A Divide and Conquer Method to Compute Binomial Ideals

Deepanjan Kesh[*]
Indian Institute of Technology, Kanpur
Kanpur, India
deepkesh@cse.iitk.ac.in

Shashank K Mehta
Indian Institute of Technology, Kanpur
Kanpur, India
skmehta@cse.iitk.ac.in

ABSTRACT

A binomial is a polynomial with at most two terms. In this paper, we give a *divide-and-conquer* strategy to compute binomial ideals. This work is motivated by the fact that any algorithm to compute binomial ideals spends a significant amount of time computing Gröbner basis and that Gröbner basis computation is very sensitive to the number of variables in the ring. The divide and conquer strategy breaks the problem into subproblems in rings of lesser number of variables than the original ring. We apply the framework on 4 problems – radicals, cellular decomposition, prime decomposition and saturation.

1. INTRODUCTION

Consider the polynomial ring $k[x_1, \ldots, x_n]$. A **binomial** in such a ring is a polynomial of the form

$$c \cdot \mathbf{x}^\alpha + d \cdot \mathbf{x}^\beta,$$

where $c, d \in k$ and $\alpha, \beta \in \mathbb{N}^n$. An ideal in the polynomial ring which has a generating set comprising only of binomials is called a **binomial ideal**. In this paper, we will be concerned with computing various binomial ideals.

Binomial ideals, unlike general polynomial ideals, possess rich combinatorial structure which can be exploited while computing various structures derived from them, for example Gröbner bases, primary decomposition, and associated primes [15, 9]. Pure difference binomials are binomials of the form $\mathbf{x}^\alpha - \mathbf{x}^\beta$. The varieties of pure difference prime binomial ideals are exactly the toric varieties. Hence, such ideals are also known as toric ideals [6, 5]. There is a large literature studying applications and computations of toric ideals [12, 1]. Moreover, quotients of polynomial rings by pure difference binomial ideals form commutative semigroup rings [8].

Apart from a purely academic interest in the subject of binomial ideals, their study is also motivated by the fact that they are often encountered in interesting problems in diverse fields. These include solving integer programs [10, 2, 16, 14], computing primitive partition identities [12, Chapters 6,7], and solving scheduling problems [13]. In algebraic statistics, closures of discrete exponential families have been identified with nonnegative toric varieties [7].

The theory of binomial ideals was developed in a seminal paper by Eisenbud and Sturmfels [5]. Their paper not only showed various properties of binomial ideals – for example, the radicals and associated primes of binomial ideals are themselves binomial ideals – but they also show how to compute these structures.

In this paper, we present a general framework to compute several of such binomial ideals, namely radical, saturation, minimal primes and cellular decompositions. This work is motivated by two crucial observations – (i) most of these computations involve computing Gröbner basis of certain ideals, and (ii) Buchberger's algorithm to compute Gröbner basis is very sensitive to the number of variables in the underlying polynomial ring. In light of these observations, we propose a *divide-and-conquer* technique to solve the aforementioned problems, with the hope that this strategy can also be applied to host of other problems related to binomial ideals, like computing associated primes, primary decomposition, primary component, and so on. The essence of the strategy is the following. Consider the polynomial ring $k[x_1, \ldots, x_n]$, and a binomial ideal $I \subseteq k[x_1, \ldots, x_n]$. We compute the image of I under the natural homomorphism in the derived rings $k[x_2, \ldots, x_n]$ and $k[x_1^{\pm}, x_2, \ldots, x_n]$ and perform the same computation on these ideals. Then we "lift" the results in the original ring and combine them to compute a solution of the original problem. Both these rings are isomorphic to polynomial rings with one less variable [11], hence Gröbner basis (actually such basis does not exist in these new rings but we use a variant for the computations) can be computed more efficiently.

The paper has been arranged as follows. Section 2 deals with some basic facts about rings and ideals, and discusses irreducible and primary decompositions in the context of Noetherian rings. In the next section, we define two maps from ideals of $k[x_1, \ldots, x_n]$ to the ideals of the derived rings, and state some useful properties. These two maps form the basis of the reduction of the problem into the subproblems, discussed earlier. Section 4 contains the main contribution of the paper – discussion of the proposed divide-and-conquer framework. In Section 5, we use this framework to compute radical, cellular decomposition, minimal primes, and saturation of binomial ideals.

[*]Support from IMPECS is acknowledged.

ISSAC 2012 Grenoble, France

2. RINGS AND IDEAL BASICS

In this paper, we will only consider commutative rings with unity. In this section, we review a few definitions and results about rings and ideals which will be used later in the paper. Also, note that k will denote an algebraically closed field.

Definition 1. [4] An ideal I of a ring R is **prime**, if I is a proper ideal, and $fg \in I$ implies $f \in I$ or $g \in I$.

Definition 2. **Radical** of an ideal I is an ideal given by $\sqrt{I} = \{ \ r \mid r^m \in I, \ m \geq 0 \ \}$. An ideal is said to radical, if it is its own radical.

We now have two simple observations regarding radical ideals.

Observation 1. *Prime ideals are radical.*

Observation 2. *$I_1 \subseteq I_2$ implies that $\sqrt{I_1} \subseteq \sqrt{I_2}$.*

Definition 3. A ring is said to be **Noetherian** if every strictly ascending chain of ideals in the ring

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$$

terminates.

The next observation presents an alternate view of Noetherian rings.

Observation 3. *A ring is Noetherian if and only if every ideal of the ring is finitely generated.*

Definition 4. Let R be a ring, $r \in R$ be a non-zero-divisor and $I \subseteq R$ be an ideal. Then, **saturation** of I w.r.t. r is the ideal given by $I : r^\infty = \{ \ s \mid sr^j \in I, \text{ for some } j \geq 0 \ \}$. Similarly, we define $I : r^n$ as the ideal $\{ \ s \mid sr^n \in I \ \}$.

Definition 5. [4] Given a ring R, and a multiplicatively closed subset $U \subset R$ not containing zero, we define the **localization** of R at U, written as $R[U^{-1}]$, to be the set of equivalence classes of pairs (r, u) with $r \in R$ and $u \in U$ with the equivalence relation $(r, u) \sim (r', u')$ if there is an element $v \in U$ such that $v(u'r - ur') = 0$ in R. The equivalence class of (r, u) is denoted by r/u. We make $R[U^{-1}]$ into a ring by defining

$$\frac{r}{u} + \frac{r'}{u'} = \frac{u'r + ur'}{uu'} \text{ and } r\frac{r'}{u} = \frac{rr'}{u}$$

for $r, r' \in R$, and $u, u' \in U$.

Definition 6. The quotient ring

$$k[x_1, \dots, x_n, y_1, \dots, y_m] / \langle \ x_1y_1 - 1, \dots, x_my_m - 1 \ \rangle,$$

for $1 \leq m \leq n$, is called a **partial Laurent polynomial ring** and it is denoted by $k[x_1, \dots, x_n, x_1^{-1}, \dots, x_m^{-1}]$, where x_i^{-1} corresponds to y_i for $1 \leq i \leq m$. If $m = n$, then it is called a **Laurent polynomial ring**.

