Primary Decompositions

with Sections on Macaulay2 and Networks

Irena Swanson and Eduardo Sáenz-de-Cabezón

Abstract This chapter contains three major sections, each one roughly corresponding to a lecture. The first section is on computing primary decompositions, the second one is more specifically on binomial ideals, and the last one is on some primary decomposition questions in algebraic statistics and networks.

1 Computation of Primary Decompositions

In a polynomial ring in one variable, say $R = \mathbb{Q}[x]$, it is easy to compute the primary decomposition say of $(x^4 - 1)$:

$$(x^4 - 1) = (x^2 + 1) \cap (x - 1) \cap (x + 1).$$

The reason that this computation is easy is that we readily found the irreducible factors of the polynomial $x^4 - 1$. In general, finding irreducible factors is a necessary prerequisite for the computation of primary decompositions. In these notes we make the STANDING ASSUMPTION that for any field k that arises as a finite field extension of $\mathbb{Q}$ or of a finite field, and for any variable x over k, one can compute all irreducible factors of any polynomial in $k[x]$. The reader interested in more details about polynomial factorization should consult [116] or [69, p. 38].

Throughout all rings are Noetherian and commutative with identity.

I. Swanson (✉)
Reed College, 3203 SE Woodstock Blvd, Portland, OR 97202, USA
e-mail: iswanson@reed.edu

E. Sáenz-de-Cabezón
Departamento de Matemáticas y Computación, Universidad de La Rioja, c/ Madre de Dios 53, 26006 Logroño, La Rioja, Spain
e-mail: eduardo.saenz-de-cabezon@unirioja.es

A.M. Bigatti et al. (eds.), *Computations and Combinatorics in Commutative Algebra*, Lecture Notes in Mathematics 2176, DOI 10.1007/978-3-319-51319-5_2

1.1 Introduction to Primary Ideals and Primary Decompositions

Definition 1 An ideal I in a ring R is **primary** if $I \neq R$ and every zerodivisor in R/I is nilpotent.

Facts

1. *Any prime ideal is primary.*
2. *If I is a primary ideal, then $\sqrt{I} = \{r \in R : r^l \in I \text{ for some } l \in \mathbb{N}\}$ is a prime ideal. Furthermore, if $P = \sqrt{I}$, then I is also called P-***primary**.
3. *If I is P-primary, there exists a positive integer n such that $P^n \subseteq I$.*
4. *The intersection of any two P-primary ideals is P-primary.*
5. *If $\sqrt{I}$ is a prime ideal, it need not be the case that I is primary, nor is it the case that the square of a prime ideal is primary. For example, let P be the kernel of the ring homomorphism $k[X, Y, Z] \to k[t]$ taking X to t^3, Y to t^4, and Z to t^5. Then $P = (x^3 - yz, y^2 - xz, z^2 - x^2y)$ is a prime ideal, the radical of P^2 is P, $x^5 + xy^3 - 3x^2yz + z^3 \notin P^2$ by an easy degree count, $x \notin P$, but*

$$x(x^5 + xy^3 - 3x^2yz + z^3) = (x^3 - yz)^2 - (y^2 - xz)(z^2 - x^2y),$$

   which proves that P^2 is not primary.
6. *Suppose that I is an ideal such that $\sqrt{I}$ is a maximal ideal. Then I is a primary ideal. Namely, if $r \in R$ is a zerodivisor modulo I, then as R/I is Artinian with only one maximal ideal, necessarily the image of r is in this maximal ideal. But then a power of r lies in I.*
7. *Let P be a prime ideal and I a P-primary ideal. Then for any $r \in R$,*

$$I : r = \begin{cases} I, & \text{if } r \notin P \\ R, & \text{if } r \in I \\ a\ P-\text{primary ideal strictly containing } I, & \text{if } r \in P \setminus I. \end{cases}$$

   Moreover, there exists $r \in R$ such that $I : r = P$.
8. *Let $R \to S$ be a ring homomorphism, and I a primary ideal in S. Then $I \cap R$ is primary to $\sqrt{I} \cap R$.*
9. *Let U be a multiplicatively closed subset of R. There is a one-to-one correspondence between prime (resp. primary) ideals in R disjoint from U and prime (resp. primary) ideals in $U^{-1}R$ given by $I \mapsto IU^{-1}R$ for I an ideal in R, and $J \mapsto J \cap R$ for J an ideal in $U^{-1}R$.*
10. *If I is P-primary and x is a variable over R, then $IR[x]$ is $PR[x]$-primary.*

Definition 3 Let I be an ideal in a ring R. A decomposition $I = \cap_{i=1}^{s} q_i$ is a **primary decomposition** of I if $q_1, \ldots, q_s$ are primary ideals.

If in addition all $\sqrt{q_i}$ are distinct and for all i, $\cap_{j \neq i} q_j \not\subseteq q_i$, then the decomposition is called **irredundant** or **minimal**.

By Facts 2, the following is immediate:

Proposition 4 *If $I = \cap_{i=1}^{s} q_i$ is a (minimal) primary decomposition, then for any multiplicatively closed set U such that $U^{-1}I \neq U^{-1}R$,*

$$U^{-1}I = \bigcap_{q_i \cap U = \emptyset} U^{-1}q_i$$

is a minimal primary decomposition. □

Emmy Noether proved the existence of primary decompositions:

Theorem 5 *Every proper ideal I in a Noetherian ring R has a (minimal) primary decomposition.*

Proof Once existence of a primary decomposition is established, existence of a minimal one is straightforward: if the radicals of two components are identical, we replace the two components with one component, namely their intersection, and if one component contains the intersection of the others, then that one component is redundant and is omitted. So it suffices to prove the existence of any primary decomposition.

If I is primary, the decomposition consists of I only. In particular, if I is a maximal ideal, it has a primary decomposition. So assume that I is not primary. Then by definition there exist $a, b \in R$ such that $ab \in I, a \notin I$ and $b \notin \sqrt{I}$. As R is Noetherian, the chain $I \subseteq I : b \subseteq I : b^2 \subseteq \cdots$ terminates. Choose n such that $I : b^l = I : b^{l+1} = \cdots$. It is straightforward to prove that $I = (I : b^l) \cap (I + (b^l))$. By assumption $a \in (I : b^l) \setminus I$ and $b^l \in (I + (b^l)) \setminus I$. Thus both $I : b^l$ and $I + (b^l)$ properly contain I. By Noetherian induction, these two larger ideals have a primary decomposition, and the intersection of the two decompositions gives a possibly redundant primary decomposition of I. □

Observe that the proof above is rather non-constructive: how does one decide whether an ideal is primary, and even if somehow one knows that an ideal is not primary, how can one determine the elements a and b? Nevertheless, this is a crucial step in the algorithm for computing primary decompositions in polynomial rings that we present. An important point for algorithmic computing is also that the ascending chain $I \subseteq I : b \subseteq I : b^2 \subseteq \cdots$ is special: as soon as we have one equality $I : b^l = I : b^{l+1}$, then for all $m \geq l, I : b^l = I : b^m$. (General ascending chains do not have this property.)

Example 6 For monomial ideals it is straightforward to decide when they are primary: a monomial ideal I in $R = k[X_1, \ldots, X_n]$ is primary if and only if whenever a variable X_j divides some minimal monomial generator of I, then a power of X_j is contained in I. This fact at the same time makes the existence of primary decompositions of monomial ideals, as outlined in the proof of Theorem 5, constructive. Namely, it is easy to check if each factor of each minimal monomial generator has a power in I. If yes, the ideal is primary, otherwise there exists a monomial generator a with variable $b = X_j$ dividing a and $b \notin \sqrt{I}$. We then repeat the construction as in the proof of Theorem 5 to obtain two strictly larger monomial ideals, and use Noetherian induction. In particular, we apply this to $I = (x^2, xy, xz)$. With $b = y$ and $a = x$ we get that $I : y = I : y^2$ and so that

$$I = (I : y) \cap (I + (y)) = (x) \cap (x^2, y, xz).$$

Now (x) is already primary (even prime), but (x^2, y, xz) is not. We apply the proof of Theorem 5 with $b = z, a = x$ to get that $(x^2, y, xz) = ((x^2, y, xz) : z) \cap ((x^2, y, xz) + (z)) = (x, y) \cap (x^2, y, z)$, so that

$$I = (x) \cap (x, y) \cap (x^2, y, z).$$

Clearly (x, y) is redundant, so that finally we get the minimal primary decomposition

$$I = (x) \cap (x^2, y, z).$$

But this is not the only possible primary decomposition. Namely, in the last step we could have used $(x^2, y, xz) = ((x^2, y, xz) : z^2) \cap ((x^2, y, xz) + (z^2)) = (x, y) \cap (x^2, y, xz, z^2)$, to get that

$$I = (x) \cap (x, y) \cap (x^2, y, xz, z^2) = (x) \cap (x^2, y, xz, z^2),$$

which gives a different primary decomposition.

This gives an example of non-uniqueness of primary decompositions. However, certain uniqueness does hold:

Theorem 7 *If $I = q_1 \cap \cdots \cap q_s$ is a minimal primary decomposition, then $\{\sqrt{q_1}, \ldots, \sqrt{q_s}\}$ equals the set of all prime ideals of the form $I : f$ as f varies over elements of R. In particular, the set $\{\sqrt{q_1}, \ldots, \sqrt{q_s}\}$ is uniquely determined. If $\sqrt{q_i}$ is minimal (under inclusion) in this set, then q_i is uniquely determined as*

$$I_{\sqrt{q_i}} \cap R.$$

More generally, for each i, there exists $l_i \in \mathbb{N}$ such that $\sqrt{q_i}^{l_i} \subseteq q_i$. Then

$$I = \bigcap_{i=1}^{s} \left((\sqrt{q_i}^{l_i} + I)_{\sqrt{q_i}} \cap R \right)$$

is also a primary decomposition.

Proof By minimality of the primary decomposition, for each i there exists $r \in \cap_{j \neq i} q_j \setminus q_i$. Then $I : r = (q_1 : r) \cap \cdots \cap (q_s : r) = q_i : r$ is primary to $\sqrt{q_i}$, and by Facts 2, there exists $r' \in R$ such that $q_i : (rr') = (q_i : r) : r'$ equals $\sqrt{q_i}$. Conversely, suppose that $I : f$ is a prime ideal. This means that $(q_1 : f) \cap \cdots \cap (q_s : f)$ is a prime ideal, so necessarily this prime ideal equals some $q_i : f$. But by Facts 2, necessarily this prime ideal equals $\sqrt{q_i}$. This proves the first two statements of the theorem.

The third statement follows from Facts 2 and Proposition 4, and the fourth one from Facts 2. For the last statement, observe that $(\sqrt{q_i}^{l_i} + I)_{\sqrt{q_i}}$ is primary to the maximal ideal and contained in the localization of q_i, so that $(\sqrt{q_i}^{l_i} + I)_{\sqrt{q_i}} \cap R$ is $\sqrt{q_i}$-primary and contained in q_i. Since it also contains I, it follows that

$$I \subseteq \bigcap_{i=1}^{s} \left((\sqrt{q_i}^{l_i} + I)_{\sqrt{q_i}} \cap R \right) \subseteq \bigcap_{i=1}^{s} q_i = I,$$

so that equality holds throughout. □

The primes appearing in this theorem are called **associated primes**, and their set is denoted as $\mathrm{Ass}(R/I)$. When the l_i are taken to be minimal possible, the resulting primary decomposition is called **canonical** (see works by Ortiz [90], Ojeda and Piedra-Sánchez [88, 89] and Ojeda [87]).

Yao proved that the (non-unique) primary components can be mixed and matched more generally than in the last statement in the theorem:

Theorem 8 ("Mix-and-match", Yao [118]) *Let* $\{P_1, \ldots, P_s\} = \mathrm{Ass}(R/I)$*, and assume that for* $j = 1, \ldots, s$*,*

$$I = \bigcap_{i=1}^{s} q_{ji},$$

is a primary decomposition of I *with* $\sqrt{q_{ji}} = P_i$ *for all* i, j*. Then* $I = \bigcap_{i=1}^{s} q_{ii}$ *is also a primary decomposition.*

The following appeared in the proof of Theorem 5: for any element $b \in R$ and any ideal I of R, $I \subseteq I : b \subseteq I : b^2 \subseteq \cdots$. By Noetherian assumption, there exists l such that $I : b^l = I : b^{l+1}$, and hence $I = (I : b^l) \cap (I + (b^l))$. Thus straightforwardly

$$\mathrm{Ass}\left(\frac{R}{I : b^l}\right) \subseteq \mathrm{Ass}\left(\frac{R}{I}\right) \subseteq \mathrm{Ass}\left(\frac{R}{I : b^l}\right) \bigcup \mathrm{Ass}\left(\frac{R}{I + (b^l)}\right).$$

Incidentally, the stable value of $I : b^n$ is also often written as $I : b^\infty$.

It is left as an exercise that

$$\mathrm{Ass}\left(\frac{R}{I : b}\right) \subseteq \mathrm{Ass}\left(\frac{R}{I}\right) \subseteq \mathrm{Ass}\left(\frac{R}{I : b}\right) \bigcup \mathrm{Ass}\left(\frac{R}{I + (b)}\right)$$

even when $I \neq (I : b) \cap (I + (b))$. This latter fact can be very helpful for example if b is a variable, so that a primary decomposition of $I + (b)$ is essentially done in the polynomial ring in fewer variables and can thus possibly be handled by induction on the dimension of the polynomial ring.

By Noetherian induction we know all the associated primes of $I : b, I : b^l, I + (b)$ and $I + (b^l)$. By the two set inclusions displayed above, all the associated primes of $I : b$ and $I : b^l$ are associated to I. In general, not all associated primes of $I + (b)$ and $I + (b^l)$ are associated to I. Thus the two displays above generate sets of prime ideals that include all the possible associated primes of I, but with possible redundancies. The following result can help resolve the redundancies:

Proposition 9 *A prime ideal P is associated to an ideal I if and only if P is minimal over $I : (I : P^\infty)$.*

Proof Both parts are preserved under localization at P, so we may assume that the ring is local with P being the maximal ideal. Then $I : P^\infty$ is the intersection of all primary components of I that are not P-primary, so that $I : (I : P^\infty)$ is either the ring if P is not associated, and is a P-primary ideal otherwise. $\square$

We also leave as an exercise the useful fact that if I is homogeneous in a $\mathbb{Z}^d$-graded ring, then so are all of the associated primes of I, and there exists a primary decomposition of I all of whose components are homogeneous. This has to do with zerodivisors in graded rings.

1.2 Computing Radicals and Primary Decompositions

In this section we present the Gianni-Trager-Zacharias algorithm [60]. We use Gröbner bases and induction on the number of variables. By the STANDING ASSUMPTION we can compute radicals and primary decompositions in $k[X_1, \ldots, X_n]$ if $n \le 1$. Now suppose that $n > 1$.

Alternate algorithms for computing primary decompositions can be found in the paper [52] by Eisenbud et al. and in the paper [102] by Shimoyama and Yokoyama. A survey with clear exposition on algorithms and the current state of computation is in the paper [42] by Decker et al.

Reduction Step 1

Proposition 10 *Let $A = k[X_1, \ldots, X_d] \subseteq R = k[X_1, \ldots, X_n]$ where k is a field. Then for any ideal I in R, $I_{A\setminus(X_1)} \cap R$ is computable.*

Proof The proof shows how to compute it.

We impose the lexicographic order $X_n > \cdots > X_1$ on R. Any term t in R can be written as aM_t, where a is a term in A and M_t is a monomial in $k[X_{d+1}, \ldots, X_n]$. For each $f \in R$, let $\widetilde{f}$ be the sum of all those terms t in f for which $M_t = M_{\mathrm{lt} f}$. Write $\widetilde{f} = a_f X_1^{e_f} M_{\mathrm{lt} f}$ for some non-negative integer e_f and some $a_f \in A \setminus (X_1)$. We also write M_f for $M_{\mathrm{lt} f}$.

Let G be a Gröbner basis of I.

