is defined by setting all those coordinates not in $\mathscr{E}$ to zero.

If X is any subscheme of k^n, corresponding to an ideal $I \subseteq S$, then the closure of the intersection of X with the coordinate cell $(k^*)^{\mathscr{E}}$ corresponds to the ideal

$$I_{\mathscr{E}} := \left((I + M(\mathscr{E})) : \left(\prod_{i \in \mathscr{E}} x_i\right)^{\infty}\right). \qquad (4.2)$$

This ideal can be identified with the image of I in $k[\mathscr{E}^{\pm}]$. If I is radical, then it is easy to see that $I = \bigcap_{\mathscr{E}} I_{\mathscr{E}}$ (a more refined version of this is proved in Theorem 6.2). If I is generated by binomials, then by Corollary 1.7 the ideal $I_{\mathscr{E}}$ is also generated by binomials.

The binomial ideals in $k[\mathscr{E}^{\pm}]$ are completely classified by Theorem 2.1, and Corollary 2.2 tells just when they are radical. Thus, to classify all binomial algebraic sets X, it suffices to tell how the intersections of X with the coordinate cells can fit together.

THEOREM 4.1. *Let k be any field. An algebraic set $X \subseteq k^n$ is cut out by binomials if and only if the following three conditions hold.*

(i) *For each coordinate cell $(k^*)^{\mathscr{E}}$, the algebraic set $X \cap (k^*)^{\mathscr{E}}$ is cut out by binomials.*

(ii) *The family of sets $U = \{\mathscr{E} \subseteq \{1, \ldots, n\} \mid X \cap (k^*)^{\mathscr{E}} \neq \varnothing\}$ is closed under taking intersections.*

(iii) *If $\mathscr{E}, \mathscr{E}' \in U$ and $\mathscr{E} \subset \mathscr{E}'$, then the coordinate projection $(k^*)^{\mathscr{E}'} \to (k^*)^{\mathscr{E}}$ maps $X \cap (k^*)^{\mathscr{E}'}$ onto a subset of $X \cap (k^*)^{\mathscr{E}}$.*

We shall use the following definition and result. A partially ordered set U is a *meet semilattice* if every finite subset $\{u_1, \ldots, u_m\} \subset U$ has a unique greatest lower bound in U. This lower bound is denoted $u_1 \wedge \cdots \wedge u_m$ and called the *meet* of $u_1, \ldots, u_m$ in U.

LEMMA 4.2. *Let U be a finite meet semilattice and R any commutative ring. For each $u \in U$, let J_u and M_u be ideals in R such that*

(a) *if $u \leqslant v$, then $\sqrt{J_u} \subseteq \sqrt{J_v}$, and*

(b) $\sqrt{M_{u \wedge v}} \subseteq \sqrt{M_u + M_v}$. *Under these assumptions, the two ideals*

$$I_1 = \bigcap_{u \in U} (J_u + M_u)$$

and

$$I_2 = \left(\bigcap_{u \in U} M_u \right) + \sum_{u \in U} \left(J_u \cap \bigcap_{t \not\geqslant u} M_t \right)$$

have the same radical $\sqrt{I_1} = \sqrt{I_2}$.

Proof. To prove that $\sqrt{I_2} \subseteq \sqrt{I_1}$, it suffices to show that for all $u, v \in U$ we have

$$J_u \cap \bigcap_{t \not\geqslant u} M_t \subseteq \sqrt{J_v} + M_v.$$

If $u \leqslant v$, then $\sqrt{J_u} \subseteq \sqrt{J_v}$ by condition (a), so $\sqrt{J_v}$ contains the left-hand side, and we are done. If, on the contrary, $u \not\leqslant v$, then v is among the indices t appearing on the left-hand side, so M_v contains the left-hand side, and this suffices as well.

To prove that $\sqrt{I_1} \subseteq \sqrt{I_2}$, choose a prime P containing I_2. We must show that P also contains I_1. Let $V = \{v \in U \,|\, M_v \subseteq P\}$. From hypothesis (b), we see that if $v, v' \in V$, then $v \wedge v' \in V$. Since $P \supset \bigcap_{u \in U} M_u$, the set V is nonempty. Thus, there is a unique minimal element $w \in V$. Since $P \supseteq I_2 \supseteq J_w \cap \bigcap_{t \not\geqslant w} M_t$ and P does not contain any M_t with $t \not\geqslant w$, we see that P contains J_w. Thus, P contains $J_w + M_w$ and with it I_1. $\qquad\square$

Here is the key part of the argument proving that binomial ideals satisfy property (iii) of Theorem 4.1, isolated for future use.

LEMMA 4.3. *Let*

$$R := k[z_1, z_1^{-1}, \ldots, z_t, z_t^{-1}] \subset R' := k[z_1, z_1^{-1}, \ldots, z_t, z_t^{-1}, y_1, \ldots, y_s]$$

be a Laurent polynomial ring and a polynomial ring over it. If $B \subset R'$ is a binomial ideal and $M \subset R'$ is a monomial ideal such that $B + M$ is a proper ideal in R', then

$$(B + M) \cap R = B \cap R.$$

Proof. Suppose $f \in (B + M) \cap R$. The terms of f are invertible in R'. Since $B + M \neq R'$, no term of f is in $B + M$. Proposition 1.10 implies that $f \in B$. $\qquad\square$

Proof of Theorem 4.1. Let $X \subset k^n$ be any algebraic set with ideal $I \subset S$. Let U be the set of subsets $\mathscr{Z} \subset \{1, \ldots, n\}$ such that $X \cap (k^*)^{\mathscr{E}}$ is nonempty, or equivalently, $I_{\mathscr{E}} \neq S$.

Suppose X is a binomial algebraic set. The ideal $I_{\mathscr{E}}$ is binomial by Corollary 1.7, so $X \cap (k^*)^{\mathscr{E}}$ is cut out by binomials, proving condition (i). To prove condition (ii), we must show that if $\mathscr{E}_1, \mathscr{E}_2 \in U$, then $\mathscr{E}_1 \cap \mathscr{E}_2 \in U$. If, on the contrary,

$\mathscr{E}_1 \cap \mathscr{E}_2 \notin U$, then for some integer d,

$$\left(\prod_{i \in \mathscr{E}} x_i\right)^d \in I + M(\mathscr{E}_1 \cap \mathscr{E}_2) = I + M(\mathscr{E}_1) + M(\mathscr{E}_2).$$

Corollary 1.6(b) implies that $(\prod_{i \in \mathscr{E}} x_i)^d$ is either in $I + M(\mathscr{E}_1)$ or $I + M(\mathscr{E}_2)$. Consequently, either $I_{\mathscr{E}_1}$ or $I_{\mathscr{E}_2}$ is the unit ideal in S, contradicting our assumption.

Write $k[\mathscr{E}]$ for the polynomial ring $k[\{x_i\}_{i \in \mathscr{E}}]$. The algebraic form of condition (iii) is the statement that if $\mathscr{E}, \mathscr{E}' \in U$ with $\mathscr{E} \subset \mathscr{E}'$, then $I_{\mathscr{E}} \cap k[\mathscr{E}] \subseteq I_{\mathscr{E}'}$. Since $I_{\mathscr{E}'} = (I_{\mathscr{E}'} : \prod_{i \in \mathscr{E}} x_i)$, it suffices to prove this condition after inverting the x_i for $i \in \mathscr{E}$. That is, if we set $R' = k[\mathscr{E}^{\pm}][\{x_i\}_{i \notin \mathscr{E}}]$, then we must show that

$$(I + M(\mathscr{E}))R' \cap k[\mathscr{E}^{\pm}] \subseteq I_{\mathscr{E}'}R'.$$

Since $\mathscr{E} \in U$, the ideal $(I + M(\mathscr{E}))R'$ is proper, and we may apply Lemma 4.3 to get $(I + M(\mathscr{E}))R' \cap k[\mathscr{E}^{\pm}] = IR' \cap k[\mathscr{E}^{\pm}]$. Since $I \subseteq I_{\mathscr{E}'}$, we are done.

Conversely, suppose that X is any algebraic set satisfying conditions (i), (ii), and (iii). We must show that the ideal I of X is generated by binomials. We have already remarked that $I = \bigcap_{\mathscr{E} \in U} I_{\mathscr{E}}$. Note that U is a partially ordered set under the inclusion relation for subsets of $\{1, \ldots, n\}$. By condition (ii), the set U is closed under intersections, so U is a meet semilattice. For $\mathscr{E} \in U$, we set $J(\mathscr{E}) := (I_{\mathscr{E}} \cap k[\mathscr{E}])S$ and, as before, $M(\mathscr{E}) = (\{x_i \mid i \notin \mathscr{E}\})$. We shall apply Lemma 4.2 to these ideals. Hypothesis (b) of Lemma 4.2 is obvious from the definition of $M(\mathscr{E})$, and hypothesis (a) is implied by the algebraic form of condition (iii) given above. The ideal $I_1 = \bigcap_{\mathscr{E} \in U}(J(\mathscr{E}) + M(\mathscr{E}))$ equals $\bigcap_{\mathscr{E} \in U} I_{\mathscr{E}} = I$. Each $J(\mathscr{E})$ is a binomial ideal by Corollary 1.3, and each $M(\mathscr{E})$ is a monomial ideal. Hence, each term in the sum

$$I_2 = \sum_{\mathscr{E} \in U}\left(J(\mathscr{E}) \cap \bigcap_{\mathscr{E}' \not\geq \mathscr{E}} M(\mathscr{E}')\right)$$

is a binomial ideal by Corollary 1.5. This shows that I_2 is binomial. Theorem 3.1 now implies that $\sqrt{I_2} = \sqrt{I_1} = I$ is binomial, as claimed. $\square$

Problem 4.4. Find the generators. In the application of Lemma 4.2 made in the proof of Theorem 4.1, are the ideals I_1 and I_2 actually equal? This is the case when the set U is totally ordered and in other examples we have tried, such as the following.