We now make a small observation associating localization and Laurent polynomial rings.

Observation 4. *Let $R = k[x_1, \dots, x_n]$ and U be the set of all monomials generated by the variables $\{x_1, \dots, x_m\}$, $1 \leq m \leq n$. Then, $R[U^{-1}]$ is isomorphic to the partial Laurent polynomial ring $k[x_1, \dots, x_n, x_1^{-1}, \dots, x_m^{-1}]$. It is also isomorphic to $R'[x_{m+1}, \dots, x_n]$ where R' is the Laurent polynomial ring $k[x_1, \dots, x_m, x_1^{-1}, \dots, x_m^{-1}]$*

Lemma 1 (corollary 2.3, [4]). *A localization of a Noetherian ring is Noetherian.*

The above lemma, and the fact that polynomial rings are Noetherian implies that partial Laurent polynomial rings are also Noetherian.

For convenience in describing the algorithm in section 4, we present an alternative notation for partial Laurent polynomial rings. Let V be the set of variables $\{x_1, x_2, \dots, x_n\}$, and $L = \{x_{i_1}, x_{i_2}, \dots, x_{i_m}\}$ be a subset of V. Then, we will denote the partial Laurent polynomial ring $k[x_1, \dots, x_n, x_{i_1}^{-1}, \dots, x_{i_m}^{-1}]$ by the tuple (k, V, L).

2.1 Irreducible decompositions

Definition 7. [3] Let R be a ring. An ideal $I \subseteq R$ is said to be **irreducible** if $I = I_1 \bigcap I_2$ implies $I = I_1$ or $I = I_2$.

Definition 8. An **irreducible decomposition** of an ideal I is an expression of I as the intersection of irreducible ideals.

Lemma 2. *If an ideal I does not have an irreducible decomposition, then $\exists$ an ideal $J \supsetneq I$ which also does not have an irreducible decomposition.*

Proof. Let I be an ideal which does not have an irreducible decomposition. This also means that I is not irreducible. Consider the set of decompositions of I as the intersection of two ideals. This is certainly non-empty as it has $\{I \bigcap R\}$. Since I is not irreducible, it has a decomposition $I = I_1 \bigcap I_2$ s.t. both of them properly contain I. Moreover, at least one of I_1 and I_2 does not have an irreducible decomposition, otherwise I will have an irreducible decomposition. J is that ideal. □

Theorem 1. *Every ideal in a Noetherian ring has an irreducible decomposition.*

Proof. If not, then using Lemma 2, we can build an strict ascending chain of ideals, each of which is not expressible as the intersection of irreducible ideals. But this is not possible as the ring is Noetherian. □

2.2 Primary Ideals

Definition 9. An ideal I in a ring R is said to be **primary** if $fg \in I$ implies either $f \in I$ or $g^n \in I$, for some $n > 0$. Equivalently, I is **primary** if $fg \in I$ implies that either $f^m \in I$ or $g^n \in I$ for some $m, n > 0$.

Lemma 3. *Let I be an ideal in a Noetherian ring R. If $fg \in I$, then there exists an $n \geq 0$ such that $\langle \ f \ \rangle \bigcap \langle \ g^n \ \rangle \subseteq I$*

Proof. As R is Noetherian, $\exists n \geq 0$ s.t. $I : g^n = I : g^\infty$. Let $h \in \langle \ f \ \rangle \bigcap \langle \ g^n \ \rangle$. This implies $h = r_2g^n = r_1f (r_1, r_2 \in R) \implies hg = r_2g^{n+1} = r_1fg \in I$. This shows that $r_2 \in I : g^{n+1} = I : g^n$ and hence $h \in I$. □

Lemma 4. *Every irreducible ideal in a Noetherian ring is primary.*

Proof. Let I be an irreducible ideal, and $fg \in I$, where $f \notin I$. Using Lemma 3, we know that

$$(I + \langle \ f \ \rangle) \bigcap (I + \langle \ g^n \ \rangle) = I.$$

Since $f \notin I$, $I + \langle \ f \ \rangle$ is strictly larger than I. Hence $I + \langle \ g^n \ \rangle = I$, which implies that $g^n \in I$. □

Definition 10. A **primary decomposition** of an ideal I is an expression of I as an intersection of primary ideals –

$$I = \bigcap_{i=1}^{r} Q_i,$$

where Q_is are primary ideals. It is called **minimal** or **irredundant** if the $\sqrt{Q_i}$ are all distinct and $Q_i \not\supseteq \bigcap_{j\neq i} Q_j$.

THEOREM 2. *Every ideal in a Noetherian ring has a primary decomposition.*

PROOF. This follows from Theorem 1 and Lemma 4. □

LEMMA 5. *Radical of intersection of ideals is intersection of radicals of the ideals.*

PROOF. Let the ideals involved be $I_1, I_2, \dots, I_n$, and we want to show that

$$\sqrt{I_1 \bigcap I_2 \bigcap \dots \bigcap I_n} = \sqrt{I_1} \bigcap \sqrt{I_2} \bigcap \dots \bigcap \sqrt{I_n}.$$

Let $f \in \sqrt{\bigcap_i I_i}$. This implies that $f^m \in \bigcap_i I_i \implies f^m \in I_i, \forall i \implies f \in \sqrt{I_i}, \forall i$. Thus, $f \in \bigcap_i \sqrt{I_i}$. So, we have

$$\sqrt{I_1 \bigcap I_2 \bigcap \dots I_n} \subseteq \sqrt{I_1} \bigcap \sqrt{I_2} \bigcap \dots \sqrt{I_n}.$$

To show the converse, let $f \in \bigcap_i \sqrt{I_i}$. Then, it is easy to see that there exists an $m \geq 0$, such that $f^m \in \bigcap_i I_i$. This implies that $f \in \sqrt{\bigcap_i I_i}$. Thus, we have

$$\sqrt{I_1} \bigcap \sqrt{I_2} \bigcap \dots \sqrt{I_n} \subseteq \sqrt{I_1 \bigcap I_2 \bigcap \dots I_n}.$$

□

LEMMA 6. *An ideal is primary iff its radical is prime.*

PROOF. **(if)** Let I be an ideal such that $\sqrt{I}$ is prime. Let $fg \in I \implies fg \in \sqrt{I}$. So, either $f \in \sqrt{I}$ or $g \in \sqrt{I}$. Hence, either $f^m \in I$ or $g^n \in I$, for $m, n \geq 0$. Thus, I is primary.

(only if) Let I be a primary ideal. Let $fg \in \sqrt{I}$ and $f \notin \sqrt{I}$. So for some $n > 0$, $f^n g^n \in I$ and $f^k \notin I$ for all k. As I is primary, there is some m such that $g^{nm} \in I$. Hence $g \in \sqrt{I}$.