Claim If $f \in I_{A\setminus(X_1)} \cap R$ then there exist $g \in G$ and $r \in A \setminus (X_1)$ such that $r\widetilde{f} \in \widetilde{g}R$.

Proof of the claim Let $f \in I_{A\setminus(X_1)} \cap R$. Then for some $c \in A \setminus (X_1), cf \in I$, so that $\mathrm{lt}(cf)$ is a multiple of $\mathrm{lt}g$ for some $g \in G$. Write $\mathrm{lt}(cf) = aX_1^e M(\mathrm{lt}g)$ for some $a \in A \setminus (X_1), e \in \mathbb{N}$, and some monomial M in $k[X_{d+1}, \dots, X_n]$. We will prove that it is possible to find g such that $e_{cf} \geq e + e_g$. Suppose that $e_{cf} < e + e_g$. Then there exists a term in cf that is a $k[X_2, \dots, X_d]$-multiple of $X_1^{e_{cf}} M_{cf}$ and that is not cancelled in $cf - aX_1^e Mg$. Thus $cf - aX_1^e Mg$ has a term t with $M_t = M_{cf}$ and $e_t = e_{cf} < e + e_g$. Suppose that we have $a_1, \dots, a_{s-1} \in A \setminus (X_1), M_1, \dots, M_{s-1}$ monomials in $k[X_{d+1}, \dots, X_n]$, and non-negative integers $e_1, \dots, e_{s-1}$ such that for all $j = 1, \dots, s-1, \mathrm{lt}(cf - \sum_{i=1}^{j-1} a_i X_1^{e_i} M_i g_i) = \mathrm{lt}(a_j X_1^{e_j} M_j g_j)$, and $e_{cf} < e_{g_j} + e_j$. Set $h = cf - \sum_{i=1}^{s-1} a_i X_1^{e_i} M_i g_i$. By the last conditions, $M_h = M_{cf} = M_j M_{g_j}$ for all j. As h is in I, we have that the initial term of h is $a_s X_1^{e_s} M_s(\mathrm{lt}g_s)$ for some $g_s \in G, a_s \in A \setminus (X_1), e_s \in \mathbb{N}$, and some monomial M_s in $k[X_{d+1}, \dots, X_n]$. Since the monomial ordering is a well-ordering, this cannot go on forever, so that for some $g \in G, e_{cf} \geq e_g + e$. But then $a_g\widetilde{cf} = a_g\widetilde{cf} = a_f X_1^{e_{cf}-e_g} M\widetilde{g}$. This proves the claim.

Set $b = \prod_{g\in G} a_g$. Certainly $I_b \cap R \subseteq I_{A\setminus(X_1)} \cap R$. Now let $f \in I_{A\setminus(X_1)} \cap R$. To prove that $f \in I_b \cap R$, it suffices to assume that among all f in $(I_{A\setminus(X_1)} \cap R) \setminus I_b$, the term M_f is smallest. By the claim, there exist $g \in G, r \in A \setminus (X_1)$ and $h \in R$ such that $\widetilde{rf} = h\widetilde{g} = ha_g X_1^{e_g} M_g$. Let $u = \gcd(r, h)$. Then $\widetilde{\frac{r}{u}f} = \frac{h}{u} a_g X_1^{e_g} M_g$. Since R is a UFD, necessarily $\frac{r}{u} \in A \setminus (X_1)$ is a factor of a_g, hence of b. Write $b = v\frac{r}{u}$. Then $\widetilde{bf} = v\widetilde{\frac{r}{u}f} = v\frac{h}{u} a_g X_1^{e_g} M_g$. Set $h = bf - v\frac{h}{u}g$. By construction, $M_h < M_{bf} = M_f$. If $M_f = 1$, then $h = 0$, and in general, $h \in I_{A\setminus(p)} \cap R$. By induction on $M_h, h \in I_b \cap R$, so that $bf = h + v\frac{h}{u}g \in I_b \cap R$, whence $f \in I_b \cap R$. This proves that $I_b \cap R = I_{A\setminus(p)} \cap R$.

Finally, $I_b \cap R = I : b^\infty$ is computable because $I : b^\infty$ is the first stabilization in the inclusions $I \subseteq I : b \subseteq I : b^2 \subseteq I : b^3 \subseteq \cdots$. □

Reduction Step 2 To compute a primary decomposition, we reduce to the case where $I \cap A$ is primary for all subrings A of R generated over k by a proper subset of the variables $X_1, \dots, X_n$.

Proof Fix one such A. Let $J = I \cap A$. By induction we can compute a minimal primary decomposition $J = q_1 \cap \cdots \cap q_s$. If $s = 1$, we are done, so we suppose that $s > 1$. We want to identify i such that $\sqrt{q_i}$ is a minimal associated prime ideal. We want to accomplish this with minimal computing effort. We could certainly compute all the radical ideals and compare them, but computing radicals can be time-consuming, so the radical is not a goal in itself, we avoid its computation. Instead, we compute some colon ideals. If $q_1 : q_i \neq q_1$ for some $i > 1$, then $\sqrt{q_1}$ is definitely not a minimal prime, so we can eliminate q_1 from further pairwise tests. If instead $q_1 : q_i = q_1$ for all $i = 2, \dots, s$, then $\sqrt{q_i}$ is a minimal prime ideal. With such cloning, in finitely many steps we identify i such that $\sqrt{q_i}$ is a minimal prime ideal. Say $i = 1$.

Now we want $r \in q_2 \cap \cdots \cap q_s \setminus \sqrt{q_1}$. Certainly we can find an element $r \in q_2 \cap \cdots \cap q_s$ but avoiding q_1 as follows: one of the generators of $q_2 \cap \cdots \cap q_s$ is not in q_1, and this can be tested. By prime avoidance, it is even true that a random/generic element r of $q_2 \cap \cdots \cap q_s$ is not in $\sqrt{q_1}$. Ask the computer to give you a random element r of $q_2 \cap \cdots \cap q_s$, and then $r \notin \sqrt{q_1}$ if and only if $q_1 : r = q_1$. Thus while random generation may not reliably produce an element of $q_2 \cap \cdots \cap q_s \setminus \sqrt{q_1}$, we do have a computable method via colon of checking for this property. In practice, one would probably ask for one random r, test it, and if the test fails, ask for a new random element, and if necessary repeat a small finite number of times. A reader uncomfortable with the randomness of this procedure, should instead compute $\sqrt{q_1}$, and then test successively for a generator of $q_2 \cap \cdots \cap q_s$ to not be in $\sqrt{q_1}$.

So suppose that we have $r \in q_2 \cap \cdots \cap q_s \setminus \sqrt{q_1}$. As on page 45, there exists a positive integer l such that $I : r^l = I : r^{l+1}$. This ideal is strictly larger than I as it contains $q_1 R$. Furthermore, $I + (r^l)$ is strictly larger than I since $r \notin \sqrt{q_1}$ and hence $r \notin \sqrt{I}$. If we can obtain a primary decomposition of the strictly larger ideals $I : r^l$ and $I + (r^l)$, then we get one also for $I = (I : r^l) \cap (I + (r^l))$. Thus by replacing I by the strictly larger ideals $I : r^l$ and $I + (r^l)$, we get strictly larger intersections with A, and we continue this until the intersections are primary.

We repeat this procedure with all the possible A. While working on a new $I \cap A'$, the intersections $I \cap A$ with the old A can only get larger, but by the Noetherian property of A it can get larger only finitely many times. Since there are only finitely many possible A this procedure has to stop.

Reduction Step 2 To compute a primary decomposition, we reduce to the case where $I \cap k[X_i]$ is non-zero for all i.

Suppose that $I \cap k[X_1] = (0)$. This is a principal prime ideal, so that by Proposition 10, there is a computable non-zero $b \in k[X_1]$ such that $Ik(X_1)[X_2, \ldots, X_n] \cap R = I : b^\infty$. Let l be a (computable) positive integer such that $I : b^\infty = I : b^l$. The ideal $I + (b^l)$ has the desired property that its intersection with $k[X_1]$ is not zero. Since $I = (I : b^l) \cap (I + (b^l))$, it suffices to find a primary decomposition of $I : b^l$.

By induction on the number of variables, we can compute a minimal primary decomposition $Ik(X_1)[X_2, \ldots, X_n] = q_1 \cap \cdots \cap q_s$. If $s = 1$, then by the one-to-one correspondence between primary ideals before and after localization, $I : b^l$ is primary, and we are done. So we may assume that $s > 1$. Then as in the proof of Reduction step 1 we can compute $r \in k(X_1)[X_2, \ldots, X_n]$ that is a non-nilpotent zerodivisor modulo $Ik(X_1)[X_2, \ldots, X_n]$. We can write $r = \frac{r_1}{r_2}$ for some $r_1 \in R, r_2 \in A \setminus (X_1)$, and by ignoring the unit r_2 we may assume that $r = r_1 \in R$. Then I is the intersection of strictly larger ideals $I : r^l$ and $I + (r^l)$ in R, and we proceed by Noetherian induction on ideals in R.

We repeat this with $I \cap k[X_i]$ for all $i > 1$.

Reduction Step 3 To compute a primary decomposition, we reduce to the case where $I \cap k[X_i]$ is non-zero for all i and $I \cap A$ is primary for all subrings A of R generated over k by a proper subset of the variables $X_1, \ldots, X_n$.

For this repeat the first two reduction steps. Again by Noetherian induction in each of the finitely many rings this step terminates in finitely many steps.

Reduction Step 4 To compute the radical, we reduce to the case where $I \cap k[X_i]$ is non-zero for all i and $I \cap A$ is primary for all subrings A of R generated over k by a proper subset of the variables $X_1, \ldots, X_n$.

Note that Reduction step 1 for the computation of primary decompositions successively replaces I by strictly larger ideals $J_1, \ldots, J_s$ such that $I = J_1 \cap \cdots \cap J_s$ and such that $J_i \cap A$ is primary for all A and all i. Since $\sqrt{I} = \sqrt{J_1} \cap \cdots \cap \sqrt{J_s}$, it suffices to compute $\sqrt{J_i}$ for all i.

If $I \cap k[X_1] = (0)$, by induction on the number of variables we can compute the radical of $Ik(X_1)[X_2, \ldots, X_n]$. Let $g_1, \ldots, g_t$ be a generating set of this radical. By possibly clearing denominators, we may assume that $g_1, \ldots, g_t \in R$. Then the radical of $Ik(X_1)[X_2, \ldots X_n]$ intersected with R equals $J = (g_1, \ldots, g_t)k(X_1)[X_2, \ldots X_n] \cap R$. This is a radical ideal, and it is computable by Proposition 10. Certainly $\sqrt{I} \subseteq J$. More precisely by Proposition 10, there exists non-zero $b \in k[X_1]$ such that $(g_1, \ldots, g_t)k(X_1)[X_2, \ldots X_n] \cap R = (g_1, \ldots, g_t) : b^\infty$. Then $I : b^\infty = I : b^l$ for some l, $I = (I : b^l) \cap (I + (b^l))$, and the radical of I is $J \cap \sqrt{I + (b^l)}$, so it suffices to compute the radical of the strictly larger ideal $I + (b^l)$. So we may assume that $I \cap k[X_1] \neq (0)$, and more generally that $I \cap k[X_i] \neq (0)$ for all i.

Repetition of this and Noetherian induction bring to a successful reduction in this step.

Theorem 11 *The radical and the primary decomposition of an ideal I in R are computable.*

Proof We have reduced to the case where $I \cap k[X_1] = (f_1), \ldots, I \cap k[X_n] = (f_n)$, and $I \cap k[X_1, \ldots, X_{n-1}]$ are primary.

By our STANDING ASSUMPTION, $(p_i) = \sqrt{(f_i)}$ is computable. In characteristic zero, this computation is easier: $p_i = \frac{f_i}{\gcd(f_i, f_i')}$.

By induction on the number of variables we can compute the radical of $I \cap k[X_1, \ldots, X_{n-1}]$. Since we assumed that $I \cap k[X_1, \ldots, X_{n-1}]$ is primary, it follows that its radical is a maximal ideal; call it M. (In characteristic zero, as in [70], $M = I \cap k[X_1, \ldots, X_{n-1}] + (p_1, \ldots, p_{n-1})$ because $k[X_1, \ldots, X_{n-1}]/(p_1, \ldots, p_{n-1}) = (k[X_1]/(p_1)) \otimes_k \cdots \otimes_k (k[X_{n-1}]/(p_{n-1}))$ is a tensor product of finitely generated field extensions of k, and is thus reduced, semisimple, so that any ideal in this ring is radical.)

Since $I \cap k[X_n] \neq (0)$, necessarily I is not a subset of MR. We can compute $g \in I \setminus MR$. Even more, since $R/MR = \frac{k[X_1, \ldots, X_{n-1}]}{M}[X_n]$ is a principal ideal domain, we can compute $g \in I$ such that $g(R/MR) = I(R/MR)$. By the STANDING ASSUMPTION, there exists $g_1, \ldots, g_s \in R$ such that the $g_i(R/MR)$ are pairwise non-associated and irreducible, and such that $g(R/MR) = g_1^{a_1} \cdots g_s^{a_s}(R/MR)$ for some positive integers $a_1, \ldots, a_s$.

Then $I \subseteq \cap_i (MR + g_i R) = MR + (g_1 \cdots g_s)R \subseteq \sqrt{I}$, the associated primes of I are $MR + g_i R, i = 1, \ldots, s$, $\sqrt{I} = \cap_i (MR + g_i R)$, and the $(MR + g_i R)$-primary component of I is $I : (\prod_{j \neq i} g_j)^\infty$. All of these are computable. $\square$

Example 12 Let $I = (x^2 + yz, xz - y^2, x^2 - z^2)$ in $\mathbb{Q}[x, y, z]$. We roughly follow the outline of the algorithm, with some human ingenuity to skip computational steps. Clearly $yz + z^2 \in I \cap k[y, z]$ and it appears unlikely that a power of z is contained in $I \cap k[y,z]$. (We could use elimination and Gröbner bases to compute precisely $I \cap k[y,z] = (yz+z^2, y^3+z^3)$.) Thus z is a non-nilpotent zerodivisor modulo I. By the algorithm we compute $I : z = (y+z, xz-z^2, x^2-z^2)$, $I : z^2 = (y+z, x-z) = I : z^3$, which is clearly prime and hence primary. Furthermore, $I+(z^2) = (x^2, yz, xz-y^2, z^2)$ has radical (x,y,z), which is a maximal ideal, so that $I + (z^2)$ is primary. Thus $I = (I : z^2) \cap (I + (z^2)) = (y+z, x-z) \cap (x^2, yz, xz-y^2, z^2)$ is a primary decomposition, and clearly it is an irredundant one.

1.3 Computer Experiments: Using Macaulay2 to Obtain Primary Decompositions

The computer algebra system Macaulay2 [62] has in-built functions to deal with primary decompositions. There is a package, included with the system, that is devoted to this topic. In this section we encourage the reader to turn on the computer, start a Macaulay2 session and experiment with the software.

To see the capabilities of Macaulay2 with respect to primary decompositions, one can first read the help pages for the package. One can do this in two ways: typing `help PrimaryDecomposition` in the command line interface, or reading the html version in a browser (by typing `viewHelp` in the command line interface. We rapidly review the main functions Macaulay2 offers to compute primary decompositions.