Example 4.5. Subsets of the vertex set of the coordinate cube. For each $\mathscr{E} \subseteq \{1, \ldots, n\}$, let $p_{\mathscr{E}}$ be the point whose ith coordinate is 1 if $i \in \mathscr{E}$ and 0 otherwise. Let U be a collection of subsets of $\{1, \ldots, n\}$. The finite algebraic set

$$X_U := \{p_{\mathscr{E}} \mid \mathscr{E} \in U\} \subset k^n$$

is cut out by binomials if and only if U is closed under taking intersections. We remark that for *any* collection U of subsets, the ideal of X_U is generated by the n binomials $x_i(x_i - 1)$ for $1 \leqslant i \leqslant n$ (these generate the ideal of all the 2^n points $p_{\mathscr{E}}$) and the $\operatorname{card}(U)$ elements

$$\prod_{i \in \mathscr{E}} (x_i - 1) \prod_{i \notin \mathscr{E}} x_i \qquad \text{for } \mathscr{E} \in U.$$

Example 4.6. A binomial algebraic set whose top-dimensional part is not binomial. Consider the following three binomial varieties in affine 4-space k^4:

$$V_1 = V(x_1 x_2 - 1, x_3, x_4), \quad \text{a hyperbola in the cell } (k^*)^{\{1,2\}};$$

$$V_2 = V(x_1, x_2, x_3 x_4 - 1), \quad \text{a hyperbola in the cell } (k^*)^{\{3,4\}};$$

$$V_3 = V(x_1, x_2, x_3, x_4), \qquad \text{the unique point in the cell } (k^*)^{\varnothing}.$$

The union of these varieties is defined by the binomial ideal

$$I(V_1 \cup V_2 \cup V_3) = I(V_1) \cap I(V_2) \cap I(V_3)$$

$$= (x_1^2 x_2 - x_1, x_1 x_2^2 - x_2, x_3^2 x_4 - x_3, x_3 x_4^2 - x_4, x_1 x_3, x_1 x_4, x_2 x_3, x_2 x_4).$$

However, the union of V_1 and V_2, the top-dimensional components, is not cut out by binomials. Its ideal $I(V_1 \cup V_2)$ has the reduced Gröbner basis

$$\{x_1 x_2 + x_3 x_4 - 1, x_3^2 x_4 - x_3, x_3 x_4^2 - x_4, x_1 x_3, x_1 x_4, x_2 x_3, x_2 x_4\}.$$

By homogenizing these equations, we get a projective binomial scheme with the same property. Note also that $(I(V_1 \cup V_2 \cup V_3) : (x_1, x_4)) = I(V_1 \cup V_2)$, so this ideal also exhibits the phenomenon of Example 1.8. $\qquad \square$

Example 4.7. Face rings of polyhedral complexes (cf. Stanley [Sta, Section 4]). By a *lattice polytope* in $\mathbf{R}^m$, we mean the convex hull of a finite subset of $\mathbf{Z}^m$. A (finite, integral) *polyhedral complex* Δ is a finite set of lattice polytopes in $\mathbf{R}^m$, satisfying

(i) any face of a polytope in Δ is a polytope in Δ;
(ii) any two of the polytopes in Δ intersect in a set that is a face of each of them.

The polytopes in Δ are called *faces* of Δ. The maximal faces are called *facets*. We write $\mathscr{F}(\Delta)$ for the set of facets of Δ. For each face $P \in \Delta$, we define a cone

$$C_P = \{(a_1, \ldots, a_m, b) \in \mathbf{R}^{m+1} \mid (a_1, \ldots, a_m, b) = (0, \ldots, 0, 0)$$

$$\text{or } b \neq 0 \text{ and } (a_1/b, \ldots, a_m/b) \in P\}.$$

Following Stanley [Sta], we define *face ring* $k[\Delta]$ of Δ to be the ring having vector space basis over k the set of monomials $\{y^\alpha \,|\, \alpha \in C_P \cap \mathbf{Z}^{m+1}$ for some $P \in \Delta\}$ with multiplication

$$y^\alpha y^\beta = \begin{cases} y^{\alpha+\beta}, & \text{if } \alpha, \beta \in C_P \text{ for some } P \in \Delta; \\ 0, & \text{otherwise.} \end{cases}$$

If Δ has a single facet P, then the face ring of Δ is the homogeneous coordinate ring $k[P]$ of the projective toric variety associated with the lattice polytope P (see, for example, Fulton [F] or Sturmfels [Stu1]). We may represent it as

$$k[P] = k[\{x_i\}_{i \in G(P)}]/I(P),$$

where the x_i are variables indexed by the unique minimal set $G(P) \subset \mathbf{Z}^{m+1}$ of additive generators for the monoid $C_P \cap \mathbf{Z}^{m+1}$ and $I(P)$ is the binomial prime ideal of relations among the monomials y^β for $\beta \in G(P)$.

More generally, let $G(\Delta) := \bigcup_{P \in \mathscr{F}(\Delta)} G(P)$. We may represent the face ring of Δ as

$$k[\Delta] = k[\{x_i\}_{i \in G(\Delta)}]/I(\Delta)$$

for some ideal $I(\Delta)$. This ideal is an intersection of binomial primes satisfying Theorem 4.1, so it is generated by binomials. The following more precise result is implicit in Stanley [Sta]; the proof was communicated to us privately by Stanley. Its geometric interpretation is that the projective scheme $\operatorname{Proj}(k[\Delta])$ is the reduced union of the toric varieties $\operatorname{Proj}(k[P])$, glued along orbit closures corresponding to intersections of facets in Δ.

PROPOSITION 4.8.   *The ideal $I(\Delta)$ defining the face ring $k[\Delta]$ is the intersection of the binomial primes $I(P) + (\{x_i\}_{i \in G(\Delta) \setminus G(P)})$, where P ranges over the set of facets $\mathscr{F}(\Delta)$. The ideal $I(\Delta)$ is generated by $\sum_{P \in \mathscr{F}(\Delta)} I(P)$ together with all the monomials $x_{i_1} \cdots x_{i_s}$ such that $i_1, \ldots, i_s$ do not all lie in any facet of Δ.*

Proof.   The k-basis given for $k[\Delta]$ in the definition is a subset of the natural vector space basis of $\prod_{P \in \mathscr{F}(\Delta)} k[P]$. The description of the multiplication gives an inclusion of k-algebras $k[\Delta] \subset \prod_{P \in \mathscr{F}(\Delta)} k[P]$. The ideal $I(\Delta)$ is by definition the kernel of the natural map $k[\{x_i\}_{i \in G(\Delta)}] \to \prod_{P \in \mathscr{F}(\Delta)} k[P]$. It follows that $I(\Delta)$ is the intersection of the ideals $J(P) := \ker(k[\{x_i\}_{i \in G(\Delta)}] \to k[P])$ for $P \in \mathscr{F}(\Delta)$, and it is immediate that $J(P) = I(P) + (\{x_i\}_{i \in G(\Delta) \setminus G(P)})$. This proves the first assertion.

Let I be the ideal generated by $\sum_{P \in \mathscr{F}(\Delta)} I(P)$ and the nonfacial monomials $x_{i_1} \cdots x_{i_s}$. The inclusion $I \subseteq I(\Delta)$ is evident, so we get a surjection from $R := k[\{x_i\}_{i \in G(\Delta)}]/I$ onto $k[\Delta]$. Each nonzero monomial in R is mapped to a monomial y^β in $k[P]$ for some P. Any two preimages of y^β differ by an element of

$I(P) \subset I$, hence they are equal in R. This shows that the surjection is injective as well, and therefore I equals $I(\Delta)$, as desired. $\qquad\square$

Problem 4.9. Intersections of binomial ideals. It would be nice to have a result like Theorem 4.1 for the intersections of arbitrary binomial ideals, not just radical binomial ideals. A first step might be to answer the following question: Which sets of primes can be the set of associated primes of a binomial ideal?

In some cases a fairly straightforward generalization to schemes of Theorem 4.1 seems to be all that is necessary. For example, the following union of three lines, contained in the closures of the $\{x_3\}$-cell, the $\{x_2, x_3\}$-cell, and the $\{x_1, x_3\}$-cell, respectively, is binomial:

$$(x_1, x_2) \cap (x_1, x_2 - x_3) \cap (x_2, x_1 - x_3).$$

If we thicken the line in the $\{x_2, x_3\}$-cell, then we get a scheme that is not binomial:

$$(x_1, x_2) \cap (x_1^2, x_2 - x_3) \cap (x_2, x_1 - x_3).$$

However, if we also thicken the line in the $\{x_3\}$-cell enough so that the line in the x_2, x_3-cell projects into it,

$$(x_1^2, x_2) \cap (x_1^2, x_2 - x_3) \cap (x_2, x_1 - x_3);$$

then again we get a binomial scheme. $\qquad\square$

5. Some binomial ideal quotients.

The theory of binomial ideals would be much easier if the quotient of a binomial ideal by a binomial were again a binomial ideal. Here is a simple example where this fails.

Example 5.1. Let $I = (x_1 - yx_2, x_2 - yx_3, x_3 - yx_1) \subset k[x_1, x_2, x_3, y]$. The ideal $(I : (1 - y)) = (x_1 + x_2 + x_3, x_2^2 + x_2x_3 + x_3^2, x_2y + x_2 + x_3, x_3y - x_2)$ is not binomial: the given generators form a reduced Gröbner basis, so Corollary 1.2 applies.

By reducing problems to coordinate cells $(k^*)^{\mathscr{E}}$ as in Section 4, we can often assume that some variables are nonzerodivisors modulo a given binomial ideal I. In such a case, certain ideal quotients of I by a binomial are again binomial. These results will play a central role in the construction of a binomial primary decomposition.

The ordinary powers of a binomial are not binomials. However, there is a natural binomial operation that has many features in common with taking powers: If m and n are terms, so that $b := m - n$ is a binomial, then we set $b^{[d]} := m^d - n^d$ and call it the dth *quasi-power* of b. If d is even, then $(-n)^d - (-m)^d = -(m^d - n^d)$. Thus, the sign of the quasi-power depends on the choice of which term of b is chosen to be "first." We may remove the ambiguity by choosing a

monomial order on S and always choosing the expression for b with $m < n$. Note that if $d \,|\, e$, then $b^{[d]} \,|\, b^{[e]}$.

THEOREM 5.2.   Let I be a binomial ideal in $S = k[x_1, \ldots, x_n]$ and $<$ a monomial order on S. Suppose $b := x^\alpha - ax^\beta$ is a binomial and $f \in S$ such that $bf \in I$ but x^α is a nonzerodivisor mod I. Let $f_1 + \cdots + f_s$ be the normal form of f modulo I with respect to $<$, where $f_1, \ldots, f_s$ are monomials. If d is a sufficiently divisible positive integer, then we have the following.

(a) The binomials $b^{[d]} f_j$ lie in I for $j = 1, \ldots, s$.

(b) $(I : b^{[d]})$ is generated by monomials modulo I, and is thus a binomial ideal.

(c) Let $p = \operatorname{char}(k)$. If $p = 0$, let $q = 1$, while if $p > 0$, let q be the largest power of p that divides d. If e is a divisor of d that is divisible by q, then $(I : (b^{[d]}/b^{[e]}))$ is a binomial ideal.

Proof.   (a) To say that $f_1 + \cdots + f_s$ is the normal form of f modulo I means that $f \equiv f_1 + \cdots + f_s \pmod{I}$ and that the f_i are terms not in $in_<(I)$. By Proposition 1.1(b), the normal form of each term $x^\alpha f_i$ or $ax^\beta f_j$ is a term. Since x^α is a nonzerodivisor modulo I, the terms $x^\alpha f_i$, $i = 1, \ldots, s$, have normal forms that are nonzero scalars times distinct monomials. The equation $(x^\alpha - ax^\beta) f \equiv 0 \bmod I$ shows that for each of the s terms $x^\alpha f_i$, there exists a term $ax^\beta f_j$ with the same normal form, and by counting we see that j is uniquely determined. Thus, there is a permutation π of $\{1, \ldots, s\}$ such that $x^\alpha f_i \equiv ax^\beta f_{\pi(i)}$ for all i. It follows at once by induction on d that

$$(x^\alpha)^d f_i \equiv (ax^\beta)^d f_{\pi^d(i)} \pmod{I}.$$

Taking d divisible by the order of π, part (a) follows.