□

LEMMA 7. *If I and J are primary and $\sqrt{I} = \sqrt{J}$, then $I \bigcap J$ is also primary.*

PROOF. Let $fg \in I \bigcap J$, and $f^j \notin I \bigcap J$ for all $j > 0$. We need to show that $g^n \in I \bigcap J$, for some $n > 0$. We claim that $f^i \notin I, \forall i > 0$. Otherwise, $f \in \sqrt{I} = \sqrt{J}$ implies $f^m \in I \bigcap J$ for some $m > 0$, which contradicts the assumption. As $f^i \notin I, \forall i$ and I is primary, we deduce that $g^{n_1} \in I$ for some $n_1 > 0$. From a similar argument $g^{n_2} \in J$ for some $n_2 > 0$. Hence the proof. □

THEOREM 3. *Every ideal in a Noetherian ring has a minimal primary decomposition.*

PROOF. Theorem 2 gives us a primary decomposition for any ideal. Repeated application of Lemma 7 gives us a primary decomposition such that all the radicals are distinct. Lastly, we can eliminate all the redundant ideals in the intersection to get a minimal primary decomposition. □

THEOREM 4. *Every radical ideal in a Noetherian ring has a prime decomposition.*

PROOF. Let I be a radical ideal in a Noetherian ring. From Theorem 2, I has a primary decomposition –

$$I = Q_1 \bigcap Q_2 \bigcap \dots \bigcap Q_n.$$

Then, applying Lemma 5, we have

$$\sqrt{I} = \sqrt{Q_1} \bigcap \sqrt{Q_2} \bigcap \dots \bigcap \sqrt{Q_n}.$$

Now, observing that $\sqrt{Q_i}$s are prime (Lemma 6), we have the proof. □

3. TWO RING HOMOMORPHISMS

3.1 Modulo Map

Let r be an element of a Noetherian ring R. Then $\theta : R \to R/\langle\ r\ \rangle$ denotes the natural homomorphism

$$\theta(a) = [a] = a + \langle\ r\ \rangle,\ \forall a \in R.$$

This induces a map Θ from the ideals in R containing r and the ideals of $R/\langle r \rangle$ as follows -

$$\Theta(I) = \{\ [a] \mid a \in I\ \},$$

where $I \subseteq R$ is an ideal containing r.

Similarly, we define a map Θ^{-1} from the ideals of $R/\langle\ r\ \rangle$ to the ideals of R containing r as follows

$$\Theta^{-1}(J) = \{\ x \mid [x] \in J\ \},$$

where $J \subseteq R/\langle\ r\ \rangle$ is an ideal.

LEMMA 8. *Θ is a bijection.*

PROOF. We will first show that for any ideal $I \subseteq R$ containing r, $\Theta^{-1}(\Theta(I)) = I$. From the definitions, we observe that $I \subseteq \Theta^{-1}(\Theta(I))$. Now let $x \in \Theta^{-1}(\Theta(I))$. So $[x] \in \Theta(I)$ and hence, there exists $s \in I$ such that $x - s = tr$, for some $t \in R$. Since $r, s \in I$, $x \in I$.

To show that $\Theta(\Theta^{-1}(J)) = J$ for every ideal J in $R/\langle\ r\ \rangle$, observe from the definitions that $J \subseteq \Theta(\Theta^{-1}(J))$. Now, let $[x] \in \Theta(\Theta^{-1}(J))$. So for some $t \in R$, $x + rt \in \Theta^{-1}(J)$. Hence $[x + rt] \in J$. But, as $[x] = [x + rt]$, so $[x] \in J$. □

It is directly verifiable from the definitions that Θ and Θ^{-1} preserve set inclusion.

LEMMA 9. *Θ and Θ^{-1} map primes to primes.*

PROOF. Let I be a prime ideal of R containing r. Also, let $[x][y] \in \Theta(I)$. So $[xy] \in \Theta(I)$ and hence $xy \in I$ (Lemma 8). Being a prime ideal, I contains either x or y. Without loss of generality, let us assume that $x \in I$. So $[x] \in \Theta(I)$. This implies that $\Theta(I)$ is prime.

Let J be any prime ideal in $R/\langle\ r\ \rangle$. Let $I = \Theta^{-1}(J)$. Also, let $xy \in I$. Then, $[x][y] = [xy] \in J$. Since J is prime, without loss of generality we can assume that $[x] \in J$. Hence, $x \in I$, establishing that I is also prime. □

LEMMA 10. *Θ distributes over finite intersections. Similarly, Θ^{-1} also distributes over finite intersections.*

PROOF. Let R be a ring and $I_1, I_2, \dots, I_n \subseteq R$ be ideals, each containing r. We would like to show that

$$\Theta\left(\bigcap_i I_i\right) = \bigcap_i \Theta\left(I_i\right).$$

Let $[f] \in \Theta\left(\bigcap_i I_i\right)$. This implies that $\exists g \in \bigcap_i I_i$ s.t. $[g] = [f]$. Thus, $f = g + hr$, for some $h \in R$. So, $f \in \bigcap_i I_i$ or $f \in I_i, \forall i$. Hence $[f] \in \Theta(I_i)$ or $[f] \in \bigcap_i \Theta\left(I_i\right)$.

As for the other direction, let $[f] \in \bigcap_i \Theta\left(I_i\right)$. Hence $[f] \in \Theta\left(I_i\right), \forall i \implies f \in I_i, \forall i$ (Lemma 8). So, $[f] \in \Theta\left(\bigcap_i I_i\right)$.

To prove the second claim, consider the ideal

$$E = \Theta^{-1}(J_1 \bigcap J_2 \bigcap \cdots),$$

where J_j are ideals in $R/\langle\ r\ \rangle$. Let $I_j = \Theta^{-1}(J_j)$. So, we have $E = \Theta^{-1}(\Theta(I_1) \bigcap \Theta(I_2) \bigcap \cdots)$. From the preceding discussion, we have $E = \Theta^{-1}(\Theta(I_1 \bigcap I_2 \bigcap \cdots))$. Finally, applying Lemma 8, we have $E = I_1 \bigcap I_2 \bigcap \cdots = \Theta^{-1}(J_1) \bigcap \Theta^{-1}(J_2) \bigcap \cdots$. □

Lemma 11. *In a Noetherian ring* $\Theta(\sqrt{I}) = \sqrt{\Theta(I)}$

Proof. From Theorem 4, we have $I \subseteq \sqrt{I} = \bigcap_i P_i$, where P_is are primes. So, we have

$$\Theta(I) \subseteq \Theta(\sqrt{I}) = \Theta(\bigcap_i P_i) = \bigcap_i \Theta(P_i)$$

Using Lemma 9 and the fact that intersection of prime ideals is radical, we know that $\Theta(\sqrt{I})$ is a radical ideal. So, we have $\sqrt{\Theta(I)} \subseteq \Theta(\sqrt{I})$.