The first thing to do is of course typing your favourite ideal and using the in-built function `primaryDecomposition`:

```
i1 : R=QQ[x,y,z];

i2 : I=ideal(x^2,x*y,x*z);

o2 : Ideal of R

i3 : primaryDecomposition I

                             2
o3 = {ideal(x), ideal  (x  , y,  z)}
```

We can immediately obtain the associated primes of `I` (in the order corresponding to the primary components):

```
i4 : associatedPrimes I

o4 = {ideal(x), ideal  (x,  y,  z)}
```

This is because when computing the primary decomposition, Macaulay2 caches the information it obtains, which can be accessed at any time, without further computations:

```
i1 : R=QQ[x,y,z];

i2 : I=ideal(x^3,x*y,x*z);

o2 : Ideal of R

i3 : peek I.cache

o3 = CacheTable{}

i4 : primaryDecomposition I

                             3
o4 = {ideal(x), ideal  (x  , y,  z)}

i6 : peek I.cache

o6 = CacheTable{AssociatedPrimes => {ideal(x), ideal  (x, y, z)}
           module => image | x3 xy xz |

           flattenRing => OptionTable{CoefficientRing => null}
                           3
           => (ideal  (x  , x*y, x*z), map(R,R,{x, y, z}))
                                  Result =>(Thing, RingMap)
```

Macaulay2 is able to use different algorithms to compute primary decompositions; they are called **strategies** in the system. They are sensitive to the input ideal:

```
i1 : R=QQ[x,y,z];

i2 : I=ideal(x^3+y+1,y^3+z+1,z^3+x+1);

o2 : Ideal of R

i3 : J=I^2;

o3 : Ideal of R

i4 : K=I^2;

o4 : Ideal of R

i5 : L=I^2;

o5 : Ideal of R

i6 : time primaryDecomposition J;
     -- used 1.27953 seconds
```

```
i7 : time primaryDecomposition (K, Strategy=>
     EisenbudHunekeVasconcelos);
     -- used 49.3968 seconds

i8 : time primaryDecomposition (L, Strategy=>
     new Hybrid from (1,2));
     -- used 41.828 seconds

i9 : peek J.cache

i10: peek K.cache

i11: peek L.cache
```

Note that the output of lines `i9`, `i10` and `i11` is too long to be printed here. We encourage the reader to check it in her/his own computer. The cached information makes a difference when obtaining further information about the ideal. The algorithms available for computing primary decompositions are Shimoyama and Yokoyama [102], Eisenbud et al. [52], a hybrid of these two algorithms, and Gianni et al. [60]. The default algorithm in Macaulay2 is Shimoyama-Yokoyama. Macaulay2 has also special strategies for monomial and binomial ideals.

2 Expanded Lectures on Binomial Ideals

In these pages I present the commutative algebra gist of the Eisenbud–Sturmfels paper [51]. The paper employs lattice and character theory, but this presentation, inspired by Melvin Hochster's, avoids that machinery.

The main results are that the associated primes, the primary components, and the radical of a binomial ideal in a polynomial ring are binomial if the base ring is algebraically closed.

Kahle wrote a program [68] that computes binomial decompositions extremely fast: the input fields do not have to be algebraically closed, but the program adds the necessary roots of numbers.

Throughout, $R = k[X_1, \dots, X_n]$, where k is a field and $X_1, \dots, X_n$ are variables over k. A **monomial** is an element of the form $\underline{X}^{\underline{a}}$ for some $a \in \mathbb{N}_0^n$, and a **term** is a scalar multiple of a monomial. The words "monomial" and "term" are often confused, and in particular, a **binomial** is defined as the difference of two terms. (In my opinion, we should switch the meanings of "monomial" and "term".) An ideal is **binomial** if it is generated by binomials.

Here are some easy facts:

1. Every monomial is a binomial, hence every monomial ideal is a binomial ideal.
2. The sum of two binomial ideals is a binomial ideal.
3. The intersection of binomial ideals need not be binomial: $(t-1) \cap (t-2) = t^2 - 3t + 2$, which is not binomial in characteristics other than 2 and 3.

4. Primary components of a binomial ideal need not be binomial: in $\mathbb{R}[t]$, the binomial ideal (t^3-1) has exactly two primary components: $(t-1)$ and (t^2+t+1).
5. The radical of a binomial ideal need not be binomial: Let t, X, Y be variables over $\mathbb{Z}/2\mathbb{Z}, k = (\mathbb{Z}/2\mathbb{Z})(t), R = k[X, Y]$, and $I = (X^2 + t, Y^2 + t + 1)$. Note that I is binomial (as $t + 1$ is in k), and $\sqrt{I} = (X^2 + t, X + Y + 1)$, and this cannot be rewritten as a binomial ideal as there is only one generator of degree 1 and it is not binomial.

Thus, for the announced good properties of binomial ideals, we do need to make a further assumption, namely, **from now on**, all fields k are algebraically closed, and then the counterexamples to primary components and radicals do not occur.

Can the theory be extended to trinomial ideals (with obvious meanings)? The question is somewhat meaningless, because **all ideals are trinomial** after adding variables and a change of variable. Namely, let $f = a_1 + a_2 + \cdots + a_m$ be a polynomial with m terms. Introduce new variables $t_3, \ldots, t_m$. Then $k[X_1, \ldots, X_n]/(f) = k[X_1, \ldots, X_n, t_3, \ldots, t_m]/(a_1 + a_2 - t_3, -t_3 + a_3 - t_4, -t_4 + a_4 - t_5, \ldots, -t_{m-2} + a_{m-2} - t_{m-1}, -t_{m-1} + a_{m-1} - t_m)$. In this way an ideal I in a polynomial ring can be rewritten for some purposes as a trinomial ideal in a strictly larger polynomial ring, so that essentially every ideal is trinomial in this sense. Then the general primary decomposition and radical properties follow-after adding more variables.

But binomial ideals are special. By Buchberger's algorithm, a Gröbner basis of a binomial ideal is binomial: all S-polynomials and all reductions of binomial ideals with respect to binomials are binomial. Thus whenever I is a binomial ideal and A is a polynomial subring generated by some of the variables of R, then $I \cap A$ is binomial. In particular, from the commutative algebra fact that $I \cap J = (tI + (t-1)J)R[t] \cap R$, where t is a variable over R, whenever I is binomial and J is monomial, then $I \cap J$ is binomial. Similarly, for any monomial $j, I \cap (j)$ and $I : j$ are binomial.

Proposition 13 *Let I be a binomial ideal, and let $J_1, \ldots, J_l$ be monomial ideals. Then there exists a monomial ideal J such that $(I + J_1) \cap \cdots \cap (I + J_l) = I + J$.*

Proof We can take a k-basis B of R/I to consist of monomials. By Gröbner bases of binomial ideals, $(I + J_k)/I$ is a subspace whose basis is a subset of B. Thus $\cap((I + J_k)/I)$ is a subspace whose basis is a subset of B, which proves the proposition. □

Binomial ideals are sensitive to the coefficients appearing in the generators. This has implications in complexity theory, as well as in practical computations. For example, if the characteristic of k is not 0 and R is a polynomial ring in $m \times n$ variables X_{ij}, the ideal generated by the 2×2-determinants of $[X_{ij}]_{i,j}$ is a prime ideal (see for example [30]), whereas the ideal generated by such permanents (both coefficients $+1$) generate a prime ideal precisely when $m = n = 2$, they generate a radical ideal precisely when $\min\{m, n\} \leq 2$, and whenever $m, n \geq 3$, the number of minimal primes is $n + m + \binom{n}{2}\binom{m}{2}$. (This is due to [73].)

2.1 Binomial Ideals in $S = k[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}] = k[X_1, \ldots, X_n]_{X_1 \cdots X_n}$

Any binomial $\underline{X}^{\underline{a}} - c\underline{X}^{\underline{b}}$ can be written up to unit in S as $\underline{X}^{\underline{a}-\underline{b}} - c$.

Let I be a proper binomial ideal in S. Write $I = (\underline{X}^{\underline{e}} - c : \underline{e} \in \mathbb{Z}^n, c_e \in k^*)$. (All c_e are non-zero since I is assumed to be proper.)

If e, e' occur in the definition of I, set $e'' = e - e', e''' = e + e'$. Then

$$\underline{X}^{\underline{e}} - c_e = \underline{X}^{\underline{e}'+\underline{e}''} - c_e \equiv c_{e'}\underline{X}^{\underline{e}''} - c_e \mod I,$$

$$\underline{X}^{\underline{e}} - c_e = \underline{X}^{\underline{e}'''-\underline{e}'} - c_e \equiv c_{e'}^{-1}\underline{X}^{\underline{e}'''} - c_e \mod I,$$

so that e'' is allowed with $c_{e''} = c_e c_{e'}^{-1}$, and e''' is allowed with $c_{e'''} = c_e c_{e'}$. In particular, the set of all allowed e forms a $\mathbb{Z}$-submodule of $\mathbb{Z}^n$. Say that it is generated by m vectors. Record these vectors into an $n \times m$ matrix A. We just performed some column reductions: neither these nor the rest of the standard column reductions over $\mathbb{Z}$ change the ideal I. But we can also perform column reductions! Namely, S also equals $k[X_1X_2^m, X_2, \ldots, X_n, (X_1X_2^m)^{-1}, (X_2)^{-1}, \ldots, (X_n)^{-1}]$, and we can rewrite any monomial $\underline{X}^{\underline{a}}$ as $(X_1X_2^m)^{a_1}X_2^{a_2-ma_1}X_3^{a_3}\cdots X_n^{a_n}$, which corresponds to the second row of the matrix becoming the old second row minus m times the old first row (and other rows remain unchanged). Simultaneously we changed the variables, but not the ring. So all row reductions are allowed, they do not change the ideal, but they do change the ideal. We work this out on an example:

Example 14 Let $I = (x^3y - 7y^3z, xy - 4z^2)$ in $k[x, y, z]$, where the characteristic of k is different from 2 and 7. This yields the 3×2 matrix of occurring exponents:

$$A = \begin{bmatrix} 3 & 1 \\ -2 & 1 \\ -1 & -2 \end{bmatrix}.$$

We will keep track of the coefficients 7 and 4 for the columns like so:

$$\begin{array}{c} A = \begin{bmatrix} 3 & 1 \\ -2 & 1 \\ -1 & -2 \end{bmatrix} \\ \quad\;\; 7 \quad 4 \end{array}$$

We first perform some elementary column reductions, keeping track of the c_e (if all c_e are 1, then there is no reason to keep track of these, they will always be 1):

$$A \to \begin{array}{c} \begin{bmatrix} 1 & 3 \\ 1 & -2 \\ -2 & -1 \end{bmatrix} \\ 7 \quad 4 \end{array} \to \begin{array}{c} \begin{bmatrix} 1 & 0 \\ 1 & -5 \\ -2 & 5 \end{bmatrix} \\ 4 \quad 7/4^3 \end{array}$$

We next perform the row reductions, and for these we will keep track of the names of variables (in the obvious way):

$$\begin{array}{c} x\\ y\\ z\end{array}\begin{bmatrix}1&0\\1&-5\\-2&5\end{bmatrix} \to \begin{array}{c}xy\\y\\z\end{array}\begin{bmatrix}1&0\\0&-5\\-2&5\end{bmatrix} \to \begin{array}{c}xyz^{-2}\\y\\z\end{array}\begin{bmatrix}1&0\\0&-5\\0&5\end{bmatrix} \to \begin{array}{c}xyz^{-2}\\y\\zy^{-1}\end{array}\begin{bmatrix}1&0\\0&0\\0&5\end{bmatrix} \to \begin{array}{c}xyz^{-2}\\zy^{-1}\\y\end{array}\begin{bmatrix}1&0\\0&5\\0&0\end{bmatrix}.$$

In these reductions, the coefficients remained 4 and $7/4^3$.

This was only a special case, but obviously the procedure works for any binomial ideal in S: the matrix A can be row- and column-reduced, keeping track of the variables and coefficients. Once we bring the matrix of exponents into standard form, every proper binomial ideal in S is of the form $((X_1)'^{m_1} - c_1, \ldots, (X_d)'^{m_d} - c_d)$ for some $d \le n$, some $m_i \in \mathbb{N}$, some $c_i \in K^*$, and some X_i' are products of positive and negative powers of $X_1, \ldots, X_n$ in a way that keeps the ring equality $S = k[X_1', \ldots, X_n', X_1'^{-1}, \ldots, X_n'^{-1}]$.

Now the following are obvious: in characteristic zero,

$$I = \bigcap_{u_i^{m_i}=c_i} (X_1' - u_1, \ldots, X_d' - u_d),$$

where all the primary components are distinct, binomial, and prime. Thus here all associated primes, all primary components, and the radical are all binomial ideals, and moreover all the associated primes have the same height and are thus all minimal over I.

In positive prime characteristic p, write each m_i as $p^{v_i} n_i$ for some positive v_i and non-negative n_i that is not a multiple of p. Then

$$I = \bigcap_{u_i^{m_i}=c_i} ((X_1' - u_1)^{p^{v_1}}, \ldots, (X_d' - u_d)^{p^{v_d}}).$$

The listed generators of each component are primary. These primary components are binomial, as $(X_i' - u_i)^{p^{v_i}} = X_i'^{p^{v_i}} - u_i^{p^{v_i}}$. The radicals of these components are all the associated primes of I, and they are clearly the binomial ideals $(X_1' - u_1, \ldots, X_d' - u_d)$. All of these prime ideals have the same height, thus they are all minimal over I. Furthermore,

$$\sqrt{I} = \bigcap_{u_i^{m_i}=c_i} (X_1' - u_1, \ldots, X_d' - u_d) = (X_1'^{n_1} - u_1^{n_1}, \ldots, X_d'^{n_d} - u_d^{n_d}),$$

for any u_i with $u_i^{m_i} = c_i$. The last equality is in fact well-defined as if $(u_i')^{m_i} = c_i$, then $0 = c_i - c_i = u_i^{m_i} - (u_i')^{m_i} = (u_i^{n_i} - (u_i')^{n_i})^{p^{v_i}}$, so that $u_i^{n_i} = (u_i')^{n_i}$. In particular, $\sqrt{I}$ is binomial.

We summarize this section in the following theorem:

Theorem 15 *A proper binomial ideal in S has binomial associated primes, binomial primary components, and binomial radical. All associated primes are minimal. In characteristic zero, all components are prime ideals, so all binomial ideals in S are radical. In positive prime characteristic p, a generating set of a primary component consists of (different) Frobenius powers of the elements in some binomial generating set of the corresponding prime ideal.* □

Example 16 In particular, if we analyze the ideal from Example 14, the already established row reduction shows that $I = (xyz^{-2} - 4, (zy^{-1})^5 - 7/4^3)$. In characteristic 5, this is a primary ideal whose radical is $I = (xyz^{-2} - 4, zy^{-1} - \sqrt[5]{7/4^3}) = (xyz^{-2} - 4, zy^{-1} - 3) = (xy - 4z^2, z - 3y) = (xy - 4 \cdot 9y^2, z - 3y) = (x - y, z - 3y)$. In characteristics other than $2, 5, 7$, we get five associated primes $(xy - 4z^2, z - \alpha y) = (x - 4\alpha^2 y, z - \alpha y)$ as α varies over the fifth roots of $7/4^3$. All of these prime ideals are also the primary components of I. (In characteristics 2 and 7, $IS = S$.)

Theorem 17 *Let I be an ideal in R such that IS is binomial. Then $IS \cap R$ is binomial. In particular, for any binomial ideal I of R, any associated prime ideal P of I such that $PS \neq S$ is binomial, and we may take the P-primary component of I (in R) to be binomial.*

Proof Let Q be a binomial ideal in R such that $QS = IS$. Then $IS \cap R = QS \cap R = Q : (X_1 \cdots X_n)^\infty$ is binomial by the facts at the beginning of this section. □

2.2 Associated Primes of Binomial Ideals Are Binomial

Theorem 18 *All associated primes of a binomial ideal are binomial ideals. (Recall that k is algebraically closed.)*

Proof By factorization in polynomial rings in one variable, the theorem holds if $n \leq 1$. So we may assume that $n \geq 2$. The theorem is clearly true if the binomial ideal I is a maximal ideal. Now let I be arbitrary.