(b) If d and d' are positive integers such that d divides d', then the binomial $b^{[d]}$ divides the binomial $b^{[d']}$, so that $(I : b^{[d]}) \subseteq (I : b^{[d']})$. Since S is Noetherian, we may choose d sufficiently divisible so that equality holds for all integers d' divisible by d. We claim that for such a choice of d, the conclusion of part (b) is satisfied. Let $f \in (I : b^{[d]})$. By induction on the number of terms f_i in the normal form of f modulo I, it suffices to show that the first term f_1 is in $(I : b^{[d]})$. By part (a) applied to $b^{[d]}$, there is an integer d' such that $f_1 \in (I : b^{[dd']})$. By the choice of d, we have $f_1 \in (I : b^{[d]})$ as desired.

For the proof of part (c), we use a general fact.

LEMMA 5.3.   Let R be any commutative ring and $f, g \in R$. If $(f, g) = R$, then $(0 : g) = (0 : fg)f$.

Proof.   It is immediate that $(0 : g) \supseteq (0 : fg)f$. For the opposite inclusion, suppose $x \in (0 : g)$. Since $(f, g) = R$, we may write $1 = af + bg$ with $a, b \in R$, so we have $x = xaf + bgx = xaf$. Since $xa \cdot fg = xg \cdot af = 0 \cdot af = 0$, we get $x = xaf \in (0 : fg)f$.   □

Proof of Theorem 5.2(c). We apply Lemma 5.3 to the ring $R = (S/I)[1/x^\alpha]$ with $f = b^{[e]}$ and $g = b^{[d]}/b^{[e]}$. The hypothesis $(f, g) = R$ of Lemma 5.3 holds because over the algebraic closure $\bar{k}$ of k we have the factorizations

$$f = \prod_{\eta \in k^*, \eta^{e/q}=1} (x^{q\alpha} - \eta a^q x^{q\beta})$$

$$= \prod_{\zeta \in k^*, \zeta^{d/q}=1, \zeta^{e/q} \neq 1} (x^{q\alpha} - \zeta a^q x^{q\beta}).$$

Any factor of f together with any factor of g generates the unit ideal, and hence $(f, g) = R$.

If J is an arbitrary ideal of S, then the preimage of JR in S is $((I + J) : (x^\alpha)^\infty)$. If $J = (I : g)$ then $I \subseteq (I : g)$. Since x^α is a nonzerodivisor modulo I, it is also a nonzerodivisor modulo $(I : g)$. Thus, the preceding formula simplifies, and the preimage of $(I : g)R$ in S is equal to $(I : g)$. Applying Lemma 5.3 and pulling everything back to S, we get

$$(I : g) = ((I + (I : fg)f) : (x^\alpha)^\infty) \quad \text{in } S.$$

By part (b), the ideal $(I : fg) = (I : b^{[d]})$ is generated modulo I by monomials. Since $f = b^{[e]}$ is a binomial, $I + (I : fg)f$ is binomial. By Corollary 1.7, the quotient $((I + (I : fg)f) : (x^\alpha)^\infty)$ is a binomial ideal, and thus $(I : g)$ is binomial as desired. $\square$

Example 5.1, continued. For $I = (x_1 - yx_2, x_2 - yx_3, x_3 - yx_1)$, the ideals $(I : (1 - y^3)) = (x_1, x_2, x_3)$ and $(I : (1 + y + y^2)) = (x_1 - x_3, x_2 - x_3, x_3y - x_3)$ are binomial.

Example 5.4. The hypothesis that x^α is a nonzerodivisor is necessary for Theorem 5.2(b) to hold. For instance, consider the radical binomial ideal

$$I = (ux - uy, uz - vx, vy - vz)$$

$$= (x, y, z) \cap (u, v) \cap (u, x, y - z) \cap (v, z, x - y) \cap (x - y, y - z, u - v)$$

in $k[x, y, z, u, v]$. Both u and v are zero divisors mod I. For each positive integer d, we have

$$(I : (u^d - v^d)) = (x - y + z, uz, yz - z^2, vy - vz).$$

This quotient is not a binomial ideal. $\square$

6. Associated primes, isolated components, and cellular decomposition. The decompositions in a univariate polynomial ring

$$(x^d - 1) = (x - 1) \cap (x^{d-1} + \cdots + x + 1)$$

$$(x^{d-1} + \cdots + x + 1) = \bigcap_{\zeta^d = 1, \zeta \neq 1} (x - \zeta) \tag{6.1}$$

show that in order for the associated primes of a binomial ideal to be binomial, we must work over a field k containing the roots of unity. Further, for the minimal primes of $(x^d - a)$ to have the form given in Corollary 2.6, the scalar $a \in k$ must have all its dth roots in k. This is the reason why k is taken to be algebraically closed in the following theorem.

THEOREM 6.1. *Let k be an algebraically closed field. If I is a binomial ideal in $S = k[x_1, \ldots, x_n]$, then every associated prime of I is generated by binomials.*

Proof. If $I = I_+(\rho) = I(\rho) \cap k[x_1, \ldots, x_n]$ for some partial character ρ on $\mathbf{Z}^n$, then Corollary 2.5 implies the desired result. We may therefore assume that there is a variable x_i such that $(I : x_i) \neq I$. If $x_i \in I$, we may reduce modulo x_i and do induction on the number of variables. Hence, we may assume that $x_i \notin I$. From the short exact sequence

$$0 \to S/(I : x_i) \to S/I \to S/(I, x_i) \to 0, \tag{6.2}$$

we see that $\mathrm{Ass}(S/I) \subseteq \mathrm{Ass}(S/(I : x_i)) \cup \mathrm{Ass}(S/(I, x_i))$. By Noetherian induction and Corollary 1.7, both sets consist of binomial primes. $\square$

Corollary 2.5 does primary decomposition for binomial ideals whose associated points are all contained in the open cell away from the coordinate hyperplanes. This suggests dividing up the primary components according to which coordinate cells they lie in. We define an ideal I of S to be *cellular* if, for some $\mathscr{E} \subseteq \{1, \ldots, n\}$, we have $I = (I : (\prod_{i \in \mathscr{E}} x_i)^\infty)$ and I contains a power of $M(\mathscr{E}) = (\{x_i\}_{i \notin \mathscr{E}})$. This means that the scheme defined by I has each of its associated points in the cell $(k^*)^{\mathscr{E}}$.

Given any ideal $I \subseteq S$, we can manufacture cellular ideals from I as follows. For each vector of positive integers $d = (d_1, \ldots, d_n)$ and each subset $\mathscr{E}$ of $\{1, 2, \ldots, n\}$, we set

$$I_{\mathscr{E}}^{(d)} := \left((I + (\{x_i^{d_i}\}_{i \notin \mathscr{E}})) : \left(\prod_{j \in \mathscr{E}} x_j \right)^\infty \right). \tag{6.3}$$

For $d = (1, \ldots, 1)$ we have $I_{\mathscr{E}}^{(d)} = I_{\mathscr{E}}$, the ideal considered for I radical in Section 4.

THEOREM 6.2.   *The ideal $I_{\mathscr{E}}^{(d)}$ is a cellular binomial ideal for all I, d and $\mathscr{E}$. For distinct $\mathscr{E}$ and $\mathscr{E}'$ the sets of associated primes $\text{Ass}(I_{\mathscr{E}}^{(d)})$ and $\text{Ass}(I_{\mathscr{E}'}^{(d)})$ are disjoint. If the integers d_i are chosen sufficiently large, then*

$$I = \bigcap_{\mathscr{E} \subseteq \{1,\ldots,n\}} I_{\mathscr{E}}^{(d)}. \tag{6.4}$$

Thus, an irredundant primary decomposition of I is obtained from given primary decompositions of the $I_{\mathscr{E}}^{(d)}$ by deleting redundant components. Equation (6.4) holds, in particular, if for some primary decomposition $I = \bigcap Q_j$ we have $x_i \in \sqrt{Q_j}$ if and only if $x_i^{d_i} \in Q_j$ for all i and j.

We say that the binomial ideals in (6.3) form a *cellular decomposition* of I.

Proof.   The $I_{\mathscr{E}}^{(d)}$ are binomial by Corollary 1.7. They are obviously cellular. The primes associated to $I_{\mathscr{E}}^{(d)}$ contain the variable x_i if and only if $i \in \mathscr{E}$, and this shows that the sets of associated primes $\text{Ass}(I_{\mathscr{E}}^{(d)})$ are pairwise disjoint.

We next show that if the d_i are chosen to have the property specified with respect to a primary decomposition $I = \bigcap Q_j$, then I is the intersection of the ideals $I_{\mathscr{E}}^{(d)}$. Our assertion about primary decomposition follows at once from this. Since I is obviously contained in the intersection of the $I_{\mathscr{E}}^{(d)}$, it suffices to prove that for each $f \in S \backslash I$, there exists an index set $\mathscr{E} \subseteq \{1, \ldots, n\}$ such that $f \notin I_{\mathscr{E}}^{(d)}$.

Let $m = x_{i_1} x_{i_2} \cdots x_{i_r}$ be a maximal product of variables such that $f \notin (I : m^{\infty})$, and define $\mathscr{E} := \{i_1, \ldots, i_r\}$. We have $(I : m^{\infty}) = \bigcap (Q_j : m^{\infty})$. Thus, there exists a primary component Q_s with $f \notin (Q_s : m^{\infty})$. It follows that $(Q_s : m^{\infty}) \neq S$; hence, $(Q_s : m^{\infty}) = Q_s$ and $f \notin Q_s$.

By the maximality in our choice of m, each variable x_j with $j \notin \mathscr{E}$ has a power throwing f into $(I : m^{\infty})$ and hence throwing f into $(Q_s : m^{\infty}) = Q_s$. We see that the variables x_j, $j \notin \mathscr{E}$, are zero divisors modulo Q_s, and hence, they are nilpotent modulo Q_s. This implies $x_j^{d_j} \in Q_s$ for $j \notin \mathscr{E}$. This proves that

$$Q_s = (Q_s : m^{\infty}) = \left((Q_s + (\{x_j^{d_j}\}_{j \notin \mathscr{E}})) : \left(\prod_{j \in \mathscr{E}} x_j \right)^{\infty} \right).$$

This ideal contains $I_{\mathscr{E}}^{(d)}$, as can be seen from (6.3), and therefore $f \notin I_{\mathscr{E}}^{(d)}$.   □

Problem 6.3.   It would be nice to have a criterion for when the d_i are large enough for (6.4) that does not require the knowledge of a primary decomposition $I = \bigcap Q_j$. Perhaps such a criterion can be found using the methods in the proof of the effective Nullstellensatz given by Kollár [Kol]. We remark that the conditions $(I : x_i^{d_i}) = (I : x_i^{\infty})$ are not sufficient. For instance, let $I := (x_1 x_4^2 - x_2 x_5^2, x_1^3 x_3^3 - x_2^4 x_4^2, x_2 x_4^8 - x_3^3 x_5^6)$ and $d = (2, 2, 0, 4, 5)$. Then $(I : x_i^{d_i}) = (I : x_i^{\infty})$ for all i, but I is properly contained in $\bigcap_{\mathscr{E}} I_{\mathscr{E}}^{(d)}$. (There are only two cellular components in this example: $\mathscr{E} = \{1, 2, 3, 4, 5\}$ and $\mathscr{E} = \{3\}$.)