Conversely, as $\sqrt{\Theta(I)}$ is radical, we have

$$\sqrt{\Theta(I)} = \bigcap_i P_i,$$

where the P_i's are some primes in the modulo ring. So, we have $\Theta^{-1}(\sqrt{\Theta(I)}) = \bigcap_i \Theta^{-1}(P_i)$. This, shows that $\Theta^{-1}(\sqrt{\Theta(I)})$ is radical and contains I. Hence $\Theta(\sqrt{I}) \subseteq \sqrt{\Theta(I)}$. □

Lemma 12. $\Theta^{-1}(\langle\ [f_1], \dots, [f_n]\ \rangle) = \langle\ f_1, \dots, f_n\ \rangle + \langle\ r\ \rangle$

Proof. Let $f \in \Theta^{-1}(\langle\ [f_1], \dots, [f_n]\ \rangle)$. So, we have $[f] \in \langle\ [f_1], \dots, [f_n]\ \rangle$. So, f can be expressed as $f - \sum_i g_i f_i = gr$, for some g_is and r in the ring. This shows that f belongs to the R.H.S. The other direction can be shown in a similar fashion. □

3.2 Localization map

Let r be a nonzero-divisor of a Noetherian ring R. Let U denote the set of all powers of r

$$U = \left\{\ r^i \mid i \geq 0\ \right\}.$$

Since r is not nilpotent, U does not contain zero. U is also multiplicatively closed. Therefore $R[U^{-1}]$ is well defined.

Let $\phi : R \rightarrow R[U^{-1}]$ be the natural homomorphism given by $\phi(a) = a/1$, $\forall a \in R$. We define a map, Φ, induced by ϕ, from the ideals in R saturated w.r.t. r to the ideals of $R[U^{-1}]$ as follows

$$\Phi(I) = \langle\ \{\ a/1 \mid a \in I\ \}\ \rangle,$$

where $I \subseteq R$ is an ideal saturated w.r.t. r. We now present some properties of Φ.

Lemma 13. *For any ideal $I \subseteq R$ saturated w.r.t. r, $x/r^n \in \Phi(I)$, for some $n \geq 0$ implies $x \in I$. Conversely, $x \in I$ implies $x/r^n \in \Phi(I), \forall n \geq 0$.*

Proof. Let $x/r^n \in \Phi(I)$. Then, by the construction of $\Phi(I)$, there exists b_i's in I such that $x/r^n = \sum_i (c_i/r^{k_i})(b_i/1)$ for some c_i's in R and non-negative k_is. As r is a nonzero-divisor, the above identity implies that $r^m x - \sum_i r^{k_i'} c_i b_i \in I$, for suitable m, k_i's $\in \mathbb{N}$. This implies that $r^m x \in I$, and using the fact that I is saturated with respect to r, we have $x \in I$.

To prove the converse, let $x \in I$. Then we have $\phi(x) = x/1 \in \Phi(I)$ and hence, $x/r^n \in \Phi(I)$, $\forall n \in \mathbb{N}$. □

Now, we will define a map, Φ^{-1}, from the ideals in $R[U^{-1}]$ to the ideals in R which are saturated with respect to r.

$$\Phi^{-1}(J) = \left\{\ a \mid \frac{a}{r^k} \in J,\ k \geq 0\ \right\}.$$

From their respective definitions, it is trivial to see that Φ and Φ^{-1} preserve set inclusion.

Observation 5. *Φ^{-1} is a map from the ideals of $R[U^{-1}]$ to the ideals of R which are saturated with respect to r.*

Proof. Suppose $r^m c \in \Phi^{-1}(J)$. So from the definition of the map $r^m c/r^k \in J$, for some $k \geq 0$. Since J is an ideal in $R[U^{-1}]$, $c/1 \in J$. Hence, from the definition of Φ^{-1}, we have $c \in \Phi^{-1}(J)$. □

We will now establish that Φ is a bijection.

Lemma 14. *$\Phi(\Phi^{-1}(J)) = J$ for all ideals J in $R[U^{-1}]$.*

Proof. Let $a/r^k \in J$. Then, $a \in \Phi^{-1}(J)$ and hence $a/1 \in \Phi(\Phi^{-1}(J))$. But $\Phi(\Phi^{-1}(J))$ is an ideal in $R[U^{-1}]$, so $a/r^k \in \Phi(\Phi^{-1}(J))$.

Now suppose $a/r^k \in \Phi(\Phi^{-1}(J))$. From Lemma 13, we have $a \in \Phi^{-1}(J)$ or $a/r^n \in J$, for some $n \in \mathbb{N}$. So $a/r^k \in J$. □

Lemma 15. *$\Phi^{-1}(\Phi(I)) = I$ for all ideals I in R which are saturated with respect to r.*

Proof. If $a \in I$, then $a/1 \in \Phi(I)$. So, $a \in \Phi^{-1}(\Phi(I))$.

Now, suppose $a \in \Phi^{-1}(\Phi(I))$. So $a/r^k \in \Phi(I)$ for some $k \in \mathbb{N}$. From Lemma 13, we have $a \in I$. □

Lemma 16. *Φ and Φ^{-1} map primes to primes.*

Proof. Let $I \subsetneq R$ be a prime ideal which is saturated with respect to r. We want to show that $\Phi(I)$ is prime. Let $(x/r^m)(y/r^n) \in \Phi(I)$. So $xy \in \Phi^{-1}(\Phi(I)) = I$. Since I is prime, I contains x or y. Without loss of generality, let us assume that $x \in I$. Hence, from Lemma 13, we have $\frac{x}{r^m} \in \Phi(I)$.

Now suppose J is a prime ideal in $R[U^{-1}]$. Let $xy \in \Phi^{-1}(J)$. So for some m, we have $(xy)/r^m \in J$ or $(x/r^m)(y/1) \in J$. As J is prime, without loss of generality, let us assume that $\frac{x}{r^m} \in J$. This implies $x \in \Phi^{-1}(J)$. □

Lemma 17. *Φ and Φ^{-1} distribute over intersections.*

Proof. Let $I_1, I_2, \dots$ be ideals in R, each saturated with respect to r. Then, $x/r^n \in \bigcap_i \Phi(I_i) \iff x/r^n \in \Phi(I_i), \forall i \iff x \in \Phi^{-1}(\Phi(I_i)) = I_i, \forall i \iff x \in \bigcap_i I_i \iff x/r^n \in \Phi(\bigcap_i I_i)$.

Next consider the ideals $J_1, J_2, \dots$ in $R[U^{-1}]$. So, $\Phi^{-1}(\bigcap_i J_i) = \Phi^{-1}(\bigcap_i \Phi(\Phi^{-1}(J_i))) = \Phi^{-1}(\Phi(\bigcap_i \Phi^{-1}(J_i))) = \bigcap_i \Phi^{-1}(J_i)$, where the second equality is due to the result in the previous paragraph. □

LEMMA 18. $\Phi(I : x^\infty) = \Phi(I) : x^\infty$.