Let $j \in [n] = \{1, \ldots, n\}$. Note that $I + (X_j) = I_j + (X_j)$ for some binomial ideal I_j in $k[X_1, \ldots, X_{n-1}]$. By induction on n, all prime ideals in $\mathrm{Ass}(k[X_1, \ldots, X_{n-1}]/I_j)$ are binomial. But $\mathrm{Ass}(R/(I + (X_j))) = \{P + (X_j) : P \in \mathrm{Ass}(k[X_1, \ldots, X_{n-1}]/I_j)\}$, so that all prime ideals in $\mathrm{Ass}(R/(I + (X_j)))$ are binomial. By the basic facts from the beginning of this section, $I : X_j$ is binomial. If X_j is a zerodivisor modulo I, then $I : X_j$ is strictly larger than I, so that by Noetherian induction, $\mathrm{Ass}(R/(I : X_j))$ contains only binomial ideals. By facts on page 45, $\mathrm{Ass}(R/I) \subseteq \mathrm{Ass}(R/(I + (X_j))) \cup \mathrm{Ass}(R/(I : X_j))$, whence also by induction on the number of variables, all associated primes of I are binomial as long as some variable is a zerodivisor modulo I.

Now assume that all variables are non-zerodivisors modulo I. Let $P \in \mathrm{Ass}(R/I)$. Since $X_1 \cdots X_n$ is a non-zerodivisor modulo I, it follows that $P_{X_1 \cdots X_n} \in \mathrm{Ass}((R/I)_{X_1 \cdots X_n}) = \mathrm{Ass}(S/IS)$. Then P is binomial by Theorem 17. □

We have already seen in Example 6 that for monomial ideals all associated primes are monomial (hence binomial).

Example 19 (Continuation of Examples 14 and 16) Let $I = (x^3y - 7y^3z, xy - 4z^2)$ in $k[x, y, z]$. We have already determined all associated prime ideals of I that do not contain any variables. So it suffices to find the associated primes of $I + (x^m), I + (y^m)$ and of $I + (z^m)$, for large m. If the characteristic of k is 2, then the decomposition is

$$I = (x^3y - y^3z, xy)I = (y^3z, xy) = (y) \cap (y^3, x) \cap (z, x),$$

If the characteristic of k is 7, then the decomposition is

$$I = (x^3y, xy - 4z^2) = (y, z^2) \cap (x^3, xy - 4z^2).$$

(The reader may apply methods of the previous section to verify that the latter ideal is primary.) Now we assume that the characteristic of k is different from 2 and 7. Any prime ideal that contains I and x also contains z, so at least we have that (x, z) is minimal over I and thus associated to I. Similarly, (y, z) is minimal over I and thus associated to I. Also, any prime ideal that contains I and z contains in addition either x or y, so that at least we have determined $\mathrm{Min}(R/I)$. Any embedded prime ideal would have to contain all of the already determined primes. Since I is homogeneous, all associated primes are homogeneous, and in particular, the only embedded prime could be (x, y, z). It turns out that this prime ideal is not associated even if it came up in our construction, but we won't get to this until we discuss the theory of primary decomposition of binomial ideals in the next section.

2.3 Primary Decomposition of Binomial Ideals

The main goal of this section is to prove that every binomial ideal has a binomial primary decomposition, if the underlying field is algebraically closed (Theorem 23). We first need a lemma and more terms.

Definition 20 An ideal I in a polynomial ring $k[X_1, \ldots, X_n]$ is **cellular** if for all $i = 1, \ldots, n, X_i$ is either a non-zerodivisor or nilpotent modulo I.

All primary monomial and binomial ideals are cellular.

Definition 21 For any binomial $g = \underline{X}^{\underline{a}} - c\underline{X}^{\underline{b}}$ and for any non-negative integer d, define

$$g^{[d]} = \underline{X}^{d\underline{a}} - c^d\underline{X}^{d\underline{b}}.$$

The following is a crucial lemma:

Lemma 22 *Let I be a binomial ideal, let $g = \underline{X}^{\underline{a}} - c\underline{X}^{\underline{b}}$ be a non-monomial binomial in R such that $\underline{X}^{\underline{a}}$ and $\underline{X}^{\underline{b}}$ are non-zerodivisors modulo I. Then there exists a monomial ideal I_0 such that for all large d, $I : g^{[d!]} = I : (g^{[d!]})^2 = I + I_0$.*

Proof For all positive integers d and e, $g^{[d]}$ is a factor of $g^{[de]}$, so that $I : g^{[d]} \subseteq I : g^{[de]}$. Thus there exists d such that for all $e \geq d$, $I : g^{[d!]} = I : g^{[e!]}$.

Let $f \in I : g^{[d!]}$. Write $f = f_1 + f_2 + \cdots + f_s$ for some terms (coefficient times monomial) $f_1 > f_2 > \cdots > f_s$. Without loss of generality $\underline{X}^{\underline{a}} > \underline{X}^{\underline{b}}$. We have that

$$f_1\underline{X}^{\underline{a}} + f_2\underline{X}^{\underline{a}} + \cdots + f_s\underline{X}^{\underline{a}} + f_1\underline{X}^{\underline{b}} + f_2\underline{X}^{\underline{b}} + \cdots + f_s\underline{X}^{\underline{b}} \in I.$$

In the Gröbner basis sense, each $f_i\underline{X}^{\underline{a}}, f_i\underline{X}^{\underline{b}}$ reduces to some unique term (coefficient times monomial) modulo I. Since $\underline{X}^{\underline{a}}$ and is a non-zerodivisor modulo I, $f_i\underline{X}^{\underline{a}}$ and $f_j\underline{X}^{\underline{a}}$ cannot reduce to a scalar multiple of the same monomial, and similarly $f_i\underline{X}^{\underline{b}}$ and $f_j\underline{X}^{\underline{b}}$ cannot reduce to a scalar multiple of the same monomial. Thus for each $j = 1, \ldots, s$ there exists $\pi(j) \in [s] = \{1, \ldots, s\}$ such that $f_j\underline{x}^{d!\underline{a}} - c^{d!}f_{\pi(j)}\underline{x}^{d!\underline{b}} \in I$. The function $\pi : [s] \to [s]$ is injective. By easy induction, for all i, $f_j(\underline{x}^{d!\underline{a}})^i - c^{d!i}f_{\pi^i(j)}(\underline{x}^{d!\underline{b}})^i \in I$. By elementary group theory, $\pi^{s!}(j) = j$, so that for all j, $f_jg^{[d!][s!]} \in I$. Then $f_jg^{[((d!)(s!))!]} \in I$, and by the choice of d, $f_jg^{[d!]} \in I$. Thus $I : g^{[d!]}$ contains monomials $f_1, \ldots, f_s$. Thus set I_0 to be the monomial ideal generated by all the monomials appearing in the generators of $I : g^{[d!]}$.

Let $f \in I : (g^{[d!]})^2$. We wish to prove that $f \in I : g^{[d!]}$. By possibly enlarging I_0 we may assume that I_0 contains all monomials in $I : g^{[d!]} = I + I_0$. This in particular means that any Gröbner basis G of $I : g^{[d!]}$ consists of monomials in I_0 and binomial non-monomials in I. Write $f = f_1 + f_2 + \cdots + f_s$ for some terms $f_1 > f_2 > \cdots > f_s$. As in the previous paragraph, for each j, either $f_j\underline{x}^{d!\underline{a}} \in I_0$ or else $f_j\underline{x}^{d!\underline{a}} - c^{d!}f_{\pi(j)}\underline{x}^{d!\underline{b}} \in I$. If $f_j\underline{x}^{d!\underline{a}} \in I_0 \subseteq I : g^{[d]}$, then by the non-zerodivisor assumption, $f_j \in I : g^{[d]}$, which contradicts the assumption. So necessarily we get the injective function $\pi : [s] \to [s]$. As in the previous paragraph we then get that each $f_j \in I : g^{[d]}$. $\square$

Without loss of generality assume that no f_i is in $I : g^{[d!]}$. Note that $fg^{[d!]} \in I : g^{[d!]}$. Consider the case that $f_j\underline{x}^{d!\underline{a}} \in I_0$ and get a contradiction. Now repeat the π argument as in a previous part to make the conclusion.

Theorem 23 *If k is algebraically closed, then any binomial ideal has a binomial primary decomposition.*

Proof Let I be a binomial ideal. For each variable X_j there exists l such that $I = (I : X_j^l) \cap (I + (X_j)^l)$, so it suffices to find the primary decompositions of the two ideals $I : X_j^l$ and $I + (X_j)^l$. These two ideals are binomial, the former by the basic facts from the beginning of this section. By repeating this splitting for another X_i on each of the two new ideals, and then repeating for X_k on the four new ideals, et cetera, with even some j repeated, we may assume that each of the intersectands is cellular.

Thus it suffices to prove that each cellular binomial ideal has a binomial primary decomposition.

So let I be cellular and binomial. By possibly reindexing, we may assume that $X_1, \dots, X_d$ are non-zerodivisors modulo I, and $X_{d+1}, \dots, X_n$ are nilpotent modulo I. Let $P \in \mathrm{Ass}(R/I)$. By Theorem 18, P is a binomial prime ideal. Since I is contained in P, P must contain $X_{d+1}, \dots, X_n$, and since the other variables are non-zerodivisors modulo I, these are the only variables in P. Thus $P = P_0 + (X_{d+1}, \dots, X_n)$, where P_0 is a binomial prime ideal whose generators are binomials in $k[X_1, \dots, X_d]$, and $X_1, \dots, X_d$ are non-zerodivisors modulo I.

So far we have I "cellular with respect to variables". (For example, we could have $I = (X_3(X_1^2 - X_2^2), X_3^2)$ and $P = (X_1 - X_2, X_3)$.) Now we will make it more "cellular with respect to binomials in the subring". Namely, let g be a non-zero binomial in P_0. (In the parenthetical example, we could have $g = X_1 - X_2$.) By Lemma 22, there exists $d \in \mathbb{N}$ such that $I : g^{[d]} = I : (g^{[d]})^2 = I +$ (monomial ideal). This in particular implies that P is not associated to $I : g^{[d]}$, and so necessarily P is associated to $I + (g^{[d]})$. Furthermore, the P-primary component of I is the P-primary component of the binomial ideal $I + (g^{[d]})$. We replace the old I by the larger binomial ideal $I + (g^{[d]})$. We repeat this to each g a binomial generator of P_0, so that we may assume that P is minimal over I. (In the parenthetical example above, we would now say with $d = 6$ that $I = (X_1^6 - X_2^6, X_3(X_1^2 - X_2^2), X_3^2)$.) Now $X_{d+1}, \dots, X_n$ are still nilpotent modulo I. The P-primary component of I is the same as the P-primary component of binomial ideal $I : (X_1 \cdots X_d)^\infty$, so by replacing I with $I : (X_1 \cdots X_d)^\infty$ we may assume that I is still cellular.

If $\mathrm{Ass}(R/I) = \{P\}$, then I is P-primary, and we are done. So we may assume that there exists an associated prime ideal Q of I different from P. Since P is minimal over I and different from Q, necessarily there exists an irreducible binomial $g = \underline{X}^{\underline{a}} - c\underline{X}^{\underline{b}} \in Q \setminus P$. Necessarily $g \notin (X_{d+1}, \dots, X_n)R$. Thus Lemma 22 applies, so there exists $d \in \mathbb{N}$ such that $I : g^{[d]} = I : (g^{[d]})^2 = I +$ (monomial ideal). Note that Q is not associated to this ideal but Q is associated to I, so that the binomial ideal $I : g^{[d]}$ is strictly larger than I. If $g^{[d]} \notin P$, then the P-primary component of I equals the P-primary component of $I : g^{[d]}$, and so by Noetherian induction (if we have proved it for all larger ideals, we can then prove it for one of the smaller ideals) we have that the P-primary component of I is binomial. So without loss of generality we may assume that $g^{[d]} \in P$. Then $g^{[d]}$ contains a factor in P of the form $g_0 = \underline{X}^{\underline{a}} - c'\underline{X}^{\underline{b}}$ for some $c' \in k$. If the characteristic of R is p, $g_0^{p^m}$ is a binomial for all m, we choose the largest m such that p^m divides d, and set $h = g^{[d]}/g_0, b = g_0^{p^m}$. In characteristic zero, we set $h = g^{[d]}/g_0$ and $b = g_0$. In either case, b is a binomial, $b \in I : h$ and $h \notin P$. Thus the P-primary component of I is the same as the P-primary component of $I : h$, and in particular, since $I \subseteq I + (b) \subseteq I : h$, it follows that the P-primary component of I is the same as the P-primary component of the binomial ideal $I + (b)$. If $b \in Q$, then $g_0 = \underline{X}^{\underline{a}} - c'\underline{X}^{\underline{b}}$ and $g = \underline{X}^{\underline{a}} - c\underline{X}^{\underline{b}}$ are both in Q. Necessarily $c \neq c'$, so that $\underline{X}^{\underline{a}}, \underline{X}^{\underline{b}} \in Q$, and since $g \notin (X_{d+1}, \dots, X_n)R$, it follows that Q contains one of the variables $X_1, \dots, X_d$. But these variables are non-zerodivisor modulo I, so that Q cannot be associated to I, which proves that

$b \notin Q$. But then I is strictly contained in $I + (b)$, and by Noetherian induction, the P-primary component is binomial. □

2.4 The Radical of a Binomial Ideal Is Binomial

Here is general commutative algebra fact: for any Noetherian commutative ring R, any ideal I, and any $X_1, \ldots, X_n$ in R,

$$\begin{aligned}\sqrt{I} &= \sqrt{I + (X_1)} \cap \cdots \cap \sqrt{I + (X_n)} \cap \sqrt{I : (X_1 \cdots X_n)^\infty} \\ &= \sqrt{I + (X_1)} \cap \cdots \cap \sqrt{I + (X_n)} \cap \sqrt{I : X_1 \cdots X_n}.\end{aligned}$$

Theorem 24 *The radical of any binomial ideal in a polynomial ring over an algebraically closed field is binomial.*

Proof This is clear if $n = 0$. So assume that $n > 0$. By the fact above,

$$\sqrt{I} = \sqrt{I + (X_1)} \cap \cdots \cap \sqrt{I + (X_n)} \cap \sqrt{I : (X_1 \cdots X_n)^\infty}.$$

Let $I_0 = \sqrt{I : (X_1 \cdots X_n)^\infty}$. We have established in Theorem 15 that $\sqrt{I_0} S = \sqrt{IS}$ is binomial in S. By Theorem 17, $\sqrt{I_0}$ is binomial.

Let $I_1 = I \cap k[X_2, \ldots, X_n]$. We know that I_1 is binomial. By induction on n, the radical of I_1 is binomial. This radical is contained in $\sqrt{I}$, so that $\sqrt{I} = \sqrt{\sqrt{I_1} + I}$. Thus without loss of generality we may assume that $\sqrt{I_1} \subseteq I$. Hence we may also assume that $\sqrt{I_1} = I_1$.

Let P be a prime ideal minimal over $I + (X_1)$. Suppose that there exists a binomial g in I that involves X_1 but is not in (X_1). Write $g = X_1 m' + m$ for some monomial terms m, m', with X_1 not appearing in m. Since P is a prime ideal, there exists a variable dividing m that is in P. Say this variable is X_2. Then P is a prime ideal minimal over $I + (X_1, X_2)$. By continuing this we get that, after reindexing, P is a prime ideal minimal over $I + (X_1, X_2, \ldots, X_d)$ and that any binomial in I is either in $(X_1, \ldots, X_d)$ or in $k[X_{d+1}, \ldots, X_d]$. By Gröbner bases rewriting,

$$\begin{aligned}I + (X_1, \ldots, X_d) &= ((I + (X_1, \ldots, X_d)) \cap k[X_{d+1}, \ldots, X_n] + (X_1, \ldots, X_d))R \\ &= (I_1 \cap k[X_{d+1}, \ldots, X_n] + (X_1, \ldots, X_d))R,\end{aligned}$$

and this is a radical ideal since I_1 is. This proves that the intersection of all the prime ideals minimal over $I + (X_1)$ equals the intersection of ideals of the form $I +$ (some variables). Hence by Proposition 13, $\sqrt{I + (X_1)} = I + J_1$ for some monomial ideal J_1. Similarly, $\sqrt{I + (X_i)} = I + J_i$ for some monomial ideals $J_1, \ldots, J_n$. By the first paragraph in this section and by Proposition 13 then $\sqrt{I} = (I + J) \cap I_0$ for some monomial ideal J. But $I \subseteq I_0$, so that $\sqrt{I} = I + J \cap I_0$, and this is a binomial ideal because J is monomial and I_0 is binomial (see p. 53). □

3 Primary Decomposition in Algebraic Statistics

Algebraic statistics is a relatively new field. The first systematic work is due to Studený [109] from an axiomatic point of view, and several works after that used the axiomatic approach. A first more concrete connection between statistics and commutative algebra is due to the paper of Diaconis and Sturmfels [46], which introduced the notion of a Markov basis. The book by Pistone et al. [92], published in 2001, is a book on commutative algebra and Gröbner bases for statisticians. Not all parts of statistics can be algebraicized, of course. Some of the current research topics in algebraic statistics are: design of experiments, graphical models, phylogenetic invariants, parametric inference, maximum likelihood estimation, applications in biology, et cetera. This section is about (conditional) independence.