The main results of this section are the following theorem and its corollary, which say that in certain cases the localization of a cellular binomial ideal is binomial. If I, J are ideals of S, then we define $I_{(J)}$ to be the intersection of all those primary components of I that are contained in some minimal prime of J. (The notation is motivated by the fact that if J is prime, then $I_{(J)} = S \cap IS_J$, where S_J is the usual localization.)

THEOREM 6.4.   *If I and J are binomial ideals in $S = k[x_1, \ldots, x_n]$ that are cellular with respect to the same index set $\mathscr{E} \subseteq \{1, 2, \ldots, n\}$, then the ideal $I_{(J)}$ is binomial.*

Proof. We may harmlessly replace J by its radical and thus assume that $J = M(\mathscr{E}) + I_+(\sigma)$ for some partial character σ on $\mathbf{Z}^{\mathscr{E}}$. By Corollary 1.2, we may assume that k is algebraically closed. Further, by Noetherian induction, we may suppose that the result is true for any binomial ideal strictly containing I.

If all the associated primes of I are contained in a minimal prime of J, then $I = I_{(J)}$, and we are done. Or else, let $P = M(\mathscr{E}) + I_+(\rho)$ be a prime associated to I that is not contained in any minimal prime of J. We consider the following sublattice of $\mathbf{Z}^{\mathscr{E}}$,

$$L := \{m \in L_\sigma \cap L_\rho : \sigma(m) = \rho(m)\}, \tag{6.5}$$

and we distinguish two cases.

Case 1. L has finite index in L_ρ. Since $L \subseteq L_\sigma$, we see in this case that $L_\rho \subseteq \mathrm{Sat}(L_\sigma)$. We first claim that $L \neq L_\rho \cap L_\sigma$. In the contrary case, we could define a partial character τ on $L_\rho + L_\sigma$ by the formula $\tau(m + \tilde{m}) = \rho(m) + \sigma(\tilde{m})$ for $m \in L_\rho$ and $\tilde{m} \in L_\sigma$. Since k^* is a divisible group, one of the saturations σ' of σ would extend τ, and thus $I_+(\rho)$ would be contained in the minimal prime $I_+(\sigma')$ of $I_+(\sigma)$, contradicting our hypothesis and establishing the claim. It follows that we may choose an element $m \in L_\rho \cap L_\sigma$ that is not in L, so that $\sigma(m) \neq \rho(m)$. The binomial $b := x^{m_+} - \sigma(m)x^{m_-}$ is in J but not in P.

Since the index of L in L_ρ is finite, there is a root of unity ζ such that $\rho(m) = \zeta\sigma(m)$. If d is a sufficiently divisible integer, and q is the largest power of the characteristic of k that divides d (or $q = 1$ if $\mathrm{char}(k) = 0$), then the ratio of quasi-powers $g = b^{[d]}/b^{[q]}$ lies in P, but not in any minimal prime of J. By Theorem 5.2(c), the ideal $I' := (I : g)$ is binomial. It is larger than I because $g \in P \in \mathrm{Ass}(S/I)$. On the other hand, $I'_{(J)} = I_{(J)}$ because g is not in any minimal prime of J, so we are done by Noetherian induction.

Case 2. L does not have finite index in L_ρ. We may choose an element $m \in L_\rho$ whose image in L_ρ/L has infinite order. Set $b = x^{m_+} - \rho(m)x^{m_-}$. For any integer $d > 0$, the quasi-power $b^{[d]}$ is in P but not in any minimal prime of J. By Theorem 5.2(b), the ideal $I' := (I : b^{[d]})$ is binomial for suitably divisible d. Again, this quotient is strictly larger than I but $I'_{(J)} = I_{(J)}$, so again we are done by Noetherian induction. $\square$

As a corollary, we deduce that the minimal primary components of a binomial ideal are all binomial. Following Eisenbud-Huneke-Vasconcelos [EHV], we write Hull(I) for the intersection of the minimal primary components of an ideal I. Note that Hull(I) = $I_{(\sqrt{I})}$.

COROLLARY 6.5. *If $I \subset S$ is a binomial ideal and P is a minimal prime of I, then the P-primary component of I is binomial. If I is a cellular binomial ideal, then Hull(I) is also binomial.*

Proof. By Theorem 6.2, we may assume that I is cellular for the first statement, as well. For the first statement, take $J = P$ in Theorem 6.4. For the second statement, take $J = \sqrt{I}$ in Theorem 6.4. $\square$

Problem 6.6. Is Hull(I) binomial for every (not necessarily cellular) binomial ideal I?

7. Primary decomposition into binomial ideals

THEOREM 7.1. *Let k be an algebraically closed field. Any binomial ideal in the polynomial ring $S = k[x_1, \ldots, x_n]$ has a minimal primary decomposition in terms of binomial ideals.*

Our attack is a Noetherian induction based on the following elementary result.

PROPOSITION 7.2. *Let I be an ideal in a Noetherian ring S. If $g \in S$ and $(I : g) = (I : g^{\infty})$, then:*

(a) $I = (I : g) \cap (I + (g))$ and $\mathrm{Ass}(S/(I : g)) \cap \mathrm{Ass}(S/(I + (g))) = \varnothing$.

(b) *The components in a minimal primary decomposition of I may be taken to be the components in minimal primary decompositions of $(I : g)$ and $I + (g)$, after deleting the components of $I + (g)$ corresponding to primes that are not in $\mathrm{Ass}(S/I)$.*

We include a proof for the reader's convenience.

Proof. (a) We obviously have $I \subseteq (I : g) \cap (I + (g))$, and we must prove the reverse inclusion. Suppose $f \in (I : g) \cap (I + (g))$. Subtracting an element of I, we may assume that $f = sg$ for some $s \in S$. Since $f \in (I : g)$, we have $sg^2 \in I$, whence $s \in (I : g^2) \subseteq (I : g^{\infty})$, and this is $(I : g)$ by hypothesis. Thus, $f = sg \in I$, proving the equality.

From the hypothesis, we see that either $g \in I$ or g is a nonzerodivisor modulo $(I : g)$. In either case, g is not contained in any associated prime of $S/(I : g)$. On the other hand, g is contained in every associated prime of $S/(I + (g))$. This proves the disjointness of the two sets of associated primes.

(b) Putting together primary decompositions of $(I : g)$ and $I + (g)$ and using part (a), we get a (possibly nonminimal) primary decomposition $I = \bigcap Q_i$ such that each Q_i is a primary ideal and the prime ideals $P_i = \sqrt{Q_i}$ are distinct. A minimal primary decomposition of I may be obtained simply by dropping

from the intersection those Q_j such that P_j is not an associated prime of I. Since $S/(I:g)$ is isomorphic to the submodule gS/I of S/I, it follows that $\mathrm{Ass}(S/(I:g)) \subseteq \mathrm{Ass}(S/I)$, and the assertion of part (b) is a consequence. $\quad\square$

In order to use Proposition 7.2 to find a binomial primary decomposition of a binomial ideal I, we need a supply of binomials $g \in S$ such that $(I:g)$ is binomial and such that $(I:g) = (I:g^\infty)$. By Corollary 1.7, we may take g to be a large power of a monomial. The following key result guarantees a further supply.

PROPOSITION 7.3. *Let $I \subset S$ be a binomial ideal, and let $b = x^\alpha - ax^\beta$ be a binomial such that x^α is a nonzerodivisor modulo I. For sufficiently divisible positive integers d, we have*

$$(I : b^{[d]}) = (I : (b^{[d]})^\infty).$$

Proof. It suffices to show that $(I : b^{[d]}) = (I : (b^{[d]})^2)$. By Theorem 5.2(b), the quotient $(I : b^{[d]})$ is generated by monomials mod I, and this ideal is independent of d for sufficiently divisible d. Using Theorem 5.2(b) again, we see that $(I : (b^{[d]})^2) = ((I : b^{[d]}) : b^{[d]})$ is generated by monomials mod I, and it suffices to show that if $m \in (I : (b^{[d]})^2)$ is a monomial then $m \in (I : b^{[d]})$. By Proposition 1.1(b), the normal form of m mod I is a term, and we may assume that it equals m. Now $(b^{[d]})^2 m \in I$ by hypothesis, so Theorem 5.2(a) implies that $b^{[d]} x^{d\alpha} m \in I$. Since $x^{d\alpha}$ is a nonzerodivisor mod I, we see that $b^{[d]} m \in I$ as required. $\quad\square$

Although we shall not apply it here, we mention a natural consequence.

COROLLARY 7.4. *Let I be a binomial ideal in S, and let $\mathscr{E} \subseteq \{1, \dots, n\}$ be a subset such that x_i is a nonzerodivisor modulo I for each $i \in \mathscr{E}$. If σ is a partial character on $\mathbf{Z}^{\mathscr{E}}$ and σ_d is the restriction of σ to dL_σ, then for sufficiently divisible integer d we have*

$$(I : I_+(\sigma_d)) = (I : I_+(\sigma_d)^\infty).$$

Proof. The ideal $I_+(\sigma_d)$ is generated by the dth quasi-powers of all binomials in $I_+(\sigma)$, and of course a finite set $\{b_1, \dots, b_s\} \subset I_+(\sigma)$ suffices. For each i, the two monomials of b_i are nonzerodivisors mod I because they are monomials in $k[\mathscr{E}]$. By Proposition 7.3, we have $(I : b_i^{[d]}) = (I : (b_i^{[d]})^2)$. Since the quasi-powers $b_i^{[d]}$ generate $I_+(\sigma_d)$, we get

$$(I : I_+(\sigma_d)) = \bigcap_{i=1}^{s} (I : b_i^{[d]}) = \bigcap_{i=1}^{s} (I : (b_i^{[d]})^2) \supseteq (I : I_+(\sigma_d)^2).$$

The reverse inclusion is obvious. $\quad\square$

Proof of Theorem 7.1. Let I be a binomial ideal. We do Noetherian induction, assuming that every binomial ideal of S strictly larger than I admits a binomial primary decomposition.

If x_i is a variable, then for large d, the element $g = x_i^d$ satisfies the conditions of Proposition 7.2, so $I = (I : g) \cap (I + (g))$, and we may derive a binomial minimal primary decomposition of I from binomial minimal primary decompositions of the ideals $(I : g)$ and $(I + (g))$. By Corollary 1.7, $(I : g)$ is a binomial ideal, and of course the same is true for $(I + (g))$. If x_i is a zero divisor modulo I but is not nilpotent modulo I, then both $(I : g)$ and $(I + (g))$ are strictly larger than I, and we are done by induction.

Thus, we may assume that every variable is either a nonzerodivisor modulo I or is nilpotent modulo I. That is, in the terminology of Section 6, I is cellular. Let $\mathscr{E}$ be the set of variables that are nonzerodivisors modulo I, and let M be the ideal generated by the variables x_i that are nilpotent modulo I.