PROOF. It follows directly from the definitions. □

LEMMA 19. *In a Noetherian ring* $\Phi(\sqrt{I}) = \sqrt{\Phi(I)}$

PROOF. The proof is identically same as that of Lemma 11 when Θ is replaced by Φ and references are suitably replaced. □

LEMMA 20. $\Phi^{-1}(\langle\ f_1/r^{a_1}, \ldots, f_n/r^{a_n}\ \rangle) = \langle\ f_1, \ldots, f_n\ \rangle : r^\infty$

PROOF. Let $f \in \Phi^{-1}(\langle\ f_1/r^{a_1}, \ldots, f_n/r^{a_n}\ \rangle)$. This implies that $f/r^k \in \langle\ f_1/r^{a_1}, \ldots, f_n/r^{a_n}\ \rangle$, for some suitable k. Hence, $f/r^k = \sum_i (g_i/r^{b_i})(f_i/r^{a_i})$. By suitable cross-multiplication, we will have $f \in \langle\ f_1, \ldots, f_n\ \rangle : r^\infty$. One must observe that the ideal being saturated w.r.t. to r is being crucially exploited in the proof.

The other direction can be similarly proved. □

4. A DIVIDE-AND-CONQUER METHOD

In this section, we focus on the main objective of this paper. We present a general algorithm (Algorithm 1) based on *divide-and-conquer* technique which is useful in computing several binomial ideals associated with a given binomial ideal. The algorithm takes as input the following 3 objects (i) A ring (k, X, L), (ii) A set of binomials, S, generating an ideal I, and (iii) A set of variables $V \subseteq X \setminus L$ called *forbidden* set. The objective of the algorithm is to compute $\mathsf{A}(\langle\ S\ \rangle)$, where A is some object associated with the binomial ideal I. In this paper, we demonstrate how to use Algorithm 1 to solve the following 4 problems – (i) Radical of a binomial ideal, (ii) Cellular decomposition of a binomial ideal, (iii) Minimal Primes of a binomial ideal, and (iv) Saturation of a binomial ideal w.r.t. all the variables in the ring.

We will restate, from the introduction, the two crucial observations behind this algorithm – (i) most computations involving binomial ideals compute Gröbner basis of certain ideals, and (ii) Buchberger's algorithm to compute Gröbner basis is very sensitive to the number of variables in the underlying polynomial ring. The motivation behind the algorithm is to divide the problem suitably into smaller subproblems, solve these subproblems in rings with less variables than the original ring, and combine these results to solve the original problem.

Let $x \in (X \setminus L) \setminus V$, and consider the maps (i) $\Theta : (k, X, L) \to (k, X\setminus\{x\}, L)$, (ii) $\Phi : (k, X, L) \to (k, X, L \bigcup \{x\})$, and (iii) $f : (k, X, L) \to (k, X, L)$ which depends on the problem $\mathsf{A}()$. The reduction step involves solution of the subproblems (i) $\mathsf{A}(\Theta(I + \langle\ x\ \rangle))$, in ring $(k, X \setminus \{x\}, L)$ and forbidden set V, (ii) $\mathsf{A}(\Theta(I : x^\infty))$, in ring $(k, X, L \bigcup \{x\})$ and forbidden set V, (iii) $\mathsf{A}(f(I))$ in ring (k, X, L) and forbidden set $V \cup \{x\}$. The first subproblem is in a ring with one less variable compared to the original ring. In the case of the second subproblem, Gröbner bases are not defined in the context of partial Laurent polynomial rings (k, X, L). But pseudo Gröbner bases [11], briefly discussed later in this section, can effectively substitute for Gröbner bases for binomial ideal computations. The time complexity of the algorithm to compute pseudo Gröbner basis was shown in that paper to be dependent on the number of variables in $X \setminus L$. Hence, this subproblem is also justifiably "smaller".

The role of the forbidden set of variables is that reduction must not be done with respect to these variables. If $V = X \setminus L$, then the computation $A(I)$ must be easy to perform without further reduction. In addition, the third subproblem should be such that it does not require the computation of a Gröbner basis since in this case the ring is same as in the original problem and involves no reduction in ring size. Here is a motivating example to justify the use of forbidden set. Suppose we want to compute the saturation, $I : (x_1 \cdots x_n)^\infty$, while I is already saturated w.r.t. x_1, x_2. Then reduction with these variables is futile. Hence we can put these variables in the forbidden set.

Next, the algorithm computes the inverse images of $\mathsf{A}(\Theta(I + \langle\ x\ \rangle))$ and $\mathsf{A}(\Phi(I : x^\infty))$ in the original ring (k, X, L). In the applications discussed in the next section, $\mathsf{A}(I)$ is either an ideal (as in the case of radical of I) or a set of ideals (as in the case of minimal primes of I). Hence these images are well defined. Abusing the notations, we denote these images respectively by $\Theta^{-1}(\mathsf{A}(\Theta(I + \langle\ x\ \rangle))$ and $\Phi^{-1}(\mathsf{A}(\Phi(I : x^\infty))$.

Finally in step 14, $\mathsf{A}(I)$ is to be constructed from these images and $\mathsf{A}(f(I))$. One can easily observe that the algorithm terminates, as in each step either cardinality of X decreases, or that of L or V increases. This algorithm is a general method and can be tuned to a particular problem by specifying the following three steps in the context of that problem.

(steps 4, 6) $V = X \setminus L$: Give the method to compute $A(I)$ in these base cases.

(step 13): Specify function f.

(step 14): Show how to combine the results of the subproblems.

In the next few subsections we show how to compute Θ, Φ, and their inverses using a generating set of the input ideal.

4.1 Computing Modulo

Let $L = \{y_1, \ldots, y_k\}$ and $X = \{x_1, \ldots, x_l\} \bigcup \{z\} \bigcup L$. Maps θ and Θ from $(k, X, L) \to (k, X\setminus\{z\}, L)$ are computed as follows. Consider an arbitrary polynomial in (k, X, L),

$$f = \sum_i \mathbf{x}^{\alpha_i}\mathbf{y}^{\beta_i} + \sum_j \mathbf{x}^{\alpha_j}\mathbf{y}^{\beta_j} z^{c_j}.$$

Then, $\theta(f) = \sum_i \mathbf{x}^{\alpha_i}\mathbf{y}^{\beta_i}$. Further, suppose $S \subset (k, X, L)$ is a set of binomials. Then, $\Theta(\langle\ S\ \rangle) = \langle\ \theta(f) \mid f \in S\ \rangle$. Conversely, if $S' \subset (k, X \setminus \{z\}, L)$, then$\Theta^{-1}(\langle\ S'\ \rangle) = \langle\ S' \bigcup \{z\}\ \rangle$, from Lemma 12.