3.1 Conditional Independence

Definition 25 A **random variable**, as used in probability and statistics, is not a variable in the algebra sense; it is a variable or function whose value is subject to variations due to chance. I cannot give a proper definition of "chance", but let us just say that examples of random variables are outcomes of flips of coins or rolls of dice. (If you are Persi Diaconis, a flip of a coin has a predetermined outcome, but not if I flip it.)

A **discrete random variable** is a random variable that can take on at most finitely many values (such as the flip of a coin or the roll of a die).

Throughout we will be using the standard notation $P(i)$ to stand for the **probability** that condition i is satisfied, and $P(i \mid j)$ to stand for the **(conditional) probability** that condition i is satisfied given that condition j holds. Whenever $P(j) \neq 0$, then

$$P(i \mid j) = \frac{P(i,j)}{P(j)}.$$

Definition 26 Random variables Y_1, Y_2 are **independent** for all possible values i of Y_1 and all possible values j of $Y_2, P(Y_1 = i \mid Y_2 = j) = P(Y_1 = i)$, or in other words, if

$$P(Y_1 = i, Y_2 = j) = P(Y_1 = i)P(Y_2 = j).$$

If this is satisfied, we write $Y_1 \perp\!\!\!\perp Y_2$.

Let $p_{ij} = P(Y_1 = i, Y_2 = j)$. Then $\sum_j p_{ij} = P(Y_1 = i)$ and $\sum_i p_{ij} = P(Y_2 = j)$. (In statistics, these sums are shortened to p_{i+} and p_{+j}, respectively.) For discrete random variables Y_1, Y_2, with Y_1 taking on all values in $[m]$ and Y_2 taking on all values in $[n]$, independence is equivalent to the following matrix equality:

$$\begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & & \vdots \\ p_{m1} & \cdots & p_{mn} \end{bmatrix} = \begin{bmatrix} P(Y_1 = 1) \\ P(Y_1 = 2) \\ \vdots \end{bmatrix} \begin{bmatrix} P(Y_2 = 1) \cdots & P(Y_2 = n) \end{bmatrix}.$$

Since the sum of the p_{ij} is 1, it follows that the rank of the matrix $[p_{ij}]$ is 1, and so $I_2([p_{ij}]) = 0$. Conversely, if $I_2([p_{ij}]) = 0$, since some p_{ij} is non-zero, necessarily $[p_{ij}]$ has rank 1. Then we can write

$$\begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & & \vdots \\ p_{m1} & \cdots & p_{mn} \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} \begin{bmatrix} b_1 \cdots & b_2 & \cdots b_m \end{bmatrix}$$

for some real numbers a_i, b_j. Since some p_{ij} is a positive real number, by possibly multiplying all a_i and b_j by -1 we may assume that all a_i, b_j are non-negative real numbers. Let $a = \sum_i a_i, b = \sum_j b_j$. Then

$$ab = \sum_{i,j} a_i b_j = \sum_{i,j} p_{ij} = 1,$$

whence we also have

$$\begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & & \vdots \\ p_{m1} & \cdots & p_{mn} \end{bmatrix} = \begin{bmatrix} a_1 b \\ \vdots \\ a_m b \end{bmatrix} \begin{bmatrix} ab_1 \cdots & ab_2 & \cdots ab_m \end{bmatrix}.$$

All the entries of the two matrices on above are non-negative, $a_i b = \sum_j a_i b_j = \sum_j p_{ij} = P(Y_1 = i)$ and $ab_j = \sum_i a_i b_j = \sum_i p_{ij} = P(Y_2 = j)$, which yields the factorization of $[p_{ij}]$ as in the rephrasing of independence. Thus $Y_1 \perp\!\!\!\perp Y_2$ if and only if $I_2([p_{ij}]_{i,j}) = 0$.

How does one decide independence in practice? Say a poll counts people according to their hair length and whether they watch soccer as follows:

	Watches soccer	Does not watch soccer
Has short hair	400	200
Has long hair	40	460

Thus watching soccer and the hair length in this group appear to not be independent: it seems that the hair length fairly determines whether one watches soccer. Even if the polling has a 10% error in representing the population, it still seems that the hair length fairly determines whether one watches soccer. However, the poll break-down among genders shows the following:

Men	Watching	*Not*
Short hair	400	100
Long hair	40	10

Women	Watching	Not
Short hair	0	100
Long hair	0	450

Now, given the gender, the probability that one watches soccer is independent of hair length (odds for watching is 4/5 for men, 0 for women).

This brings up an issue: in general one does not find such clean numbers with determinant precisely 0, and so one has to do further manipulations of the data to decide whether it is statistically likely that there is an independence of data.

Here I continue with the obvious needed definition arising from the previous example:

Definition 27 Random variables Y_1 and Y_2 are **independent given** the random variable Y_3, if for every value i of Y_1, j of Y_2 and k of Y_3,

$$P(Y_1 = i \mid Y_2 = j, Y_3 = k) = P(Y_1 = i \mid Y_3 = k).$$

If $P(Y_3 = k) > 0$, this is equivalent to saying that $P(Y_1 = i, Y_2 = j, Y_3 = k)P(Y_3 = k) = P(Y_1 = i)P(Y_2 = j)$. We write such independence as $Y_1 \perp\!\!\!\perp Y_2 \mid Y_3$.

Let M be the 3-dimensional hypermatrix whose (i, j, k) entry is $P(Y_1 = i, Y_2 = j, Y_3 = k)$, $Y_1 \perp\!\!\!\perp Y_2 \mid Y_3$. Then $Y_1 \perp\!\!\!\perp Y_2 \mid Y_3$ means that on each k-level of M, the ideal generated by the 2×2-minors of the matrix on that level is 0.

Here are the **axioms** of conditional independence:

1. **Triviality:** $X \perp\!\!\!\perp \emptyset \mid Z$. (Algebraically this says that the ideal generated by the 2×2-minors of an empty matrix is 0.)
2. **Symmetry:** $X \perp\!\!\!\perp Y \mid Z$ implies $Y \perp\!\!\!\perp X \mid Z$. (Algebraically this follows as the ideal of minors of a matrix as the same as the ideal of the transpose of that matrix.)
3. **Weak union:** $X \perp\!\!\!\perp \{Y_1, Y_2\} \mid Z$ implies $X \perp\!\!\!\perp Y_1 \mid \{Y_2, Z\}$. Here we point out that if U and V is a (discrete) random variable, so is $\{U, V\}$, whose values are pairs of values of U and V, of course. (Algebraically this says the following: let $p_{ijkl} = P(X = i, Y_1 = j, Y_2 = k, Z = l)$. The assumption says that for all values l of Z, the ideal generated by the 2×2-minors of the matrix $[p_{ijkl}]_{i,(j,k)}$ is 0. But then for fixed l and a fixed value k of Y_2, the ideal generated by the 2×2-minors of the submatrix $[p_{ijkl}]_{i,j}$ is 0 as well, which is the conclusion.)
4. **Decomposition:** $X \perp\!\!\!\perp \{Y_1, Y_2\} \mid Z$ implies $X \perp\!\!\!\perp Y_1 \mid Z$. (Algebraically this says that if for each $l, I_2([p_{ijkl}]_{i,(j,k)}) = 0$ then $I_2([p_{ij+l}]_{i,j}) = 0$, where $+$ means that the corresponding entry is the sum $\sum_k p_{ijkl}$.)

5. **Contraction:** $X \perp\!\!\!\perp Y \mid \{Z_1, Z_2\}$ and $X \perp\!\!\!\perp Z_2 \mid Z_1$ implies $X \perp\!\!\!\perp \{Y, Z_2\} \mid Z_1$. (Algebraically this says that if for each $k, l, I_2([p_{ijkl}]_{i,j}) = 0$ and for each $k, I_2([p_{i+kl}]_{i,l}) = 0$, then for each $k, I_2([p_{ijkl}]_{i,(j,l)}) = 0$.)
6. **Intersection axiom:** Under the assumption that all $P(X = i, Y = j, Z = k)$ are positive, $X \perp\!\!\!\perp Y \mid Z$ and $X \perp\!\!\!\perp Z \mid Y$ implies $X \perp\!\!\!\perp \{Y, Z\}$.

The last axiom is the focus of the next section.

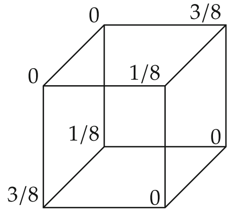
3.2 Intersection Axiom

Algebraically the intersection axiom says that if all p_{ijk} are positive, if for each $k, I_2([p_{ijk}]_{i,j}) = 0$, and if for each $j, I_2([p_{ijk}]_{i,k)}) = 0$, then $I_2([p_{ijk}]_{i,(j,k)}) = 0$.

Example 28 Here we show that the assumption on the p_{ijk} being positive is necessary. Let M be the $2 \times 2 \times 2$-hypermatrix whose (i, j, k) entry is

$$p_{ijk} = \begin{cases} 1/8, & \text{if } i = j = k = 1; \\ 3/8, & \text{if } i = 2, j = k = 1; \\ 3/8, & \text{if } i = 1, j = k = 2; \\ 1/8, & \text{if } i = j = k = 2; \\ 0, & \text{otherwise.} \end{cases}$$

We can view this in a $2 \times 2 \times 2$-hypermatrix, with the third axis going up, the second axis going to the right, and the first axis coming out of the page:



Then

$$[p_{ij1}]_{i,j} = \begin{bmatrix} 1/8 & 0 \\ 3/8 & 0 \end{bmatrix}, [p_{ij2}]_{i,j} = \begin{bmatrix} 0 & 3/8 \\ 0 & 1/8 \end{bmatrix},$$

$$[p_{i1k}]_{i,k} = \begin{bmatrix} 1/8 & 3/8 \\ 0 & 0 \end{bmatrix}, [p_{i2k}]_{i,k} = \begin{bmatrix} 0 & 0 \\ 3/8 & 1/8 \end{bmatrix},$$

and all have zero determinants. However,

$$[p_{ijk}]_{i,(j,k)} = \begin{bmatrix} 1/8 & 0 & 0 & 3/8 \\ 3/8 & 0 & 0 & 1/8 \end{bmatrix}$$

in which one 2×2-minor is not zero. Note that the last matrix is the flattening of the hypermatrix—squish into the $x - y$ plane, without any overlaps.

The intersection axiom says that if all p_{ijk} are non-zero, the conditions on the vanishing on the minors along each k and along each j-level are enough to make the "slanted" 2×2-minors zero as well.

We parse the intersection axiom further. Now let X_{ijk} stand for a variable (algebraic, not random, variable). The axiom says that the simultaneous zero $\underline{\alpha}$ of $I_2([X_{ijk}]_{i,j})$ for each k and of $I_2([X_{ijk}]_{i,k})$ for each j is also a zero of $I_2([X_{ijk}]_{i,(j,k)})$ if all entries in $\underline{\alpha}$ are positive. Via Hilbert's Nullstellensatz this says that

$$I_2([X_{ijk}]_{i,(j,k)}) \subseteq \sqrt{\sum_k I_2([X_{ijk}]_{i,j}) + \sum_j I_2([X_{ijk}]_{i,k}) : (\prod_{i,j,k} X_{ijk})^\infty}.$$

Certainly

$$\sum_k I_2([X_{ijk}]_{i,j}) + \sum_j I_2([X_{ijk}]_{i,k}) \subseteq I_2([X_{ijk}]_{i,(j,k)}).$$

Statisticians have known that $\left(\sum_k I_2([X_{ijk}]_{i,j}) + \sum_j I_2([X_{ijk}]_{i,k})\right) : (\prod_{i,j,k} X_{ijk})^\infty = I_2([X_{ijk}]_{i,(j,k)})$, and they have also known that the latter ideal is a prime ideal not containing any variables; see a proof in Theorem 29. Thus

$$I_2([X_{ijk}]_{i,(j,k)}) = \left(\sum_k I_2([X_{ijk}]_{i,j}) + \sum_j I_2([X_{ijk}]_{i,k})\right) : (\prod_{i,j,k} X_{ijk})^\infty,$$

so that the intersection axiom says that one of the associated primes and even primary components of $\sum_k I_2([X_{ijk}]_{i,j}) + \sum_j I_2([X_{ijk}]_{i,k})$ is $I_2([X_{ijk}]_{i,(j,k)})$. Fink in [54] determined all other associated prime ideals of $\sum_k I_2([X_{ijk}]_{i,j}) + \sum_j I_2([X_{ijk}]_{i,k})$, proving the conjecture of Cartwright and Engström (conjecture is stated in [47, p. 146]).

The papers [8] and [111] algebraically generalize the **intersection axiom** to the following: if all for all possible values i_j of Y_j, $P(Y_1 = i_1, \dots, Y_n = i_n) > 0$, and if $Y_1 \perp\!\!\!\perp Y_i \mid (\{Y_2, \dots, Y_n\} \setminus \{Y_i\})$ for all $i = 2 \dots, n$, then $Y_1 \perp\!\!\!\perp \{Y_2, \dots, Y_n\}$.

3.3 A Version of the Hammersley-Clifford Theorem

For completeness I give in this section the most algebraic proof I can think of of the Hammersley-Clifford Theorem. A different proof can be found in [74, p. 36], and there is more discussion in [47, p. 80].

Let G be an undirected graph on the set of vertices $[n]$. Let $Y_1, \ldots, Y_n$ be discrete random variables. Associated to this graph is a collection of conditional independence statements:

$$\{Y_i \perp\!\!\!\perp Y_j \mid \big(\{Y_1, \ldots, Y_n\} \setminus \{Y_i, Y_j\}\big) : i \neq j, (i,j) \text{ is not an edge in } G\}.$$

(Such a graphical model of conditional independence statements is said to satisfy the **pairwise Markov property**.) If Y_i takes on r_i distinct values, then we need $r_1 \cdots r_n$ variables X_a, and we denote by I_G the ideal generated by all the 2×2-minors of all the matrices obtained from all the conditional independence statements (over some understood field F).

For example, if $n = 3$ and the only edge in the graph is $(2, 3)$, the associated conditional independences are

$$Y_1 \perp\!\!\!\perp Y_2 \mid Y_3 \text{ and } Y_1 \perp\!\!\!\perp Y_3 \mid Y_2,$$

which are precisely the hypotheses of the intersection axiom. Fink [54] analyzed the corresponding ideal. Swanson and Taylor [111] analyzed the ideals for arbitrary n and $t \in [n]$ with the graph being the complete graph on vertices $t + 1, \ldots, n$; Ay and Rauh [8] analyzed the case for arbitrary n and $t = 1$.

Theorem 29 (Hammersley and Clifford) *Let n, G, I_G be as above. Then $I_G : (\prod_a X_a)^\infty$ is a binomial prime ideal which does not contain any variables. In particular, $I_G : (\prod_a X_a)^\infty$ is a minimal prime ideal over I_G, and its primary component is the prime ideal.*

Furthermore, the variety of the prime ideal in this theorem has a monomial parametrization, which is explicit in the proof below.

Proof Suppose that Y_i takes on r_i distinct values. Without loss of generality these values are in the set $[r_i]$. If any r_i equals 0 or 1, the conditional independence statements can be rephrased without using that Y_i. So we may assume that all r_i are strictly bigger than 1.