Let $J = I \cap k[\mathscr{E}]$. By Corollary 1.3, J is a binomial ideal. By Corollary 2.5, J has the form $I_+(\rho)$ for some partial character ρ with domain of definition L_ρ contained in the lattice of monomials in the variables $\mathscr{E}$. Any prime ideal containing I must contain a minimal prime of $I_+(\rho)$, and by Corollary 2.5 these have the form $I_+(\rho_i)$, where the ρ_i are the extensions of ρ to the saturation of L_ρ. Since M is nilpotent modulo I, the minimal prime ideals of I have the form $I_+(\rho_i) + M$.

If every associated prime ideal of I is minimal, then the (unique) primary components of I may be obtained by localizing, in the sense of Theorem 6.4, and are thus binomial. On the other hand, suppose I has an embedded prime ideal P. By Theorem 6.1, P is binomial. The ideal P contains M, and the variables x_i in $\mathscr{E}$ are nonzerodivisors modulo P, so $P = I(\sigma) + M$ for some saturated partial character σ of the lattice of monomials in $k[\mathscr{E}]$. We have $I_+(\rho) \subset I_+(\sigma)$, so σ is an extension of ρ to the lattice L_σ.

Since P is not minimal over J, the lattice L_σ contains an element α that is not in the saturation of L_ρ; equivalently, no multiple of α is in L_ρ. Thus, the quasi-powers of the binomial $b = x^{\alpha_+} - \sigma(\alpha)x^{\alpha_-}$ are all outside of I, though they are all zero divisors modulo I. If d is a sufficiently divisible integer and we set $g = b^{[d]}$, then $(I : g)$ is a binomial ideal by Theorem 5.2, and by Theorem 7.3 we have $(I : g) = (I : g^\infty)$. Applying Proposition 7.2, we reduce our problem to the binomial primary decomposition of the strictly larger ideals $(I : g)$ and $I + (g)$, and we are done by Noetherian induction. $\qquad\square$

We can make the result of Theorem 7.1 a little more explicit. The situation turns out to be quite different in characteristic zero and in characteristic $p > 0$.

To express the result, we introduce some further notation: If I is a binomial ideal in $S = k[x_1, \ldots, x_n]$, then we write $\mathscr{E}_I \subseteq \{1, \ldots, n\}$ for the set of indices i such that x_i is a nonzerodivisor modulo I, and $k[\mathscr{E}_I]$ for the polynomial subring of S generated by the variables in $\mathscr{E}_I$. We write $M(I) = (\{x_i\}_{i \notin \mathscr{E}_I})$ for the ideal generated by the other variables. If the characteristic of k is $p > 0$ and $q = p^e$ is a power of p, then we write $I^{[q]}$ for the ideal generated by the qth powers of elements of I.

THEOREM 7.1′. *Let I be a binomial ideal in $k[x_1, \ldots, x_n]$, where k is algebraically closed.*

(a) *If k has characteristic $p > 0$, then, for sufficiently large powers $q = p^e$,*

$$I = \bigcap_{P \in \mathrm{Ass}(S/I)} \mathrm{Hull}(I + P^{[q]}) \tag{7.1}$$

is a minimal primary decomposition into binomial ideals.

(b) *If k has characteristic zero, and e is a sufficiently large integer, then*

$$I = \bigcap_{P \in \mathrm{Ass}(S/I)} \mathrm{Hull}(I + M(P)^e + (P \cap k[\mathscr{E}_P])) \tag{7.2}$$

is a minimal primary decomposition into binomial ideals.

Remark. (a) Formula (7.1) does not even make sense in characteristic zero, while Formula (7.2) fails in positive characteristic. For example, if $\mathscr{E}_P = \{1, \ldots, n\}$ for all $P \in \mathrm{Ass}(S/I)$ (the Laurent case), then (7.2) states that I is the intersection of its associated primes, or, equivalently, I is radical. This is true only in characteristic zero.

(b) The proof given below of part (a) yields a simple alternative proof of Theorem 7.1 in the case of characteristic $p > 0$.

Proof of Theorem 7.1'. Let $I = \bigcap_i Q_i$ be a minimal primary decomposition of I and set $P_i = \sqrt{Q_i}$. By Theorem 6.1, each P_i is binomial.

(a) The "beginner's binomial theorem" $(x + y)^q = x^q + y^q$ shows that $P^{[q]}$ is binomial. For large e we have

$$I \subseteq \mathrm{Hull}(I + P_i^{[q]}) \subseteq \mathrm{Hull}(I + P_i^q) \subseteq Q_i$$

so

$$I \subseteq \bigcap_i \mathrm{Hull}(I + P_i^{[q]}) \subseteq \bigcap_i Q_i = I.$$

By Corollary 6.5, the terms $\mathrm{Hull}(I + P^{[q]})$ are binomial, and we are done.

(b) By Theorem 7.1, we may assume that each Q_i is binomial. By the same argument as in part (a), it suffices to show that $I + M(P_i)^e + (P_i \cap k[\mathscr{E}_{P_i}]) \subseteq Q_i$. Since P_i is nilpotent modulo Q_i, we have $M(P_i)^e \subset Q_i$ for large e, and it suffices in fact to show that $P_i' := P_i \cap k[\mathscr{E}_{P_i}] \subseteq Q_i \cap k[\mathscr{E}_{P_i}] =: Q_i'$. Since Q_i contains a power of P_i, it follows that a power of P_i' lies in Q_i'. By Corollary 1.3, Q_i' is binomial. Since the characteristic of k is zero, Q_i' is radical by Corollary 2.5, and we are done. $\qquad\square$

In spite of Theorem 7.1, there are still many open questions about the decomposition of binomial ideals.

Problem 7.5. Does every binomial ideal have an irreducible decomposition into binomial ideals? Find a combinatorial characterization of irreducible binomial ideals.

8. Other decompositions and circuit ideals. In this section we discuss some special results related to primary decomposition. We also introduce a systematic way of "approximating" binomial prime ideals.

If we are given any ideal I in S, then a prime ideal P is associated to I if and only if there exists an $f \in S$ such that $(I : f) = P$. Such a polynomial f might be called a *witness* for the prime P. In the case where I is binomial and hence P is binomial, one may ask whether there exists a binomial witness. The answer to this question is easily seen to be "no": take $P = (x - 1)$ and $I = (x^d - 1)$, where every witness, like $1 + x + \cdots + x^{d-1}$, has at least d terms; or take $P = (x_1, x_2, \ldots, x_n)$ and $I = (\{x_i^2 - x_i\}_{i=1,\ldots,n})$, the ideal of the vertices of the cube, where it is easy to show that any witness, like $\prod (x_i - 1)$, has at least 2^n terms. However, the following "witness theorem" provides a monomial witness in a restricted sense.

THEOREM 8.1. *Let I be a cellular binomial ideal in $S = k[x_1, \ldots, x_n]$, and let $\mathscr{E} = \mathscr{E}(I)$. If $P = I_+(\sigma) + M(\mathscr{E})$ is an associated prime of I, then there exists a monomial m in the variables $\{x_i\}_{i \notin \mathscr{E}}$ and a partial character τ on $\mathbf{Z}^{\mathscr{E}}$ such that σ is a saturation of τ and*

$$(I : m) \cap k[\mathscr{E}] = I_+(\tau).$$

Proof. The proof is by Noetherian induction. First, if I contains all the variables $\{x_i\}_{i \in \mathscr{E}}$, then we are in the Laurent case: $I = I_+(\tau) + M(\mathscr{E})$ for some τ, by Corollary 2.5. In this case, the assertion holds with $m = 1$. Otherwise, there exists a variable, say x_1 after relabeling, such that both the cellular ideals $(I : x_1)$ and

$$I' := \left((I + (x_1)) : \left(\prod_{i \in \mathscr{E}} x_i \right)^{\infty} \right)$$

strictly contain I.

By Noetherian induction, we may assume that Theorem 8.1 holds for $(I : x_1)$ and I'. As in the proof of Theorem 6.1, every associated prime P of I is associated to $(I : x_1)$ or to I'. If P is associated to $(I : x_1)$, then we have a presentation

$$((I : x_1) : m') \cap k[\mathscr{E}] = I_+(\tau)$$

for some monomial m'. Taking $m = x_1 m'$, the claim follows.

We may therefore assume that P is associated to I'. By the Noetherian induction again, there exists a monomial m and a partial character τ with saturation σ

such that

$$\left(\left((I + (x_1)) : \left(\prod_{i \in \mathscr{E}} x_i\right)^\infty\right) : m\right) \cap k[\mathscr{E}] = I_+(\tau). \tag{8.1}$$

We claim that this ideal equals $(I : m) \cap k[\mathscr{E}]$. Certainly, $(I : m) \cap k[\mathscr{E}]$ is contained in (8.1). Note also that (8.1) is a proper ideal.

Let f be any polynomial in (8.1). Suppose that mf has a term in $I + (x_1)$. Since the terms in f are all in $k[\mathscr{E}]$, we would have $m \in ((I + (x_1)) : (\prod_{i \in \mathscr{E}} x_i)^\infty)$, and the ideal in (8.1) would not be proper. Therefore, no term of mf is in $I + (x_1)$. Using Proposition 1.10, we conclude that $mf \in I$, as required. $\square$

Using Theorem 8.1, we get the following alternative decomposition of a binomial ideal. We conjecture that Corollary 8.2 holds in finite characteristic as well.

COROLLARY 8.2. *Let k be a field of characteristic zero, let I be a cellular binomial ideal in $S = k[x_1, \ldots, x_n]$, and let $\mathscr{E} = \mathscr{E}(I)$. Then I has the following presentation as a finite intersection of unmixed binomial ideals:*

$$I = \bigcap_{m \text{ a monomial in } \{x_i\}_{i \notin \mathscr{E}}} \mathrm{Hull}(I + ((I : m) \cap k[\mathscr{E}])). \tag{8.2}$$

Proof. The intersection given in (8.2) clearly contains I. On the other hand, if $P = I_+(\sigma) + M(\mathscr{E})$ is an associated prime of I, then by Theorem 8.1 there is a monomial m in the variables $\{x_i\}_{i \notin \mathscr{E}}$ such that $(I : m) \cap k[\mathscr{E}] = I_+(\tau)$, and σ is a saturation of τ. Thus,

$$\mathrm{Hull}(I + ((I : m) \cap k[\mathscr{E}])) = \mathrm{Hull}(I + I_+(\tau)) \subseteq \mathrm{Hull}(I + I_+(\sigma))$$

$$= \mathrm{Hull}(I + (P \cap k[\mathscr{E}]));$$

hence the intersection in Formula (8.2) is contained in the intersection in Formula (7.2). $\square$

The first step in the computation of a primary decomposition of a binomial ideal I is to find a cellular decomposition as in (6.3). In certain cases, the cellular decomposition is already a primary decomposition. We next show that this event happens when the algebraic set defined by I is irreducible and not contained in any coordinate hyperplane.