4.2 Computing Localization

Consider the ring (k, X, L) as defined in the previous subsection. If $f \in (k, X, L)$, then $\phi(f) = f/1$.

Computing Φ and Φ^{-1} is also easy. For any $S \subset (k, X, L)$, $\Phi(\langle\ S\ \rangle) = \langle\ \{\ f/1 \mid f \in S\ \}\ \rangle$. In the reverse direction, for any $S' \subset (k, X, L \bigcup \{z\})$, we define $\Phi^{-1}(\langle\ S'\ \rangle)$ as follows. Let $S' = \{f_1/z^{a_1}, \ldots, f_k/z^{a_k}\}$. Then $\Phi^{-1}(\langle\ S'\ \rangle) = \langle\ f_1, \ldots, f_k\ \rangle : z^\infty$ The correctness follows from Lemmas 13 and 20.

To see how we can compute saturation with respect to z in a partial Laurent polynomial ring, we briefly revisit the results on *pseudo-Gröbner basis* in [11].

4.3 pseudo-Gröbner Basis

Gröbner bases are defined for ideals in rings $k[x_1, \ldots, x_n]$ ([3, Chapter 2]). This notion has been generalized for binomial ideals in partial Laurent polynomial rings, called pseudo-Gröbner bases in [11, Section 5]. Here we reproduce some relevant results.

Algorithm 1: A framework for computing binomials ideals - A

```
Data: A ring $(k, X, L)$, where $k$ is algebraically
      closed, and $\mathsf{char}(k) = 0$; forbidden set
      $V \subseteq X \setminus L$; a binomial generating set $S$ of an
      ideal in the ring.
Result: $\mathsf{A}(\langle S \rangle)$
1  if $X = \phi$ then                    // The ring is a field
2  |   Nothing to do ;
3  else if $X = L$ then   // Laurent polynomial ring
4  |   Compute $\mathsf{A}(\langle S \rangle)$ and return ;
5  else if $V = X \setminus L$ then    // No more reductions
6  |   Compute $\mathsf{A}(\langle S \rangle)$ and return ;
7  end
8  Let $x \in (X \setminus L) \setminus V$ ;
   /* computing $\mathsf{A}(\Theta(\langle S \rangle + \langle x \rangle))$ and lift     */
9  Call A with ideal $\Theta(\langle S \rangle + \langle x \rangle)$, ring
   $(k, X \setminus \{x\}, L)$ and forbidden set $V$ ;
10 Compute $\Theta^{-1}(\mathsf{A}(\Theta(\langle S \rangle + \langle x \rangle)))$ ;
   /* computing $\mathsf{A}(\Phi(\langle S \rangle : x^{\infty}))$ and lift       */
11 Call A with ideal $\Phi(\langle S \rangle : x^{\infty})$, ring $(k, X, L \bigcup \{x\})$
   and forbidden set $V$ ;
12 Compute $\Phi^{-1}(\mathsf{A}(\Phi(\langle S \rangle : x^{\infty})))$ ;
   /* computing $\mathsf{A}(f(\langle S \rangle : x^{\infty}))$                   */
13 Call A with ideal $f(\langle S \rangle)$, ring $(k, X, L)$ and
   forbidden set $V \bigcup \{x\}$ ;
   /* Computing $\mathsf{A}(\langle S \rangle)$                                 */
14 Combine $\Theta^{-1}(\mathsf{A}(\Theta(\langle S \rangle + \langle x \rangle)))$,
   $\Phi^{-1}(\mathsf{A}(\Phi(\langle S \rangle : x^{\infty})))$ and $\mathsf{A}(f(\langle S \rangle))$ to get
   $\mathsf{A}(\langle S \rangle)$ ;
   /* Return                                               */
15 return $\mathsf{A}(\langle S \rangle)$ ;
```

Definition 11. A binomial $a\mathbf{x}^{\alpha} + b\mathbf{x}^{\beta} \in (k, X, L)$ is said to be **balanced** if $x_i \in X \setminus L$ implies $\alpha_i = \beta_i$.

Definition 12. For every finite binomial set G, G_1 and G_2 will denote its partition, where the former will represent the set of non-balanced binomials and the latter will represent the set of balanced binomials of G.

Definition 13. A binomial basis $G = (G_1, G_2)$ of a binomial ideal I will be called a pseudo Gröbner basis with respect to a given term-order if G_1 reduces every binomial of I to $0(\mathsf{mod}(G_2))$.

THEOREM 5. *[11, Theorem 3] Every binomial ideal in (k, X, L) has a Gröbner basis with respect to any term-order.*

The Buchberger's algorithm to compute Gröbner basis has been adopted to compute pseudo-Gröbner basis in [11, Algorithm 4]. Finally, the following theorem shows that saturation can be computed in similar way as in $k[x_1, \ldots, x_n]$.

THEOREM 6. *[11, Theorem 3] Let (G_1, G_2) be a pseudo Gröbner basis of a homogeneous binomial ideal in (k, X, L) with respect to a graded reverse lexicographic term order with the variable $x_i \notin L$ being the least. Then $(G_1' = G_1 \div x_i^{\infty}, G_2' = G_2 \div x_i^{\infty})$ is a pseudo Gröbner basis of $I : x_i^{\infty}$.*

Here $S \div x^{\infty}$ is the result of the division of each polynomial in S by the largest possible power of x.

5. COMPUTING $\mathsf{A}(I)$

As mentioned in the previous section, we will describe the steps 4, 6, 13 and 14 of the algorithm in context of four problems – (i) radical of a binomial ideal, (ii) cellular decomposition of a binomial ideal, (iii) the minimal prime ideals of a binomial ideal, and (iv) the saturation of a binomial ideal with respect to all variables in the ring.

5.1 Radical Ideal

THEOREM 7. *Let R be an Noetherian ring, $r \in R$ a non-zero-divisor, and $I \subseteq R$ be an ideal. Then,*

$$\sqrt{I + \langle r \rangle} \bigcap \sqrt{I : r^{\infty}} = \sqrt{I},$$

for some $r \in R$.

PROOF. From Theorem 4, we know that every radical in a Noetherian ring has a prime decomposition. Let the prime decomposition of $\sqrt{I}$ be

$$\sqrt{I} = P_1 \bigcap P_2 \bigcap \cdots \bigcap P_n.$$

Let the collection of the primes in the decomposition be denoted by $\mathcal{P}$. Define two ideals

$$\mathcal{P}_r = \left(\bigcap_{r \in P \in \mathcal{P}} P \right), \overline{\mathcal{P}_r} = \left(\bigcap_{r \notin P \in \mathcal{P}} P \right)$$

It is easy to see that $I + \langle r \rangle \subseteq \mathcal{P}_r$. Hence, $\sqrt{I + \langle r \rangle} \subseteq \mathcal{P}_r$. Next, we want to show that $\sqrt{I : r^{\infty}} \subseteq \overline{\mathcal{P}_r}$.