If G is a complete graph on $[n]$, then $I_G = 0$, so that $I_G = 0 = I_G : (\prod_a X_a)^\infty$ is a binomial prime ideal which does not contain any variables. In the sequel we assume that G is not a complete graph, so that I_G is a non-zero (binomial) ideal.

Fix a pair of distinct i, j in $[n]$ such that (i, j) is not an edge in G. Fix $\alpha = (\alpha_1, \ldots, \alpha_n)$, with α_k varying over the possible values of the random variable Y_k. Let M_α be the $r_i \times r_j$ generic matrix whose (k, l)-entry is X_a with $a_i = k, a_j = l$, and all other components in a identical to the corresponding components in α. (Obviously α_i and α_j are not needed to specify M_α.) The ideal I_{ij} expressing the conditional independence statement $Y_i \perp\!\!\!\perp Y_j \mid \big(\{Y_1,\dots,Y_n\}\setminus\{Y_i,Y_j\}\big)$ is generated by all $I_2(M_\alpha)$ as α varies.

By definition $I_G = \sum_{i,j} I_{ij}$, as i,j vary over distinct elements of $[n]$ such that (i,j) is not an edge (and without loss of generality $i<j$).

A clique in G is a subset of its vertices any two of which are connected by an edge. For any maximal clique L of G and for each $c_L \in \prod_{i\in L}[r_i]$, let T_{L,c_L} be a variable over the underlying field F. Let $\varphi : F[X_a : a] \to F[T_{L,c_L} : L, c_L]$ be the F-algebra homomorphism such that $\varphi(X_a) = \prod_L T_{L,a(L)}$, as L varies over the maximal cliques of G, and where $a(L)$ is the $|L|$-tuple consisting only of the L-components of a. Let P be the kernel of φ.

Warning: Whereas I_G is the sum of the I_{ij} where (i,j) is not an edge, the variables T_{L,c_L} and thus the map φ instead use (cliques of) edges and isolated vertices.

We prove that $I_G \subseteq P$. It suffices to prove that $I_{ij} \subseteq P$, where (i,j) is not an edge. For simplicity, suppose that $(1,2)$ is not an edge in G. By reindexing it suffices to prove that $X_{(1,1,\dots,1)}X_{(2,2,1,\dots,1)} - X_{(1,2,1,\dots,1)}X_{(2,1,1,\dots,1)} \in P$. To simplify notation, we treat below $T_{L,c(L)}$ as 1 if L is not a clique of G. Note that no clique contains both 1 and 2. Then φ maps $X_{(1,1,\dots,1)}$ to

$$\prod_{1\in L} T_{L,(1,\dots,1)} \prod_{2\in L} T_{L,(1,\dots,1)} \prod_{1,2\notin L} T_{L,(1,\dots,1)},$$

$X_{(2,2,1,\dots,1)}$ to

$$\prod_{1\in L} T_{L,(2,1,\dots,1)} \prod_{2\in L} T_{L,(2,1,\dots,1)} \prod_{1,2\notin L} T_{L,(2,\dots,1)},$$

$X_{(1,2,1,\dots,1)}$ to

$$\prod_{1\in L} T_{L,(1,\dots,1)} \prod_{2\in L} T_{L,(2,1\dots,1)} \prod_{1,2\notin L} T_{L,(1,\dots,1)},$$

and $X_{(2,1,1,\dots,1)}$ to

$$\prod_{1\in L} T_{L,(2,1,\dots,1)} \prod_{2\in L} T_{L,(1,\dots,1)} \prod_{1,2\notin L} T_{L,(2,\dots,1)},$$

so that $X_{(1,1,\dots,1)}X_{(2,2,1,\dots,1)} - X_{(1,2,1,\dots,1)}X_{(2,1,1,\dots,1)}$ is mapped by φ to 0. Thus $I_G \subseteq P$.

As φ is a homogeneous monomial map of positive degree, P is generated by binomials and does not contain any variables. It follows that $I_G : (\prod_a X_a)^\infty \subseteq P$.

Now let $f \in P$. The proof below that $f \in I_G : (\prod_a X_a)^\infty$ is fairly elementary, only long in notation. Since P is the kernel of a homogeneous monomial map, we may assume that $f = X_{a_1}\cdots X_{a_m} - X_{b_1}\cdots X_{b_m}$ for some n-tuples $a_1,\dots,a_m,b_1,\dots,b_m$. To show that $f \in I_G : (\prod_a X_a)^\infty$, it suffices to prove that any monomial multiple of f is in $I_G : (\prod_a X_a)^\infty$. Fix a non-edge (i,j). Suppose that in a_k neither the ith nor the jth component is 1. Let c_k be the n-tuple whose ith and jth components are 1 and whose other components agree with the components of a_k. Both X_{a_k} and X_{c_k} lie in the same submatrix of $[X_a]_a$ that gives I_{ij}, so that $X_{a_k}X_{c_k}$ reduces modulo I_{ij} and hence modulo I_G to $X_{a'_k}X_{c'_k}$ where a'_k and c'_k each have entry 1 either in the ith or the jth components. Let U be the product of all such X_{c_k}. Then modulo I_G, Thus Uf reduces with respect to I_G to a binomial in which the subscripts of all the variables appearing in the first monomial have at least one of i, j components equal to 1, and in the second monomial the number of non-1 ith and jth components in the subscripts does not increase. By repeating this for the second monomial as well, we may assume that for each variable appearing in f, the ith or the jth component in the subscript is 1. If we next similarly clean positions i', j' in this way, we do not at the same time lose the cleaned property of positions i and j: as factors of the multipliers U keep the clean (i, j) property. By repeating this cleaning, in finitely many rounds we get a binomial f in P such that for each non-edge (i, j) and for each variable appearing in f, the ith or the jth component of the subscript of that variable is 1.

With the assumption that for each non-edge (i, j), the ith or the jth component of a_k and of b_k is 1, we claim that $f = 0 \in I_G$. If $a_i = b_j$ for some $i, j \in [m]$, then the binomial f/X_{a_i} has the same property of many components being 1, and it suffices to prove that $f/X_{a_i} = 0 \in I_G$. Thus without loss of generality we may assume that $m > 0$ and that $a_i \neq b_j$ for all $i, j \in [m]$. Let K_j (resp. L_j) be the set of all $i \in [n]$ such that the ith component in a_j (resp. b_j) is not 1. By possibly reindexing we may assume that K_1 is maximal among all such sets. By the assumption on the 1-entries, necessarily K_1 is contained in a maximal clique L of G, and for all $i \in [n] \setminus L$, the ith component in a_1 is 1. Since $f \in P$, the variable $T_{L,a_1(L)}$ must also divide $\varphi(X_{b_k})$ for some $k \in [m]$. This means that a_1 and b_k agree in the L-components, and in particular, $K_1 \subseteq L_k$. By maximality of K_1, necessarily $K_1 = L_k$, whence $a_1 = b_k$, which is a contradiction.

This proves that $P = I_G : (\prod_a X_a)^\infty$ is a binomial prime ideal containing no variables. Thus $I_G : (\prod_a X_a)^\infty$ is contained in the P-primary component of I_G, and since $I_G : (\prod_a X_a)^\infty$ is primary (even prime) and contains I_G, necessarily it is the P-primary component. $\square$

In particular, if $n = 3$ and the only edge in G is $(2, 3)$, then I_G is the ideal of the intersection axiom, which fills in the details in the discussion on page 65. Even more simply, if $n = 2$ and G contains no edges, then $I_G = I_G : (\prod_a X_a)^\infty$ is the ideal generated by the 2×2-minors of the generic matrix.

Remark 30 To any monomial parametrization $\varphi : F[X_c : c] \to F[T_d : d]$ we can associate a $0-1$ matrix A whose (c, d)-entry equals 1 if T_d is a factor of $\varphi(X_c)$, and is 0 otherwise. In the theorem above the indices c were n-tuples; here we assume that these are ordered in some way, so that for any monomial $\prod_c X_c^{e_c}$ we can talk about the exponent vector $(e_c : c)$. For any binomial $\prod_c X_c^{e_c} - \prod_c X_c^{f_c}$ in the kernel of φ, the corresponding vector $(e_c : c) - (f_c : c)$ is in the kernel of A. Conversely, for any integer vector $(e_c : c)$ in the kernel of A, the binomial $\prod_{e_c>0} X_c^{e_c} - \prod_{e_c<0} X_c^{-e_c}$ is a binomial in the kernel of φ. Thus finding a set the kernel of φ is the same as finding the kernel of A as a $\mathbb{Z}$-submodule of the set of all integer vectors. The generating set of the latter kernel is a **Markov basis** for A, and its connections to algebraic statistics were first explored by Diaconis and Sturmfels in [46].

3.4 Summary/Unification of Some Recent Papers

This is a partial summary of the papers Fink [54], Herzog et al. [64], Ohtani [86], Ay-Rauh [8], Swanson and Taylor [111]: there are some similarities in the methods and results of these papers, but there does not seem to be one all-encompassing theorem. I present these results using as much of the common language as I can, but the four papers have further details and results.

Let $r_1, r_2, \ldots, r_n$ be positive integers, and let $N = [r_1] \times [r_2] \times \cdots \times [r_n]$ (where for any positive integer r, $[r] = \{1, 2, \ldots, r\}$). Let R be the polynomial ring in variables X_a over a field, where a varies over elements in N. We will often refer to the generic hypermatrix $[X_a : a \in N]$, so we give it a name, say M.

A generalized two-by-two determinant of M, for given $a, b \in N$ and $K \subseteq [n]$, is

$$f_{K,a,b} = X_a X_b - X_{\mathrm{s}(K,a,b)} X_{\mathrm{s}(K,b,a)},$$

where $\mathrm{s}(K, a, b)$ is an element of N with

$$\mathrm{s}(K,a,b)_j = \begin{cases} b_j, & \text{if } j \in K; \\ a_j, & \text{if } j \notin K. \end{cases}$$

If $K = \{i\}$, we also write $\mathrm{s}(i, a, b)$ for $\mathrm{s}(\{i\}, a, b)$ and $f_{i,a,b}$ for $f_{\{i\},a,b}$. When a and b differ only in positions i and j, then $f_{i,a,b}$ is precisely a standard two-by-two determinant of the submatrix of M obtained by keeping the entries that agree with a and b in the positions $k \neq i, j$.

Let $t \in [n]$. For each $i \in [t]$ let G_i be a simple graph on $[r_1] \times \cdots \times \widehat{[r_i]} \times \cdots \times [r_n]$. (These graphs play a very different role from the ones in Sect. 3.3.) Define

$$I^{\langle t \rangle}(G_1, \ldots, G_t) =$$
$$(f_{i,a,b} : i \le t, \{(a_1, \ldots, \widehat{a_i}, \ldots, a_n), (b_1, \ldots, \widehat{b_i}, \ldots, b_n)\} \text{ is an edge in } G_i).$$

These ideals have been studied as follows:

1. Fink [54]: $n = 3, t = 1$, and G_1 is the grid graph on $[r_2] \times [r_3]$, namely $G_1 = \left(\cup_{j \in [r_2], k_1, k_2 \in [r_3]} \{(j, k_1), (j, k_2)\}\right) \cup \left(\cup_{k \in [r_3], j_1, j_2 \in [r_2]} \{(j_1, k), (j_2, k)\}\right)$.
2. Herzog et al. [64] and independently Ohtani [86]: $n = 2, r_1 = 2, t = 1$.
3. Ay and Rauh [8]: $t = 1$.
4. Swanson and Taylor [111]: for each i, G_i is the grid graph on $[r_1] \times \cdots \times \widehat{[r_i]} \times \cdots \times [r_n]$, i.e., the edges consist of those pairs of $(n-1)$-tuples that differ in precisely one component.

Throughout $t \in [n]$. For each $i \in [t]$, let $N_i = [r_1] \times \cdots \times \widehat{[r_i]} \times \cdots \times [r_n]$, and let G_i be a graph on N_i. We write G for $\{G_1, \ldots, G_t\}$. We use the Hamming distance on N: $d(a, b) = \#\{i \in [n] : a_i \neq b_i\}$, and $D(a, b) = \{i \in [n] : a_i \neq b_i\}$.

Definition 31 We say that $a, b \in N$ are **directly connected relative to** G_i if $\{(a_1, \ldots, \widehat{a_i}, \ldots, a_n), (b_1, \ldots, \widehat{b_i}, \ldots, b_n)\}$ is an edge in G_i.

We say that $a, b \in N$ are **connected relative to** G_i if there exist $c_1, c_2, \ldots, c_{k-1} \in N$ such that with $c_0 = a$ and $c_k = b$, for each $j = 1, \ldots, k$, c_{j-1} and c_j are directly connected relative to G_i. We call $a = c_0, c_1, \ldots, c_{k-1}, c_k = b$ a **path** from a to b relative to G_i.

We say that $a, b \in N$ are **connected relative to** G if there exist $c_1, c_2, \ldots, c_{k-1} \in N$ such that with $c_0 = a$ and $c_k = b$, for each $j = 1, \ldots, k$, there exists $i \in [t]$ such that c_{j-1} and c_j are directly connected relative to G_i. We call $a = c_0, c_1, \ldots, c_{k-1}, c_k = b$ a **path** from a to b relative to G.

Lemma 32 *Let $i \in [t]$ and let $c_0, \ldots, c_k$ be a path relative to G_i. Then*

$$\left(\prod_{j=1}^{k-1} X_{c_j}\right) \cdot f_{i,c_0,c_k} \in I^{\langle t \rangle}(G_i).$$

Proof (Similar Versions of This Are Proved in [8] and [111].) If the ith components in c_0 and c_k are identical then $f_{i,c_0,c_k} = 0$. If c_0, c_k without the ith components form an edge in G_i, then $f_{i,c_0,c_k} \in I^{\langle t \rangle}(G_i)$. In particular, the lemma holds if $k \leq 1$. Now let $k \geq 2$. Then modulo $I^{\langle t \rangle}(G_i)$, with U an abbreviation for $X_{c_1} \cdots X_{c_{k-2}}$,

$$\begin{aligned}
X_{c_0} U X_{c_{k-1}} X_{c_k} &\equiv X_{\mathrm{s}(i,c_0,c_{k-1})} U X_{\mathrm{s}(i,c_{k-1},c_0)} X_{c_k} \text{ (by induction on } k) \\
&\equiv X_{\mathrm{s}(i,c_0,c_{k-1})} U X_{\mathrm{s}(i,\mathrm{s}(i,c_{k-1},c_0),c_k)} X_{\mathrm{s}(i,c_k,\mathrm{s}(i,c_{k-1},c_0))} \\
&\qquad \text{(since } \mathrm{s}(i, c_{k-1}, c_0), c_k \text{ is a path relative to } G_i) \\
&= X_{\mathrm{s}(i,c_0,c_{k-1})} U X_{\mathrm{s}(i,c_{k-1},c_k)} X_{\mathrm{s}(i,c_k,c_0)} \\
&\equiv X_{\mathrm{s}(i,\mathrm{s}(i,c_0,c_{k-1}),\mathrm{s}(i,c_{k-1},c_k))} U X_{\mathrm{s}(i,\mathrm{s}(i,c_{k-1},c_k),\mathrm{s}(i,c_0,c_{k-1}))} X_{\mathrm{s}(i,c_k,c_0)} \\
&\qquad \text{(by induction on } k, \text{ since} \\
&\qquad \mathrm{s}(i, c_0, c_{k-1}), c_1, \ldots, c_{k-2}, \mathrm{s}(i, c_{k-1}, c_k) \text{ is a path relative to } G_i) \\
&= X_{\mathrm{s}(i,c_0,c_k)} U X_{c_{k-1}} X_{\mathrm{s}(i,c_k,c_0)},
\end{aligned}$$

which proves the lemma. □

Remark 33 Note how the ith entry in the path is not important! But if we want to mix G_i and G_j, the ith entries make a difference (and it is not clear how to control for that fully, in fact, the ideals in [111] have embedded primes whose characterization is not complete).