THEOREM 8.3. *Let $I \subset S$ be a binomial ideal. If $\sqrt{I}$ is prime and does not contain any of the variables, then for each subset $\mathscr{E}$ of the variables and sequence d of sufficiently large integers, the ideal $I_{\mathscr{E}}^{(d)}$ is primary. Thus, the cellular decomposition (6.3) is a (possibly nonminimal) primary decomposition of I.*

Proof. Set $P = \sqrt{I}$, and let $\mathscr{E}$ be any subset of $\{1, \dots, n\}$. We define $I_\mathscr{E}^{(d)}$ as in Formula (6.3) and $P_\mathscr{E}$ as in Formula (4.2). Clearly, $I_\mathscr{E}^{(d)} \subseteq P_\mathscr{E} \subseteq \sqrt{I_\mathscr{E}^{(d)}}$, so that $I_\mathscr{E}^{(d)}$ is a proper ideal if and only if $P_\mathscr{E}$ is a proper ideal. In this case, $P_\mathscr{E} \cap k[\mathscr{E}] = P \cap k[\mathscr{E}]$, by Lemma 4.3, and thus $P_\mathscr{E} = (P \cap k[\mathscr{E}]) + M(\mathscr{E})$. This shows that $P_\mathscr{E}$ is prime, so $P_\mathscr{E} = \sqrt{I_\mathscr{E}^{(d)}}$. We conclude that every associated prime of $I_\mathscr{E}^{(d)}$ contains $P_\mathscr{E}$.

Let Q be any associated prime of $I_\mathscr{E}^{(d)}$. By Theorem 6.1 and Corollary 2.6, we can write $Q = I_+(\sigma)S + M(\mathscr{E})$, where σ is a partial character on $\mathbf{Z}^\mathscr{E}$. By Theorem 8.1, there exists a positive integer e and a monomial $m \notin I_\mathscr{E}^{(d)}$ such that $I_+(\sigma_e)m \subset I_\mathscr{E}^{(d)}$. (Here σ_e denotes the restriction of σ to the lattice $eL_\sigma \subseteq L_\sigma$.)

Let f be any element of $I_+(\sigma_e)$. Then $fm \in I_\mathscr{E}^{(d)}$, so there exists a monomial m' in $k[\mathscr{E}]$ such that $fmm' \in I + (\{x_i^{d_i}\}_{i \notin \mathscr{E}})$. Since $mm' \notin I_\mathscr{E}^{(d)}$ and $f \in k[\mathscr{E}]$, the terms of fmm' are not in $I + (\{x_i^{d_i}\}_{i \notin \mathscr{E}})$. It follows by Proposition 1.10 that $fmm' \in I \subseteq P$. Since the prime P does not contain any monomials, it follows that $f \in P$. This shows that $I_+(\sigma_e)$ is contained in P. Since $P \cap k[\mathscr{E}]$ is contained in $I_+(\sigma)$, it follows that $I_+(\sigma) = P \cap k[\mathscr{E}]$ and consequently $Q = P_\mathscr{E}$. We conclude that $P_\mathscr{E}$ is the only associated prime of $I_\mathscr{E}$. $\qquad\square$

Example 8.4. Theorem 8.3 does not hold in general for binomial ideals I whose radical is prime but contains a variable x_i. For example, $I = (x_1^2, x_1(x_2 - x_3)) = (x_1) \cap (x_1^2, x_2 - x_3)$ has radical $(x_1, x_2 - x_3)$, but if $\mathscr{E} = \{2, 3\}$ then $I = I_\mathscr{E}^{(d)}$ is not primary.

We next determine which of the ideals $P_\mathscr{E}$ arising in the proof of Theorem 8.3 is proper. (This is somewhat weaker than saying that the corresponding cell $(k^*)^\mathscr{E}$ contains an associated point of I.) This condition is phrased in terms of combinatorial convexity. It is well known in the theory of toric varieties. Let $P = I_+(\sigma)$ be a binomial prime ideal in S such that $x_i \notin P$ for all i. Let $d = \dim(P)$. Then $\mathbf{Z}^n/L_\sigma$ is a free abelian group of rank d, and $V = (\mathbf{Z}^n/L_\sigma) \otimes_{\mathbf{Z}} \mathbf{R}$ is a d-dimensional real vector space. Let $\bar{e}_i$ denote the image in V of the ith unit vector in $\mathbf{Z}^n$. We consider the d-dimensional convex polyhedral cone

$$\mathscr{C} := \{\lambda_1 \bar{e}_1 + \lambda_2 \bar{e}_2 + \cdots + \lambda_n \bar{e}_n : \lambda_1, \lambda_2, \dots, \lambda_n \geq 0\}. \tag{8.3}$$

A subset $\mathscr{E}$ of $\{1, \dots, n\}$ is said to be a *face* of P if $\mathrm{pos}(\{\bar{e}_i : i \in \mathscr{E}\})$ is a face of $\mathscr{C}$.

PROPOSITION 8.5. *With notation as above, the ideal $P_\mathscr{E}$ is proper if and only if $\mathscr{E}$ is a face of P.*

Proof. Suppose $\mathscr{E}$ is not a face. By elementary convexity, this is equivalent to the following: the generators of $\mathscr{C}$ satisfy a linear dependency of the form $\lambda_1 \bar{e}_{i_1} + \cdots + \lambda_s \bar{e}_{i_s} = \mu_1 \bar{e}_{j_1} + \cdots + \mu_t \bar{e}_{j_t}$, where $\lambda_1, \dots, \lambda_s, \mu_1, \dots, \mu_t$ are positive integers, $\{i_1, \dots, i_s\} \subseteq \mathscr{E}$, and $\{j_1, \dots, j_t\} \nsubseteq \mathscr{E}$. The ideal P therefore contains some binomial $x_{i_1}^{\lambda_1} \cdots x_{i_s}^{\lambda_s} - c \cdot x_{j_1}^{\mu_1} \cdots x_{j_t}^{\mu_t}$, $c \in k^*$. This shows that a power of $x_{i_1}^{\lambda_1} \cdots x_{i_s}^{\lambda_s}$

lies in $P + M(\mathscr{E})$, and consequently $P_{\mathscr{E}}$ contains a unit. Conversely, let $\mathscr{E}$ be a face. Then there is no linear dependency as above, which means that every binomial in P lies in $k[\mathscr{E}]$ or in $M(\mathscr{E})$. Therefore, $P_{\mathscr{E}} = (P \cap k[\mathscr{E}]) + M(\mathscr{E})$, and this is clearly a proper ideal. $\square$

Proposition 8.5 can be rephrased as follows. If an ideal I satisfies the hypothesis of Theorem 8.3, then its associated points are in natural bijection with a subset of the faces of $\sqrt{I}$. We close this section by describing a class of binomial ideals with these properties.

Example 8.6. Circuit ideals. Let ρ be a saturated partial character on $\mathbf{Z}^n$. If $v \in \mathbf{Z}^n$, then the *support* of v is the set of basis elements of $\mathbf{Z}^n$ that appear with nonzero coefficient in the expression of v. A primitive nonzero element v of the lattice L_σ is said to be a *circuit* if the support of v is minimal with respect to inclusion. The *circuit ideal* $C(\rho)$ is the ideal generated by the binomials $x^{\alpha_+} - \rho(\alpha)x^{\alpha_-}$, where α runs over all circuits of L_σ. Clearly, $C(\rho)$ is contained in the prime ideal $I_+(\rho)$. For certain special lattices L_ρ arising in combinatorics, we have $C(\rho) = I_+(\rho)$; for instance, this is the case for lattices presented by totally unimodular matrices (see Section 4 of [Stu2]). In general, we have only the following proposition.

PROPOSITION 8.7. *With notation as above,*

$$\sqrt{C(\rho)} = I_+(\rho).$$

In particular, we see that Proposition 8.5 applies to circuit ideals. For the proof, we need to know that L is generated by circuits, which is a special case of the following.

LEMMA 8.8. *Let R be an integral domain. If $\phi: R^n \to R^d$ is an epimorphism, then the kernel of ϕ is the image of the map $\psi: \wedge_{d+1} R^n \to R^n$, $\xi \mapsto \xi \lfloor \wedge_d \phi$. The circuits in the kernel of ϕ are, up to multiplication by elements of the quotient field, precisely the nonzero images of the standard basis vectors of $\wedge_{d+1} R^n$. These images are the relations given by Cramer's rule,*

$$\psi(e_{i_0} \wedge e_{i_1} \wedge \cdots \wedge e_{i_d}) = \sum_{j=0}^{d} (-1)^j \cdot \det(\phi_{i_0, \ldots, i_{j-1}, i_{j+1}, \ldots, i_d}) \cdot e_{i_j}.$$

Proof. To prove the first statement, let U be a $d \times n$-integer matrix such that $\phi \cdot U$ is the $d \times d$-identity matrix. If $v \in \ker(\phi)$, then an elementary computation in multilinear algebra gives:

$$\psi(\wedge_d U \wedge v) = (\wedge_d U \wedge v) \lfloor \wedge_d \phi = ((\wedge_d \phi) \cdot (\wedge U)) \cdot v = v.$$

Call the relations $\psi(e_{i_0} \wedge e_{i_1} \wedge \cdots \wedge e_{i_d})$ *Cramer relations*. If a Cramer relation is

nonzero, then it is a relation among $d + 1$ elements of R^d that generate a sub-module of rank d in R^d. Any relation among these $d + 1$ images must be a multiple of the Cramer relation by an element of the quotient field. In particular, the Cramer relation is a circuit in $\ker(\phi)$.

To show conversely that every circuit in $\ker(\phi)$ is, up to multiplication by an element of the quotient field, a Cramer relation, it now suffices to prove that every circuit has support contained in a set of $d + 1$ vectors whose images gen-erate a module of rank d. For every circuit c there is a number r such that c is a relation among $r + 1$ vectors spanning a submodule of rank exactly r. (If the rank were lower, then there would be two independent relations, and thus a relation involving a subset of the terms.) Since the images of the basis vectors of R^n span a submodule of rank $d \geqslant r$, we can find $d - r$ such vectors whose images, together with the images of the vectors in the support of c, span a submodule of rank d, and we are done. $\square$

Remarks. The statements about circuits are false if R is not an integral domain: if x is a zero divisor, then the only circuits in the kernel of the map $(1, x): R^2 \to R$ are the column vector with entries $0, y$, where $xy = 0$, so the rela-tion defined by Cramer's rule is not a circuit, and the circuits do not generate all the relations. However, the Cramer relations still do generate, and this fact has been extended by Buchsbaum and Rim [BR] to a natural free resolution.