Let $f \in I : r^{\infty}$. Then, $r^n f \in I$ for some $n \geq 0$. This implies that for all $P \in \mathcal{P}, r^n f \in P$. In particular, if $r \notin P$, then $f \in P$. We deduce that $I : r^{\infty} \subseteq \overline{\mathcal{P}_r}$, and hence $\sqrt{I : r^{\infty}} \subseteq \overline{\mathcal{P}_r}$. Putting the two observation together we have

$$\sqrt{I + \langle r \rangle} \bigcap \sqrt{I : r^{\infty}} \subseteq \mathcal{P}_r \bigcap \overline{\mathcal{P}_r} = \sqrt{I}$$

The converse containment $\sqrt{I} \subseteq \sqrt{I + \langle r \rangle} \bigcap \sqrt{I : r^{\infty}}$ is obvious. □

This theorem leads to the following result which will help us in the formulation of step 14.

THEOREM 8. *Let R be an Noetherian ring, $r \in R$ a non-zero-divisor, and $I \subseteq R$ be an ideal. Then,*
$$\sqrt{I} = \Theta^{-1}\left(\sqrt{\Theta\left(I + \langle r \rangle\right)}\right) \bigcap \Phi^{-1}\left(\sqrt{\Phi\left(I : r^{\infty}\right)}\right).$$

PROOF. We will continue to use the notations defined in the previous theorem. From the proof of Theorem 7, we have

$$I + \langle r \rangle \subseteq \mathcal{P}_r \tag{1}$$

From the containment preserving property and the commutation with intersection property of Θ, we have

$$\Theta\left(I + \langle r \rangle\right) \subseteq \Theta\left(\bigcap_{r \in P \in \mathcal{P}} P \right) = \bigcap_{r \in P \in \mathcal{P}} \Theta\left(P\right).$$

Similarly

$$\sqrt{\Theta\left(I + \langle r \rangle\right)} \subseteq \sqrt{\bigcap_{r \in P \in \mathcal{P}} \Theta\left(P\right)} = \bigcap_{r \in P \in \mathcal{P}} \sqrt{\Theta\left(P\right)}.$$

The last equality is due to Lemma 5.

As the P's are primes, from Lemma 9 we know that the $\Theta(P)$s are primes and hence from observation 1, we have $\sqrt{\Theta\left(I+\langle r\rangle\right)} \subseteq \left(\bigcap_{r\in P\in\mathcal{P}} \Theta\left(P\right)\right)$. Hence $\Theta^{-1}\left(\sqrt{\Theta\left(I+\langle r\rangle\right)}\right) \subseteq \mathcal{P}_r$.

Similarly, starting from the following relation given in the proof of theorem 7

$$I : r^\infty \subseteq \overline{\mathcal{P}_r}$$

we can deduce that

$$\Phi^{-1}\left(\sqrt{\Phi\left(I : r^\infty\right)}\right) \subseteq \overline{\mathcal{P}_r}.$$

Combining the two results gives

$$\Theta^{-1}\left(\sqrt{\Theta\left(I+\langle r\rangle\right)}\right) \bigcap \Phi^{-1}\left(\sqrt{\Phi\left(I : r^\infty\right)}\right) \subseteq \sqrt{I}.$$

To prove the converse, from Lemmas 11 and 19 we have $\sqrt{I} \subseteq \Theta^{-1}(\sqrt{\Theta(I+\langle\ r\ \rangle} \bigcap \Phi^{-1}(\sqrt{\Phi(I : r^\infty}).$

□

First thing to note is that we will not use the $\mathsf{A}(f(I))$ branch of the reduction for this problem. Thus, Theorem 7 shows that the *combine* step (step 14) is intersection. Also, we will have $V = \emptyset$. The base case computation in step 4 of the algorithm is trivial because all binomial ideals in a Laurent polynomial ring are already radical as shown below.

THEOREM 9 (COROLLARY 2.2, [5]). *Let J be a binomial ideal in the ring (k, X, ϕ). Then, if k is algebraically closed and $\mathsf{char}(k) = 0$, then $J : (\Pi_{x\in X} x)^\infty$ is radical.*

COROLLARY 1. *Let k be an algebraically closed field, with $\mathsf{char}(k) = 0$. Then, all binomial ideals in (k, X, X) are radical.*

PROOF. Let J be a binomial ideal in the ring (k, X, X), where $X = \{x_1, \ldots, x_n\}$. Consider the ideal localization map, Φ_n, from $(k, X, X \setminus \{x_n\})$ to (k, X, X). Under this map, we know that $\Phi_n^{-1}(J)$ is saturated w.r.t x_n. Similarly, if we consider the map Φ_{n-1} from $(k, X, X \setminus \{x_{n-1}, x_n\})$ to $(k, X, X \setminus \{x_n\})$, then the ideal $\Phi_{n-1}^{-1}(\Phi_n^{-1}(J))$ is saturated w.r.t. x_{n-1}. So we have

$$\begin{aligned} \Phi_n^{-1}(J) &= \Phi_n^{-1}(J) : x_n^\infty \\ \Longrightarrow\ \Phi_{n-1}^{-1}(\Phi_n^{-1}(J)) &= \Phi_{n-1}^{-1}(\Phi_n^{-1}(J) : x_n^\infty) \\ &= \Phi_{n-1}^{-1}(\Phi_n^{-1}(J)) : x_n^\infty \quad (\text{ Lemma 18}) \end{aligned}$$

Thus, $\Phi_{n-1}^{-1}(\Phi_n^{-1}(J))$ is saturated w.r.t. $\{x_{n-1}, x_n\}$. Continuing this argument we see that $\Phi_1^{-1}(\cdots(\Phi_n^{-1}(J))\cdots)$, in the ring (k, X, ϕ), is saturated w.r.t. $\{x_1, \ldots, x_n\}$. From the previous theorem $\Phi_1^{-1}(\cdots(\Phi_n^{-1}(J)))$ is radical. Now, by repeated application of Lemma 19 we deduce that J is radical too. □

5.2 Cellular Decomposition: $\mathsf{A} = \mathsf{Cellular}$

In this section we will generalize the notion of **cellular ideals** to partial Laurent polynomial rings, establish that every ideal has a cellular decomposition, and use our framework to compute such a decomposition.

Let (k, X, L) be a partial Laurent polynomial ring. For a given set of variables $\mathscr{E} \subseteq (X \setminus L)$ and a vector $d = (d_i)_{i\in(X\setminus L)\setminus\mathscr{E}}$, we define the ideal $M(\mathscr{E})^{(d)}$ as –

$$M(\mathscr{E})^{(d)} := \langle\ \left\{\ x_i^{d_i}\ \mid i \in (X \setminus L) \setminus \mathscr{E}\ \right\}\ \rangle.$$

Now, we are ready to define cellular ideals.