Lemma 34 *Let $i \in [t]$. Let H be the set of all elements of the form $\left(\prod_{j=1}^{k-1} X_{c_j}\right) \cdot f_{i,c_0,c_k}$ as $c_0, \ldots, c_k$ vary over paths relative to G_i. Then H is a (redundant) Gröbner basis in the lexicographic order.*

Proof Let $f = \left(\prod_{j=1}^{k-1} X_{c_j}\right) \cdot f_{i,c_0,c_k}$ and $g = \left(\prod_{j=1}^{l-1} X_{d_j}\right) \cdot f_{i,d_0,d_l}$. We want to show that the S-polynomial of f and g reduces to 0 with respect to H. In the lexicographic order, the leading monomial of f_{i,c_0,c_k} is either $X_{c_0}X_{c_k}$ or $X_{\mathrm{s}(i,c_0,c_k)}X_{\mathrm{s}(i,c_k,c_0)}$. In the latter case, since $f_{i,c_0,c_k} = -f_{i,\mathrm{s}(i,c_0,c_k),\mathrm{s}(i,c_k,c_0)}$ and since $\mathrm{s}(i, c_0, c_k), c_1, \ldots, c_{k-1}, \mathrm{s}(i, c_k, c_0)$ is a path relative to G_i, by possibly replacing c_0 and c_k with their switches we may assume that the leading term of f is $X_{c_0}X_{c_k}$. Similarly we may assume that the leading term of g is $X_{d_0}X_{d_l}$. By standard Gröbner bases, if $\{c_0, c_k\}$ and $\{d_0, d_l\}$ are disjoint, then the S-polynomial of f and g reduces to 0. If $c_0 = d_0$ and $c_k = d_l$, then $S(f, g) = m(X_{\mathrm{s}(i,d_0,d_l)}X_{\mathrm{s}(i,d_l,d_0)} - X_{\mathrm{s}(i,c_0,c_k)}X_{\mathrm{s}(i,c_k,c_0)})$, where $m = \mathrm{lcm}(X_{c_1} \cdots X_{c_k}, X_{d_1} \cdots X_{d_l})$ is the product of all the variables in a path from $\mathrm{s}(i, d_0, d_l) = \mathrm{s}(i, c_0, c_k)$ to $\mathrm{s}(i, d_l, d_0) = \mathrm{s}(i, c_k, c_0)$. so that this S-polynomial is in H. It remains to consider the case $c_0 = d_0$ and $c_k \neq d_l$. Then $S(f, g) = m(X_{c_k}X_{\mathrm{s}(i,d_0,d_l)}X_{\mathrm{s}(i,d_l,d_0)} - X_{d_l}X_{\mathrm{s}(i,c_0,c_k)}X_{\mathrm{s}(i,c_k,c_0)})$, where $m = \mathrm{lcm}(X_{c_1} \cdots X_{c_k}, X_{d_1} \cdots X_{d_l})$. Consider the term $X_{c_k}X_{\mathrm{s}(i,d_0,d_l)}$: if it is bigger in the lexicographic order than $X_{\mathrm{s}(i,c_k,d_l)}X_{\mathrm{s}(i,d_0,c_k)}$, then since m is a product of the right variables in the right path, we can reduce $S(f, g)$ further. Any further reductions of the two degree-three terms in the binomial part can be reduced similarly because m has enough variables, until $S(f, g)$ reduces to 0. □

Papers [54, 64, 86], and [8] go further and determine minimal Gröbner bases, via further restrictions on admissible paths.

3.5 A Related Game

One would understand the primary components of I_G in the previous section much better if one understood the following:

Problem 35 Let $a_1, \ldots, a_m, b_1, \ldots, b_m$ be n-tuples ($2m$ of them) such that $X_{a_1} \cdots X_{a_m} - X_{b_1} \cdots X_{b_m} \in I^{\langle n \rangle}(G)$. (For ideals in [111], an equivalent and more elementary check for ideal membership is that for each $i = 1, \ldots, n$, the ith components of $a_1, \ldots, a_m$ are up to order the same as the ith components of $b_1, \ldots, b_m$.) Carry out the successive rewriting of $X_{a_1} \cdots X_{a_m}$ with respect to the generators of $I^{\langle n \rangle}(G)$ to get to $X_{b_1} \cdots X_{b_m}$.

Since this is a hard problem, I would like instead somebody to make it a computer game or an app:

Game The computer serves you two lists of n-tuples of positive integers: $a_1, \ldots, a_m$ and $b_1, \ldots, b_m$. (In one version of the game, $X_{a_1} \cdots X_{a_m} - X_{b_1} \cdots X_{b_m} \in I^{\langle n \rangle}(G)$, in another version whether this is so is determined by chance.) The following move is allowed on the list $a_1, \ldots, a_m$: if a_i and a_j differ in exactly two components, say k

and l, replace the list $a_1, \ldots, a_m$ with the list $c_1, \ldots, c_m$ where $c_i = \mathrm{s}(k, a_i, a_j) = \mathrm{s}(l, a_j, a_i), c_j = \mathrm{s}(k, a_j, a_i) = \mathrm{s}(l, a_i, a_j)$, and for all $s \neq i, j, c_s = a_s$. Repeat the moves on the new list $c_1, \ldots, c_m$ until you get the list $b_1, \ldots, b_m$. You get bonus points for accomplishing the task in few moves.

I envision users all over the world solving (playing with) instances of this while waiting for a bus or in coffee shops, and they could be competing for the shortest number of moves, with possibly short answers being transmitted to some central station.

3.6 Binomial Edge Ideals with Macaulay2

Let us make now a short review of some of the preceding results with the computer algebra system Macaulay2 at hand.

First, we will make use of the package `Binomials` so we load it into the system:

```
i1 : needsPackage "Binomials"
```

Consider now a simple graph G on n vertices and a polynomial ring in $2n$ variables, for each edge (i, j) we consider the binomial $f(i, j) = x_i y_j - x_j y_i$. The ideal generated by such binomials is the **binomial edge ideal** of G, J_G. We construct it with the following simple Macaulay2 function:

```
i2 : graphminorsedge = (n,LL) -> (
     HHR = QQ[x_1..x_n, y_1..y_n];
     ideal apply(LL, k-> x_(k_0) * y_(k_1) - x_(k_1) * y_(k_0))
)
```

Observe that this is a generalization of the ideal of 2-minors of a $2n$-matrix of indeterminates (which corresponds to the binomial edge ideal of the complete n-graph).

We say that the graph G is **closed** with respect to the labelling if for all (i, j), (k, l) such that $i < j$ and $k < l$ we have another edge (j, l) if $i = k$ and (i, k) if $j = l$. With the help of Macaulay2 the reader can try some examples of ideals of closed graphs and some ideals of non-closed graphs to see how Theorem 1 in [64] works.

A nice exercise is to experiment with closed **bipartite graphs** to find their Gröbner bases.

In general, if the graph is not closed, the Gröbner basis does not coincide with the binomials given by the edges, but can we find the basis in the graph? Let us define admissible paths $i_1, \ldots, i_r$ as follows:

1. $i_k \neq i_l \forall 1 \leq k \neq l \leq r$.
2. For each $k = 1, \ldots, r-1$ either $i_k < i$ or $i_k > j$.
3. For any proper subset $\{j_1, \ldots, j_s\}$ of $\{i_1, \ldots, i_{r-1}\}$ the sequence $i, j_1, \ldots, j_s, j$ is not a path.

One can write a function to construct all admissible paths and use it to find all the admissible paths in a closed graph. Now, for each admissible path p construct the monomial $u_p = \prod_{(i_k>i)}(x_{i_k})\prod_{(i_l<i)}(y_{i_l})$. The Gröbner basis is then given by $\bigcup_{i<j}\{u_p f_{i,j} | p$ is an admissible path from i to $j\}$.

We can follow [86] that describes operations on graphs that lead to a primary decomposition of J_G. First, define complete vertices as those such that all their neighbours are connected among them. We perform the following operations on any vertex v that is not complete:

1. Delete v and all the edges incident to v
2. Add all edges that connect vertices in the neighbourhood of v.

From each of these operations we obtain a graph, G' and G'' respectively, each of one has less non-complete vertices. These graph operations yield algebraic operations:

1. $J_{G'} + (x_v, y_v)$
2. $I_{G''} + I_2(N_G(v))$ where $N_G(v)$ is given by the binomials involving v.

Taking as base case the complete graph, whose ideal is prime, this decomposition leads to an alternative algorithm for primary decompositions. We encourage the reader to use Macaulay2 to write a program that implements Ohtani's procedure and compare the results with the in-built primary decomposition algorithms.

3.7 A Short Excursion Into Networks Using Monomial Primary Decompositions

To finish this chapter, let us enter into the world of networks, bringing primary decompositions with us. We will use primary decompositions of monomial ideals here. The monomial case, simpler than the general polynomial case has however multiple applications. We include this section to add yet another view of the use of primary decompositions. Networks are ubiquitous and there are many different approaches to them. A beautiful survey on the topic is [84]. One can see networks as graphs, where we call vertices to the nodes and edges to the connections. Graphs have been extensively studied using commutative algebra, cf. for example [80, 115]. We will in this section introduce the reader to the use of primary decompositions to study the problem of network resilience, in particular the design of attack strategies to break a connected network into disconnected pieces.

Consider a connected network (graph) N. We want to remove nodes (and all the incident connections) so that the network becomes disconnected as soon as possible. What is a good strategy to choose which nodes to delete first? A simple intuitive strategy is to delete first the nodes with biggest degree (i.e. with most connections incident to it). Other strategies are based on different data like betweenness centrality, etc. The approach we are using in this section is to attack the network based on its vertex covers.

A vertex cover of a graph (we see now networks as graphs) is a set C of vertices such that each edge of the graph is incident to at least one vertex of C. C is a **minimal** vertex cover if no subset of C is a vertex cover. C is a **minimum** vertex cover if it is a vertex cover of minimal cardinality. Minimal and minimum vertex covers are not unique in general. Given a graph G we denote by $mvc(G)$ the set of minimal vertex covers of G and by $MVC(G)$ the set of minimum vertex covers of G. We furthermore denote as $\tau(G)$ cardinality of any minimum vertex cover of G, $\tau(G)$ is called the *covering number* of G. For any vertex v we define the *covering degree* and *covering index* of a vertex n as follows

Definition 36 The **covering degree** of v, denoted $cd(v)$ is the number of minimal vertex covers that contain v,

$$cd(v) := \#\{V' \in mcv(G) \text{ such that } v \in V'\}.$$

The **covering index** of v, denoted $ci(v)$ is computed as the number of minimum vertex covers that contain v plus the ratio of the number of minimal vertex covers that contain v to the total number of minimal vertex covers of G,

$$ci(v) := \#\{V' \in MCV(G) \text{ such that } v \in V'\} + \frac{cd(v)}{|mcv(G)|}$$

Two strategies to break up our graph (network) G consist in deleting first the node with highest covering degree or to delete first the vertex with highest covering index, and then proceed downwards. These strategies have been proven to be efficient in several network models [100].

To use these strategies we need to compute all minimal and/or minimum vertex covers, which is a difficult problem in general (it is an example of an NP-hard problem). Here is were computational commutative algebra can help. To every graph G one can associate its edge ideal I_G [115], which is a monomial ideal. Every primary component (equivalently every generator of its Alexander dual) corresponds to a minimal vertex cover of G. One can see that the covering number of G is exactly the codimension of I_G. With these correspondences at hand one can then use a computer algebra system to compute covering degree and covering index of every vertex of G and employ the described strategies.

Example 37 Let G be a line graph with three nodes x, y, z and two edges $(x, y), (y, z)$. It is clear that G has four vertex covers $\{x, y\}, \{x, z\}, \{y, z\}$ and $\{y\}$ but only two of them are minimal, $\{x, z\}$ and $\{y\}$, and only the last one is a minimum vertex cover.

We will use the Macaulay2 package `EdgeIdeals` and compute the algebraic equivalent to the above description:

```
i1 : loadPackage "EdgeIdeals";

i2 : R=QQ[x,y,z];

i3 : G=graph {{x,y},{y,z}};

i4 : I=edgeIdeal G;
```

```
i5 : primaryDecomposition I

o5 = {monomialIdeal(y), monomialIdeal (x, z)}

i6 : codim I

o6 = 1

i7 : dual(I)

o7 = monomialIdeal (y, x*z)
```

As the number of vertices in the graph grows, the number of minimal vertex coverings grows exponentially, to say it algebraically, as the number n of variables grows, the number of primary components a monomial ideal in n variables (i.e. the number of generators of it Alexander dual) grows exponentially. A known (achievable) higher bound is $3^{\frac{n}{3}}$. So computing covering degree and index is expensive in general. Is there any advantage in using the strategies based on covering index and degree instead of using just vertex degree for example? As example 37 shows, it might happen that vertex degree and covering degree or index are correlated and the result of using vertex degree is similar, while the computational effort is much smaller. Experiments show, however, see [100] that vertex degree or betweenness centrality are not correlated to covering degree and index in several types of network models. Furthermore, the attacks based on covering degree and index are far more efficient that those based on vertex degree or betweenness centrality.

We propose the reader to experiment with the primary decompositions of edge ideals of some structured graphs, like the wheel n-graph or with random network models, such as Erdös-Renyi, Watts-Strogatz or Albert-Barabasi.

Combinatorics and Algebra of Geometric Subdivision Operations

Fatemeh Mohammadi and Volkmar Welker

1 Introduction

In the subsequent sections we survey results from combinatorics, discrete geometry and commutative algebra concerning invariants and properties of subdivisions of simplicial complexes. For most of the time we are interested in deriving results that hold for specific subdivision operations that are motivated from combinatorics, geometry and algebra. In particular, we study barycentric, edgewise and interval subdivisions (see Sect. 3 for the respective definitions). Even though we mention some suspicion that part of the results we present may only be a glimpse of what is true for general subdivision operations we do not focus on this aspect. In particular, we are quite sure that some asymptotic results and some convergence results from Sect. 9 are just instances of more general phenomena. Overall, retriangulations are subtle geometric operations and we refer the reader to the book [40] for a comprehensive introduction. Since our focus lies on specific constructions we make only little use of the theory from [40]. Nevertheless, we are convinced that if one wants to go beyond specific subdivision operations it will become inevitable to dig deeper into the theory of triangulations.

We start in Sect. 2 with a quick introduction on abstract and geometric simplicial complexes. For most of the paper we work with abstract simplicial complexes but for some definitions and perspectives the geometric viewpoint turns out to be advantageous. In Sect. 3 we introduce the concept of a subdivision and the three

F. Mohammadi
School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
e-mail: fatemeh.mohammadi@bristol.ac.uk

V. Welker (✉)
Fachbereich Mathematik und Informatik, Philipps-Universität Marburg, Hans-Meerwein-Strasse, 35032 Marburg, Germany
e-mail: welker@mathematik.uni-marburg.de

A.M. Bigatti et al. (eds.), *Computations and Combinatorics in Commutative Algebra*, Lecture Notes in Mathematics 2176, DOI 10.1007/978-3-319-51319-5_3

guiding examples which are considered in our text. We define barycentric, edgewise and interval subdivision, the latter being a special case of a subdivision operation studied in differential geometry. In Sect. 4 we introduce the algebraic side of the picture. This side centers around the Stanley-Reisner ring of a simplicial complex Δ. We also introduce the basic enumerative invariants of a simplicial complex relevant for this manuscript—the f- and the h-vector of a simplicial complex and their relation to the Hilbert-series of the Stanley-Reisner ring. With this preparation in Sect. 5 we can provide the known results on the effect of three subdivision operations on the f- and h-vector of a simplicial complex. The following Sect. 6 lists combinatorial and algebraic invariants and properties of simplicial complexes, and describes when they are invariant under subdivisions. Then in Sect. 7 properties of the h-vector that arise after a few subdivisions are studied. This is shown to relate to algebraic properties of Veronese algebras and the analytic behavior of the h-polynomial. In particular, polynomials with real roots are in the spotlight: we explain how they are tied to Koszul algebras and the Charney-Davis conjecture. In Sect. 8 we approach the behavior of f- and h-vectors after a few subdivisions from the point of view of Lefschetz properties of quotients of the Stanley-Reisner ring by a regular sequence of linear forms. Besides exhibiting results we speculate about connections of consequences of the Lefschetz property and real rootedness. Then in Sect. 9 we study the behavior of h- and f- vectors when the number of subdivisions goes to infinity. In addition we present results on the limiting behavior of graded Betti numbers of the Stanley-Reisner ring under subdivisions. Finally, in Sect. 10 we study how subdivisions can be used to define free resolutions of monomial ideals. We show that in this context arrangements of hyperplanes appear as a natural object that induce subdivisions which support resolutions. Therefore, the section also contains an introduction to cellular resolutions and some basics about arrangements of hyperplanes.