Proof of Proposition 8.7. It is easy to see that every element of L_ρ is a pos-itive rational linear combination of circuits. Therefore, the convexity argument in the proof of Proposition 8.5 applies to circuit ideals as well, and $C(\rho)_\mathscr{E}$ is a proper ideal if and only if $\mathscr{E}$ is a face of $I_+(\rho)$. Now, suppose that $\mathscr{E} \subset \{1, \ldots, n\}$ is a face. Let $\rho|_\mathscr{E}$ denote the restriction of ρ to the sublattice $L_\rho \cap \mathbf{Z}^\mathscr{E}$. By Lemma 8.8 applied to this sublattice, we have $I_+(\rho|_\mathscr{E}) = (C(\rho|_\mathscr{E}) : (\prod_{i \in \mathscr{E}} x_i)^\infty)$. Clearly, the circuits of $L_\rho \cap \mathbf{Z}^\mathscr{E}$ are just the circuits of L_ρ that have support in $\mathscr{E}$. Hence, $C(\rho|_\mathscr{E}) \subseteq C(\rho) \cap k[\mathscr{E}]$, and we conclude

$$C(\rho)_\mathscr{E} = \left((C(\rho) + M(\mathscr{E})) : \left(\prod_{i \in \mathscr{E}} x_i \right)^\infty \right) = \left(((C(\rho) \cap k[\mathscr{E}]) + M(\mathscr{E})) : \left(\prod_{i \in \mathscr{E}} x_i \right)^\infty \right)$$

$$\supseteq \left(C(\rho|_\mathscr{E}) : \left(\prod_{i \in \mathscr{E}} x_i \right)^\infty \right) + M(\mathscr{E}) = I_+(\rho|_\mathscr{E}) + M(\mathscr{Z}) = I_+(\rho)_\mathscr{E}.$$

Since the reverse inclusion is obvious, we have $C(\rho)_\mathscr{E} = I_+(\rho)_\mathscr{E}$. Our claim follows by taking the intersection over all faces $\mathscr{E}$ of $I_+(\rho)$. $\square$

Problem. It remains an interesting combinatorial problem to characterize the embedded primary components of the circuit ideal $C(\rho)$. In particular, which faces of (the polyhedral cone associated with the prime) $I_+(\rho)$ support an asso-ciated prime of $C(\rho)$? An answer to this question might be valuable for the ap-

plications of binomial ideals to integer programming and statistics mentioned in the introduction.

9. Algorithms. In this final section, we present algorithms for computing various aspects of the primary decomposition of a binomial ideal. In each case, we outline only the basic steps, and we disregard questions of efficiency. It remains an interesting problem to find best possible procedures. Our Algorithms 9.1–9.7 differ greatly from the known algorithms for general polynomial ideals, given for example by Gianni-Trager-Zacharias [GTZ] and Eisenbud-Huneke-Vasconcelos [EHV]. The older algorithms immediately leave the category of binomial ideals (in the sense that they either make changes of coordinates or use syzygy computations and Jacobian ideals). The algorithms presented below work almost entirely with binomials and thus maintain maximal sparseness. This is an important advantage because sparseness is a significant factor in the effectiveness of computations.

Algorithm 9.1. Radical
Input: A binomial ideal I in $S = k[x_1, \ldots, x_n]$.
Output: A finite set of binomials generating the radical $\sqrt{I}$ of I.
1. If $I = (0)$, output $\{0\}$. If $I = S$, output $\{1\}$.
2. Otherwise, compute $J = (I : (x_1 \cdots x_n)^\infty)$, for instance, by introducing a new variable t and eliminating t from $I + (tx_1 \cdots x_n - 1)$.
3. If $\operatorname{char}(k) = p > 0$ compute the radical of J by computing the p-saturation of its associated lattice as in Corollary 2.2. Set $J := \sqrt{J}$.
4. For $i = 1, \ldots, n$:
   4.1 Replace x_i by 0 in all generators of I.
       Let J_i be the resulting ideal in $k[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$.
   4.2 Compute $\sqrt{J_i}$ by recursively calling Algorithm 9.1.
5. Compute and output a reduced Gröbner basis for the intersection

$$J \cap (\sqrt{J_1}S + (x_1)) \cap (\sqrt{J_2}S + (x_2)) \cap \cdots \cap (\sqrt{J_n}S + (x_n)).$$

Comments. The correctness follows from the results in Sections 2 and 3, in particular Theorem 3.1 and Formula (3.1). If the characteristic of k is zero, then Step 3 is unnecessary: in this case J is already radical by Corollary 2.2. As it stands, Algorithm 9.1 requires $n!$ recursive calls. The following algorithm accomplishes the same task in 2^n iterations.
    In what follows we use the abbreviation $M := M(\mathscr{E}) = (\{x_i\}_{i \notin \mathscr{E}})$.

Algorithm 9.2. Minimal primes
Input: A binomial ideal I in $S = k[x_1, \ldots, x_n]$.
Output: Binomial prime ideals $P_1, \ldots, P_s$ whose intersection is irredundant and equals $\sqrt{I}$.
  • For each subset $\mathscr{E}$ of $\{1, \ldots, n\}$:

1. Decide whether the ideal

$$I_{\mathscr{E}} := \left((I + M(\mathscr{E})) : \left(\prod_{i \in \mathscr{E}} x_i \right)^{\infty} \right)$$

is proper. If not, stop here. Otherwise continue.

2. Determine the unique partial character ρ on $\mathbf{Z}^{\mathscr{E}}$ such that $I_{\mathscr{E}} = I_+(\rho) + M(\mathscr{E})$.

3. If $\mathrm{char}(k) = p$, then replace ρ by the unique extension ρ' of ρ to the p-saturation of L_{ρ} as in Corollary 2.2.

4. Compute the saturations $\rho_1, \ldots, \rho_g$ of ρ, and save the g primes $I_+(\rho_i) + M(\mathscr{E})$.

• Among all prime ideals computed, remove the redundant ones and output the others.

Comments. The correctness of Algorithm 9.2 follows from Theorem 6.1 and the results in Section 4. In the worst case, each of the 2^n subsets $\mathscr{E}$ will contribute a minimal prime: this happens for $(\{x_i^2 - x_i, i = 1, \ldots, n\})$ as in Example 4.5. On the other hand, for many binomial ideals we can avoid having to inspect all 2^n cells. One natural shortcut arises if (in the course of the algorithm) we find that $I_{\mathscr{E}_1} = S$ and $I_{\mathscr{E}_2} \neq S$ for $\mathscr{E}_1 \subset \mathscr{E}_2$. Then we may ignore all subsets $\mathscr{E}$ with $\mathscr{E} \cap \mathscr{E}_2 = \mathscr{E}_1$: for such $\mathscr{E}$ the ideal $I_{\mathscr{E}}$ cannot be proper by Theorem 4.1(ii). Also Proposition 8.5 allows some savings: if I is a cellular radical ideal, then one may precompute the faces of the cone $\mathscr{C}$ in Formula (8.3) using some convex hull algorithm. The same techniques can be used to speed up the next algorithm. The correctness of Algorithm 9.3 is essentially the content of Theorem 6.2.

Algorithm 9.3. Cellular decomposition
Input: A binomial ideal I in $S = k[x_1, \ldots, x_n]$.
Output: Cellular ideals $J_{\mathscr{E}}$, indexed by a set of subsets of $\{1, \ldots, n\}$, such that $\bigcap_{\mathscr{E}} J_{\mathscr{E}} = I$.

1. Fix a vector $d = (d_1, \ldots, d_n)$ of sufficiently large integers (see Problem 6.3).

2. For each $\mathscr{E} \subseteq \{1, \ldots, n\}$, let $J_{\mathscr{E}} := I_{\mathscr{E}}^{(d)}$ as defined in Formula (6.3).

3. Output those proper ideals $J_{\mathscr{E}}$ which are minimal with respect to inclusion.

In the remaining four algorithms, we shall restrict ourselves to ideals which are cellular (i.e., $I = I_{\mathscr{E}}^{(d)}$ for $d_i \gg 0$). For general ideals, this requires to run Algorithm 9.3 beforehand.

Algorithm 9.4. Test for primary ideals
Input: A subset $\mathscr{E} \subset \{1, \ldots, n\}$ and a binomial ideal I which is cellular with respect to $\mathscr{E}$.
Output: The radical of I, and the decision ("YES", "NO") whether I is primary. In the negative case, the algorithm generates two distinct associated prime ideals of I.

1. Compute the unique partial character σ on $\mathbf{Z}^{\mathscr{E}}$ such that $I \cap k[\mathscr{E}] = I_+(\sigma)$.

If the characteristic is $p > 0$, replace σ by its p-saturation. Output: "The radical of I equals $I_+(\sigma) + M$."

2. If σ is not saturated, then output "NO, the radical of I is not prime," choose two distinct saturations σ_i and σ_j of σ, output the two associated primes $I_+(\sigma_i) + M$ and $I_+(\sigma_j) + M$, and STOP.

3. Compute a Gröbner basis of I, and let $\mathcal{T}$ be the set of *maximally standard* monomials in the variables $\{x_i\}_{i \notin \mathcal{E}}$. In other words, $\mathcal{T}$ is equal to the set of monomials in $(\text{in}(I) : M) \backslash (\text{in}(I) + (x_j, j \in \mathcal{E}))$.

4. If $(I : m) \cap k[\mathcal{E}] \subseteq I_+(\sigma)$ for all $m \in \mathcal{T}$, then output "YES, I is primary."

5. Otherwise, choose $m \in \mathcal{T}$ such that $(I : m) \cap k[\mathcal{E}] = I_+(\rho) \nsubseteq I_+(\sigma)$. Let ρ' be any saturation of ρ. Output: "NO, I is not primary. The primes $I_+(\sigma) + M$ and $I_+(\rho') + M$ are both associated to I."

Comments. In light of Theorem 8.1, every associated prime of I is associated to $((I : m) \cap k[\mathcal{E}]) + M$ for some monomial m in the variables $\{x_i\}_{i \notin \mathcal{E}}$. The maximal proper ideals of the form $(I : m)$ are gotten from monomials m in the finite set $\mathcal{T}$ constructed in Step 3. In Step 5, the ideal $I_+(\rho)$ properly contains the prime ideal $I_+(\sigma)$. Therefore, $I_+(\sigma)$ is properly contained in any associated prime $I_+(\rho')$ of $I_+(\rho)$.

Algorithm 9.5. Associated primes
Input: A subset $\mathcal{E} \subset \{1, \ldots, n\}$ and a binomial ideal I which is cellular with respect to $\mathcal{E}$.
Output: The list of associated primes $P_1, \ldots, P_s$ of I.
1. Compute a Gröbner basis of I.
2. Let $\mathcal{U}$ be the set of standard monomials in the variables $\{x_i\}_{i \notin \mathcal{E}}$.
3. For each $m \in \mathcal{U}$:
    3.1. Compute the partial character τ that satisfies $I_+(\tau) = (I : m) \cap k[\mathcal{E}]$.
    3.2. For each saturation τ' of τ, output the prime ideal $I_+(\tau') + M$.

Comments. The standard monomials in Step 2 are those not contained in the initial ideal of I. The primes $I_+(\tau') + M$ are associated to $I_+(\tau) + M$. It follows that $I_+(\tau') + M$ is associated to I. Theorem 8.1 shows that every associated prime of I occurs in this way. The set $\mathcal{U}$ is finite because a power of $M = (x_i, i \notin \mathcal{E})$ lies in I. Note that the set $\mathcal{T}$ in Step 3 of Algorithm 9.4 consists precisely of the maximal (with respect to divisibility) monomials in $\mathcal{U}$.

Algorithm 9.6. Minimal primary component
Input: A cellular binomial ideal I whose radical $\sqrt{I}$ is prime.
Output: A set of binomial generators for the primary ideal $\text{Hull}(I) = I_{(\sqrt{I})}$.
0. Set $J = \sqrt{I}$ and let σ be the saturated partial character such that $J = I_+(\sigma) + M$.

1. Call Algorithm 9.4 to determine whether I is primary. If yes, output I and STOP. If no, we get another associated prime $P = I_+(\rho) + M$ properly containing J.