We complement our text by a list of problems, whose difficulty reaches from simple to serious research level. We add some Macaulay2 [62] sessions whenever explicit computations are feasible. We assume little background knowledge and refer the reader to the survey article [19] for f- and h-vector theory of simplicial complexes, to [29] and [91] for background on commutative algebra and to [81] for background in algebraic topology.

We do not cover Stanley's theory of local h-vectors. This is an important theory and may relate to many aspects of subdivisions we discuss here. There is an excellent recent survey of old and recent developments in this field by Athanasiadis and we refer the reader to [7] and [6]. Also there are interesting non-simplicial subdivision operations. In particular, cubical subdivision operations appear to be well structured and interesting objects. First results in the spirit of this survey can be found in [101].

2 Abstract and Geometric Simplicial Complexes

An abstract simplicial complex Δ over the ground set Ω is a subset $\Delta \subseteq 2^{\Omega}$ of the powerset of Ω such that $A \subseteq B \in \Delta$ implies $A \in \Delta$. All simplicial complexes that are of interest in this text are over finite ground set Ω and therefore from now on we will always implicitly assume that a simplicial complex is over a finite ground set and hence finite itself. The elements $F \in \Delta$ are called the faces of Δ and the inclusionwise maximal faces are called facets. The dimension of a face F is $\dim F := \#F - 1$ and the dimension $\dim \Delta$ of Δ is $\max_{F\in\Delta} \dim F$.

Besides this combinatorial aspect of simplicial complexes there is also a geometric aspect. For this recall that a geometric $(d-1)$-dimensional simplex in $\mathbb{R}^n$ is the convex hull

$$\mathrm{conv}\{v_1, \dots, v_d\} := \{\sum_{i=1}^{d} \lambda_i v_i \ : \ \begin{array}{c} \lambda_1, \dots, \lambda_d \geq 0 \\ \lambda_1 + \dots + \lambda_d = 1 \end{array}\}$$

of d affinely independent vectors $v_1, \dots, v_d$. A face of $\mathrm{conv}\{v_1, \dots, v_d\}$ is the convex hull of a subset of $\{v_1, \dots, v_d\}$. In particular, any face of $\mathrm{conv}\{v_1, \dots, v_d\}$ is again a geometric simplex. Here we consider the empty set as the convex hull of the empty set and the empty set as a face of a geometric simplex. The 0-dimensional vertices are the singletons $\{v_i\}$ for $1 \leq i \leq d$ and the v_i are called the vertices of the geometric simplex. A geometric simplicial complex Γ is a collection of geometric simplices in some $\mathbb{R}^d$ such that

1. if $\sigma \in \Gamma$ and τ is a face of σ then $\tau \in \Gamma$.
2. if $\sigma, \tau \in \Gamma$ then $\sigma \cap \tau$ is a face of both σ and τ.

Analogous to the case of abstract simplicial complexes, we call the elements of a geometric simplicial complex Γ the faces of Γ. The vertex set of a geometric simplicial complex Γ is the collection of all vertices of faces of Γ.

The vertex scheme $\Delta(\Gamma)$ of Γ is the collection of all vertex sets of simplices $\sigma \in \Gamma$. It is immediate from the above definitions that $\Delta(\Gamma)$ is a simplicial complex. If Δ is an abstract simplicial complex and Γ a geometric simplicial complex such that after a suitable relabeling of the vertices we have that $\Delta(\Gamma) = \Delta$ then we say that Γ is a geometric realization of Δ. We consider the union $\bigcup_{\sigma\in\Gamma} \sigma \subseteq \mathbb{R}^d$ as a topological space with the subspace topology inherited from the Euclidean topology on $\mathbb{R}^d$. It is a well known basic fact from topology that every simplicial complex has a geometric realization and that any two geometric realizations are homeomorphic. Therefore, it is unambiguous to write $|\Delta|$ to denote any geometric realization of Δ. In the sequel we will write Δ_{d-1} for an abstract $(d-1)$-simplex, i.e., the power set of a d-element set, and Γ_{d-1} for the standard geometric $(d-1)$-simplex, i.e., the convex hull $\mathrm{conv}(e_1, \dots, e_d)$ of the d unit vectors $e_1, \dots, e_d$ in $\mathbb{R}^d$.

Given two simplicial complexes $\Delta(1)$ and $\Delta(2)$ such that their geometric realizations $|\Delta(1)|$ and $|\Delta(2)|$ are homeomorphic, the relation between the combinatorial and the algebraic invariants of $\Delta(1)$ and $\Delta(2)$ is subtle and complicated. We will be interested in the situation when $\Delta(1)$ is a *refinement* of $\Delta(2)$. Given two geometric simplicial complexes $\Gamma(1), \Gamma(2)$ in $\mathbb{R}^d$, we say that $\Gamma(1)$ is a subdivision of $\Gamma(2)$ if $\bigcup_{\sigma\in\Gamma(1)} \sigma = \bigcup_{\sigma\in\Gamma(2)} \sigma$ and every simplex $\sigma \in \Gamma(2)$ is a union of simplices in $\Gamma(1)$. Now we say that an abstract simplicial complex $\Delta(1)$ is a subdivision of the abstract simplicial complex $\Delta(2)$ if there are geometric realizations $\Gamma(1)$ of $\Delta(1)$ and $\Gamma(2)$ of $\Delta(2)$ such that $\Gamma(1)$ is a subdivision of $\Gamma(2)$. Note that even though our definition of subdivision is the most common definition in the topology literature, there are more general concepts of subdivision (see e.g. [105]).

3 Subdivisions of Simplicial Complexes

In this section we list a few well known subdivision operations on simplicial complexes. Clearly, this list is not exhaustive and for sure there are many more such operations lurking in the literature. Rather, we concentrate on three subdivision operations. Two of them have been shown to exhibit particularly nice properties in our context and the third is still mostly unexplored (Fig. 1).

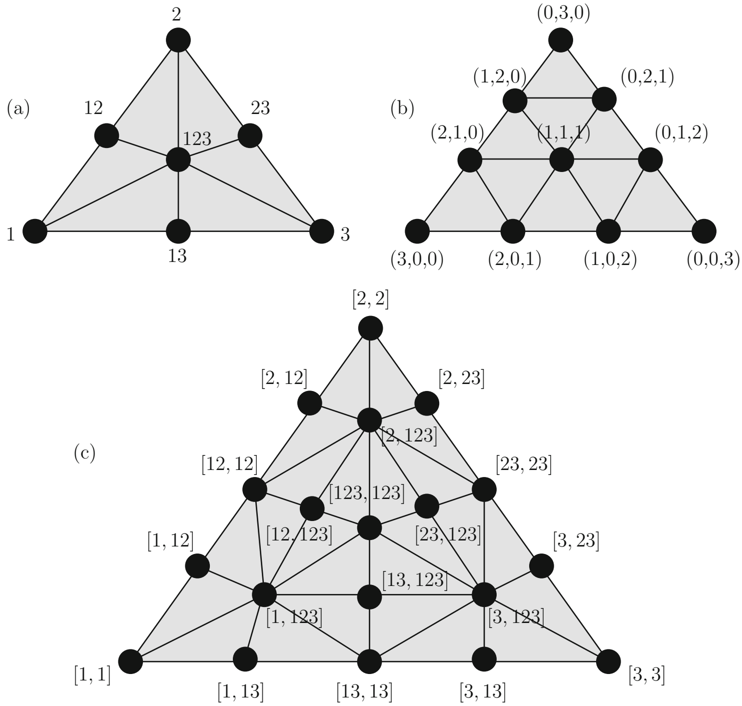


Fig. 1 Barycentric (**a**), 3rd edgewise (**b**), interval (**c**) subdivision of a 2-simplex

3.1 Barycentric Subdivision

The barycentric subdivision of a geometric simplicial complex can be described as follows. Let $v_1, \ldots, v_d \in \mathbb{R}^n$ be affinely independent. For $\emptyset \neq A \subseteq \{v_1, \ldots, v_d\}$ let

$$b_A = \frac{1}{\#A} \sum_{v \in A} v$$

be the barycenter of the simplex conv(A). Then for any chain $\emptyset \subset A_1 \subset \cdots \subset A_l$ of subsets of $\{v_1, \ldots, v_d\}$ let $\sigma_{A_1 \subset \cdots \subset A_l}$ be the convex hull conv$(b_{A_1}, \ldots, b_{A_l})$. For a geometric simplicial complex Γ with vertex scheme $\Delta(\Gamma)$ the set of simplices $\sigma_{A_1 \subset \cdots \subset A_l}$ for chains of subsets $\emptyset \subset A_1 \subset \cdots \subset A_l$ from $\Delta(\Gamma)$ defines a subdivision of Γ which is called the barycentric subdivision of Γ. We write sd(Γ) for the barycentric subdivision of Γ. If Δ is an abstract simplicial complex then define its barycentric subdivision as the simplicial complex sd(Δ) over the ground set $\Delta \setminus \{\emptyset\}$ whose simplices are the subsets $\{A_1, \ldots, A_l\}$ of $\Delta \setminus \{\emptyset\}$ for which with a suitable numbering $A_1 \subset \cdots \subset A_l$. It is easy to verify that $V(\mathrm{sd}(\Gamma))$, the vertex scheme of the barycentric subdivision of a geometric simplicial complex Γ, is (up to relabelling the vertices) the barycentric subdivision of the vertex scheme of Γ, sd$(\Delta(\Gamma))$. Barycentric subdivision is a classical subdivision operation from topology. Some of its many applications can be found in texts on algebraic topology such as [81].

3.2 Edgewise Subdivision

Barycentric subdivision is easily described but has some geometric flaws. In particular, the volumes of the $(d-1)$-simplices in a barycentrically subdivided geometric $(d-1)$-simplex differ. A subdivision that does not have this problem is the edgewise subdivision. It is best explained for geometric $(d-1)$-simplices. The general case then follows after one has checked that it is possible to patch the subdivided simplices. Edgewise subdivisions exist for all natural numbers $r \geq 1$. Let $r \geq 1$ then the rth edgewise subdivision of the $(d-1)$-simplex Γ_{d-1} is defined as follows. Consider the rth dilation $r\Gamma_{d-1}$ of the $(d-1)$ simplex with vertices the unit basis vectors in $\mathbb{R}^d$. The integer points in $r\Delta_{d-1}$ are the d-tuples $(i_1, \ldots, i_d)$ of non-negative integers such that $i_1 + \cdots + i_d = r$. We write $\Omega_{d,r}$ for this set. Now we make a change of coordinates and map $(i_1, \ldots, i_d)$ to $\iota(i_1, \ldots, i_d) = (i_1, i_1 + i_2, \ldots, i_1 + \cdots + i_d)$. We subdivide $r\Gamma_{d-1}$ by simplices conv(A) where $A \subseteq \Omega_{d,r}$ and either $\iota(v - v') \in \{0,1\}^d$ or $-\iota(v - v') \in \{0,1\}^d$ for all $v, v' \in A$. Now the rth edgewise subdivision of Γ_{d-1} is obtained from this subdivision of $r\Gamma_{d-1}$ by dilating with factor $\frac{1}{r}$. In general, the rth edgewise subdivision $\Gamma^{\langle r \rangle}$ is obtained from Γ by applying it to every simplex in Γ. The geometric rth edgewise subdivision clearly induces a subdivision on the vertex scheme of Γ. This way we can speak of the rth edgewise subdivision $\Delta^{\langle r\rangle}$ of an abstract simplicial complex Δ. The term rth edgewise subdivision is motivated by the fact that edges of Γ are subdivided into r equal pieces in $\Gamma^{\langle r\rangle}$. Edgewise subdivision first appeared in a paper by Freudenthal [55] but has found numerous applications in discrete geometry [48], K-theory [61] or commutative algebra [27]. We explain the latter in more detail later in the text.

3.3 Interval Subdivision

This subdivision operation is easiest described starting with an abstract simplicial complex Δ. First, we consider $\Delta\setminus\{\emptyset\}$ as a partially ordered set ordered by inclusion. Let Ω be the set of formal symbols $[A, B]$ for any inclusion $A \subseteq B$ in $\Delta \setminus \{\emptyset\}$. Note $A = B$ is permitted. Now we consider the partial order on the intervals induced by containment and define $\mathrm{Int}(\Delta)$ to be the simplicial complex of all chains of intervals in this order. By Walker [117, Theorem 6.1. (a)] we obtain that $\mathrm{Int}(\Delta)$ is a subdivision of Δ. Indeed this subdivision also appears as the special case $N = 1$ of the subdivision from [32, Fig. 1.2].

Problem 1 Prove that $\mathrm{Int}(\Delta)$ coincides with the subdivision from [33, Fig. 1.2] if one sets $N = 1$ in [33].

4 The Stanley-Reisner Ring

The algebraic object usually associated to a simplicial complex Δ is the face or Stanley-Reisner ring $\mathbb{K}[\Delta]$ of Δ. Let Δ be a simplicial complex over ground set Ω. The ring $\mathbb{K}[\Delta]$ is the quotient of the polynomial ring $\mathbb{K}[x_\omega \,:\, \omega \in \Omega]$ over the field $\mathbb{K}$ and the Stanley-Reisner ideal I_Δ generated by the $\underline{\mathbf{x}}_N := \prod_{i\in N} x_i$ for minimal non-faces N of Δ. Note that a subset $N \subseteq \Omega$ is a minimal non-face of Δ if $N \notin \Delta$ and all proper subsets of N are in Δ.

Since we will have to deal with monomials and ideals generated by monomials more often in this text, we introduce some notation here. A monomial in $\mathbb{K}[x_\omega \,:\, \omega \in \Omega]$ is a product $\prod_{\omega\in\Omega} x_\omega^{\alpha_\omega}$ for some non-negative integers α_ω. We also write $\underline{\mathbf{x}}^\alpha$ for $\prod_{\omega\in\Omega} x_\omega^{\alpha_\omega}$ where $\alpha = (\alpha_\omega)_{\omega\in\Omega}$. In this notation we have for the squarefree monomials $\underline{\mathbf{x}}_N$ introduced above the identity $\underline{\mathbf{x}}_N = \underline{\mathbf{x}}^\alpha$ for $\alpha = \sum_{\omega\in N} e_\omega$ for the unit basis vectors $(e_\omega)_{\omega\in\Omega}$ of $\mathbb{R}^\Omega$. The support $\mathrm{supp}(\underline{\mathbf{x}}^\alpha)$ of a monomial $\underline{\mathbf{x}}^\alpha$ is the set $\{\omega \,:\, \alpha_\omega \neq 0\}$. An ideal I in $\mathbb{K}[x_\omega \,:\, \omega \in \Omega]$ is called a monomial ideal if it is generated by monomials. The Stanley-Reisner ideals are exactly the monomial ideals generated by squarefree monomials $\underline{\mathbf{x}}_N$ for some collection of subsets $N \subseteq \Omega$.

http://www.springer.com/978-3-319-51318-8

Computations and Combinatorics in Commutative Algebra
EACA School, Valladolid 2013
Bigatti, A.M.; Gimenez, P.; Sáenz-de-Cabezón, E. (Eds.)
2017, VIII, 127 p. 25 illus., 16 illus. in color., Softcover
ISBN: 978-3-319-51318-8