2. We shall now follow the proof of Theorem 6.4 verbatim. First, compute the lattice L in Formula (6.5).

3. If L has finite index in L_ρ, then proceed as in Case 1 of the proof of Theorem 6.4:

    3.1 Compute a binomial $b \in P \setminus J$.

    3.2 Select an integer d which might be sufficiently divisible.

    3.3 Let q be the largest power of char(k) that divides d and set $g := b^{[d]}/b^{[q]}$.

    3.4 Compute a reduced Gröbner basis $\mathscr{G}$ for the ideal $(I : g)$.

    3.5 If $\mathscr{G}$ consists of binomials, call Algorithm 9.6 recursively with input $\mathscr{G}$. Otherwise, return to Step 3.2 and try a multiple of d.

4. If L has infinite index in L_ρ then proceed as in Case 2 of the proof of Theorem 6.4:

    4.1 Compute a vector $m \in L_\rho$ whose image in the quotient lattice L_ρ/L has infinite order. Set $b := x^{m_+} - \rho(\sigma)x^{m_-}$.

    4.2 Select an integer d which might be sufficiently divisible.

    4.3 Compute a reduced Gröbner basis $\mathscr{G}$ for the ideal $(I : b^{[d]})$.

    4.5 If $\mathscr{G}$ consists of binomials, call Algorithm 9.6 recursively with input $\mathscr{G}$. Otherwise, return to Step 4.2 and try a multiple of d.

Comments. The correctness of Algorithm 9.6 follows from Theorem 6.4.

Algorithm 9.7.   Primary decomposition
Input: A cellular binomial ideal I.
Output: Primary binomial ideals Q_i whose intersection is irredundant and equals I.

1. Compute the associated primes $P_1, \ldots, P_s$ using Algorithm 9.5.

2. Choose a sufficiently large integer e.

3. For each prime P_i:

    3.1 If char$(k) = p > 0$, then let $R_i := I + P_i^{[p^e]}$.

    3.2 If char$(k) = 0$, then let $R_i := I + M^e + (P_i \cap k[\mathscr{E}])$.

    3.3 Compute Hull(R_i) using Algorithm 9.6. Output $Q_i = $ Hull(R_i).

Comments. The correctness of this algorithm follows from Theorem 7.1′. When computing with concrete binomial ideals, it makes sense to replace M^e in Step 3.2 by $(x_i^{e_i}, i \notin \mathscr{E})$ for sufficiently large integers e_i. Good choices of these integers, and many other algorithmic details, will require further theoretical study and experimentation.

Examples 9.8. Here are a few examples of binomial primary decompositions.

(a) The ideal $I = (ab - cd, a^2, b^2, c^2, ac, bc)$ is primary but $I + (a)$ is not primary.

(b) The ideal $I = (x^3 - y^3, x^4y^5 - x^5y^4)$ has the following two primary decompositions:

$$I = (x - y) \cap (I + (x^9, y^9)) = (x - y) \cap (x^2 + xy + y^2, x^4y^5 - x^5y^4, x^{10}, y^{10}).$$

It can be shown that each primary decomposition of I in which the embedded component has a quadratic generator is *not* binomial. This proves that binomial

ideals behave differently from monomial ideals with regard to the following result of Bayer, Galligo and Stillman: Every monomial ideal has a unique "maximal primary decomposition" in which each component is a monomial ideal (see Eisenbud [E, Exercise 3.11]).

(c) The homogeneous ideal $I = (c^5 - b^2 d^3,\ a^5 d^2 - b^7,\ b^5 - a^3 c^2,\ a^2 d^5 - c^7)$ is a circuit ideal (cf. Example 8.6). Its radical is the prime $P = I + (ab - cd)$. The projective toric variety defined by P is the rational normal curve of degree 7. The polyhedral cone $\mathscr{C}$ in Formula (8.3) has dimension $\dim(P) = 2$. The faces of P are $\{a, b, c, d\}$, $\{a\}$, $\{d\}$ and $\varnothing$. The cellular decomposition has one component for each face:

$$I = P \cap (b^2 c^2 - a^2 d^2,\ b^5 - a^3 c^2, b^2 d^2,\ c^4,\ c^2 d^2,\ d^4)$$

$$\cap\ (b^2 c^2 - a^2 d^2,\ c^5 - b^2 d^3,\ a^2 c^2,\ b^4,\ a^2 b^2,\ a^4) \cap (I + (a^7,\ b^9,\ c^9,\ d^7)).$$

This intersection is a primary decomposition of I, as predicted by Theorem 8.3.

(d) The following radical binomial ideal appears in Eisenbud-Sturmfels [ES, Example 2.9]:

$$J = (x_2 x_5 - x_1 x_6, x_3, x_4) \cap (x_1 x_4 - x_3 x_5, x_2, x_6) \cap (x_3 x_6 - x_2 x_4, x_1, x_5)$$

to show that the Noether complexity of an ideal can be lower than that of any initial ideal. Note that $J = I(\Delta)$ for a polyhedral complex Δ consisting of three quadrangles (cf. Example 4.7 and Proposition 4.8). It would be interesting to study the Noether complexity of binomial ideals in general.

(e) The following binomial ideal appears in Kollár [Kol, Example 2.3]:

$$(x_1^{d_1},\ x_1 x_n^{d_2 - 1} - x_2^{d_2},\ x_2 x_n^{d_2 - 1} - x_3^{d_3}, \ldots, x_{n-2} x_n^{d_{n-1} - 1} - x_{n-1}^{d_{n-1}},\ x_{n-1} x_n^{d_n - 1} - x_0^{d_n}).$$

This ideal has radical $(x_0, x_1, \ldots, x_{n-1})$ and it is primary. This ideal provides a lower bound for the effective Nullstellensatz because it contains $x_0^{d_1 \cdots d_n}$ but not $x_0^{d_1 \cdots d_n - 1}$.

REFERENCES

[A]   V. I. ARNOLD, *A-graded algebras and continued fractions*, Comm. Pure Appl. Math. **42** (1989), 993–1000.

[BS]   D. BAYER AND M. STILLMAN, *On the complexity of computing syzygies*, J. Symbolic Comput. **6** (1988), 135–147.

[BGN]   E. BECKER, R. GROBE, AND M. NIERMANN, *Real zeros and real radicals of binomial ideals*, manuscript, 1996.

[Br]   W. D. BROWNAWELL, *Bounds for the degrees in the Nullstellensatz*, Ann. of Math. (2) **126** (1987), 577–591.

[Bu]   B. BUCHBERGER, "Gröbner bases: an algorithmic method in polynomial ideal theory" in *Multidimensional Systems Theory*, Math. Appl. **16**, D. Reidel, Dordrecht, 1985.

[BE]   D. BUCHSBAUM AND D. EISENBUD, *Generic free resolutions and a family of generically perfect ideals*, Adv. Math. **18** (1975), 245–301.

[BR]   D. BUCHSBAUM AND D. S. RIM, *A generalized Koszul complex, II, depth and multiplicity*, Trans. Amer. Math. Soc. **111** (1964), 197–224.

[CT]   P. CONTI AND C. TRAVERSO, "Buchberger algorithm and integer programming" in *Applied Algebra, Algebraic Algorithms, and Error-Protecting Codes*, Lect. Notes in Comput Sci. **539**, Springer-Verlag, New York, 1991, 130–139.

[CLO]   D. COX, J. LITTLE, AND D. O'SHEA, *Ideals, Varieties, and Algorithms*, Undergrad. Texts Math., Springer-Verlag, New York, 1992.

[DMS]   W. DECKER, N. MANOLACHE, AND F. SCHREYER, "Geometry of the Horrocks bundle on $\mathbf{P}^5$" in *Complex Projective Geometry (Trieste, 1989/Bergen, 1989)*, London Math. Soc. Lecture Note Ser. **179**, Cambridge Univ. Press, Cambridge, 1992, 128–148.

[DS]   P. DIACONIS AND B. STURMFELS, *Algebraic algorithms for generating from conditional distributions*, to appear in Ann. Statist.

[E]   D. EISENBUD, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Math., Springer-Verlag, New York, 1995.

[EHV]   D. EISENBUD, C. HUNEKE, AND W. VASCONCELOS, *Direct methods for primary decomposition*, Invent. Math. **110** (1992), 207–235.

[ES]   D. EISENBUD AND B. STURMFELS, *Finding sparse systems of parameters*, J. Pure Appl. Algebra **94** (1994), 143–157.

[F]   W. FULTON, *Introduction to Toric Varieties*, Ann. of Math. Stud. **131**, Princeton Univ. Press, Princeton, 1993.

[GTZ]   P. GIANNI, B. TRAGER, AND G. ZACHARIAS, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symbolic Comput. **6** (1988), 149–167.

[Gi]   R. GILMER, *Commutative Semigroup Rings*, Chicago Lectures in Math., Univ. of Chicago Press, Chicago, 1984.

[H]   I. HOVEIJN, *Aspects of resonance in dynamical systems*, Ph.D. thesis, University of Utrecht, Netherlands, 1992.

[Kol]   J. KOLLÁR, *Sharp effective Nullstellensatz*, J. Amer. Math. Soc. **1** (1988), 963–975.

[Kor]   E. KORKINA, *Classification of A-graded algebras with 3 generators*, Indag. Math. (N.S.) **3** (1992), 27–40.

[KPR]   E. KORKINA, G. POST, AND M. ROELOFS, *Algèbres graduées de type A*, C.R. Acad. Sci. Paris Ser. I Math. **314** (1992), 653–655.

[L]   S. LANG, *Algebra*, Addison-Wesley, Reading, Mass., 1965.

[MM]   E. MAYR AND A. MEYER, *The complexity of the word problems for commutative semigroups and polynomial ideals*, Adv. Math. **46** (1982), 305–329.

[RS]   L. ROBBIANO AND M. SWEEDLER, "Subalgebra bases" in *Commutative Algebra*, Lecture Notes in Math. **1430**, Springer-Verlag, Berlin, 1990, 61–87.

[Sta]   R. STANLEY, "Generalized *H*-vectors, intersection cohomology of toric varieties, and related results" in *Commutative Algebra and Combinatorics*, Adv. Stud. Pure Math. **11**, North-Holland, Amsterdam, 1987, 187–213.

[Stu1]   B. STURMFELS, *Gröbner bases of toric varieties*, Tôhoku Math. J. **43** (1991), 249–261.

[Stu2]   ———, *Asymptotic analysis of toric ideals*, Mem. Fac. Sci. Kyushu Univ. Ser. A **46** (1992), 217–228.

[T]   R. THOMAS, *A geometric Buchberger algorithm for integer programming*, to appear in Math. Oper. Res.

[X]   S. XAMBO, *On projective varieties of minimal degree*, Collect. Math. **32** (1981), 149–163.

[Y]   C. K. YAP, *A new lower bound construction for commutative Thue systems with applications*, J. Symbolic Comput. **12** (1991), 1–27.

EISENBUD: DEPARTMENT OF MATHEMATICS, BRANDEIS UNIVERSITY, WALTHAM, MASSACHUSETTS 02254, USA; eisenbud@math.brandeis.edu

STURMFELS: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720, USA; bernd@math.berkeley.edu