Definition 14. We define an ideal I of (k, X, L) to be **cellular**, if for some some $\mathscr{E} \subseteq (X \setminus L)$, we have $I = I : \left(\prod_{i\in\mathscr{E}} x_i\right)^\infty$, and I contains $M(\mathscr{E})^{(d)}$ for some vector d.

Next, we will state a trivial observation characterizing cellular ideals.

OBSERVATION 6. *An ideal I is cellular iff $\exists\mathscr{E} \subseteq (X \setminus L)$ and $d = (d_i)_{i\in(X\setminus L)\setminus\mathscr{E}}$, such that*

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

In such a case, we will denote I by $I_{\mathscr{E}}^{(d)}$.

This observation helps us to make the following claim regarding cellular ideals and Φ^{-1}.

LEMMA 21. Φ^{-1} *preserves cellular ideals.*

PROOF. Let Φ^{-1} be a map from (k, X, L) to $(k, X, L \setminus \{x\})$, where $x \in L$, and consider the cellular ideal $I = I_{\mathscr{E}}^{(d)}$ in (k, X, L). As $\Phi^{-1}(I)$ is saturated w.r.t. x, it corresponds to the cellular ideal $\Phi^{-1}(I)_{\mathscr{E}\bigcup\{x\}}^{(d')}$, where d' is the same vector as d, except that it does not contain the component corresponding to x. □

LEMMA 22. *Let $s \in \mathbb{N}$ be such that $I : r^s = I : r^\infty$ in some Noetherian ring R. Then,*

$$I = (I + \langle\ r^s\ \rangle) \bigcap (I : r^s)\,.$$

PROOF. Let $f \in (I + \langle\ r^s\ \rangle) \bigcap (I : r^s)$. Then

$$\begin{aligned} f &= i + gr^s \in I : r^s \text{ for some } i \in I, g \in R \\ \Longrightarrow\ fr^s &= ir^s + gr^{2s} \in I. \end{aligned}$$

This, coupled with the fact that $I : r^{2s} = I : r^s$, we have $f \in I$. □

Now, we are ready to state how to compute a cellular decomposition of I. The computation will not use $\mathsf{A}(\Theta(I))$ branch of the reduction. $f(I)$ is defined as $I + \langle\ x^s\ \rangle$, where $s \in \mathbb{N}$ is such that $I : x^s = I : x^\infty$. By using Lemma 21, we see that cellular decomposition of $\Phi(I : x^\infty)$ gives us a cellular decomposition of $I : x^s$. To combine the decompositions of $\mathsf{A}(I : x^s)$ and $\mathsf{A}(f(I))$, we use Lemma 22.

What remains is to specify the computations at the base cases, i.e., $X = L \bigcup V$. Ideals in the base cases are already cellular because variables in $V = X \setminus L$ are nilpotents of the ideals. Hence, there is no computation required in steps 4 and 6.

5.3 Prime Decomposition: $\mathsf{A} = \mathsf{Prime}$

In this case, as in the computation of a radical, the $\mathsf{A}(f(I))$ branch will not be used. We will first handle the base case, i.e. how to compute the minimal primes of a binomial ideal in a Laurent polynomial ring (step 4). To do this, we will mention (without proof) a set of results from [5].

Definition 15. A **partial character** on $\mathbb{Z}^n$ is a homomorphism ρ from a sublattice L_ρ of $\mathbb{Z}^n$ to the multiplicative group k^*. A partial character will always refer to the tuple (ρ, L_ρ).

For a binomial ideal I in (k, X, X), let us define a partial character $(\rho, L(I))$. It is easy to verify that

$$L(I) = \{ \ \alpha \mid \mathbf{x}^\alpha - c \in I \ \} \, .$$

is a lattice. The function ρ is given by

$$\rho(\alpha) = c, \text{ where } \mathbf{x}^\alpha - c \in I.$$

Conversely, given a partial character (ρ, L), we will define a binomial ideal as

$$I(\rho) = \langle \ \{ \ \mathbf{x}^\alpha - c \mid \alpha \in L, \rho(\alpha) = c \ \} \ \rangle.$$

THEOREM 10. *For any proper binomial ideal in (k, X, X), there is a unique partial character ρ on $\mathbb{Z}^n$ such that $I = I(\rho)$.*

Definition 16. If L is a sublattice of $\mathbb{Z}^n$, then the saturation of L is the lattice

$$\mathsf{Sat}(L) = \{ \ m \in \mathbb{Z}^n \mid dm \in L \text{ for some } d \in \mathbb{Z} \ \} \, .$$

We can compute $\mathsf{Sat}(L)$ for any lattice L by simple change of variables in (k, X, X).

Definition 17. If (ρ, L_ρ) is a partial character, any partial character $(\rho', Sat(L_\rho))$ is called a **saturation** of (ρ, L_ρ) if ρ' coincides with ρ when restricted to L_ρ.

THEOREM 11. *If g is the order of the group $\mathsf{Sat}(L_\rho)/L_\rho$, then there are g distinct saturations of ρ: $\rho_1, \ldots, \rho_g$. Also*

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

THEOREM 12. *The radical of a cellular ideal is of the form $I(\rho) + M(\mathscr{E})^{(d)}$ (d is vector with all 1s), and its minimal primes are the lattice ideals with the saturations of ρ.*

So in a Laurent polynomial ring, to determine the set of minimal primes of a binomial ideal $I = I(\rho)$, all we need to do is to compute the saturations of ρ. The lattice ideals corresponding to these saturations are the associated primes of $I(\rho)$. The minimal of these ideals constitute the prime decomposition.

Now, let us discuss how we can combine the results from the modulo and the localization branch (step 14). From the recursive calls of the algorithm we have computed the minimal primes of $\Theta(I + \langle \ r \ \rangle)$ and $\Phi(I : r^\infty)$. Let the set of minimal primes be denoted by $\mathcal{P}_\Theta$ and $\mathcal{P}_\Phi$, respectively. So, we have

$$\sqrt{\Theta(I + \langle \ r \ \rangle)} = \bigcap_{P \in \mathcal{P}_\Theta} P$$

$$\sqrt{\Phi(I : r^\infty)} = \bigcap_{P \in \mathcal{P}_\Phi} P.$$

From Theorem 8, we have

$$\sqrt{I} = \Theta^{-1} \left(\sqrt{\Theta \left(I + \langle \ r \ \rangle \right)} \right) \bigcap \Phi^{-1} \left(\sqrt{\Phi \left(I + \langle \ r \ \rangle \right)} \right)$$

$$= \left(\bigcap_{P \in \mathcal{P}_\Theta} \Theta^{-1}(P) \right) \bigcap \left(\bigcap_{P \in \mathcal{P}_\Phi} \Phi^{-1}(P) \right)$$

We know that Θ and Φ map primes to primes (Lemmas 9 and 16). The desired set of prime ideals is $\{ \ \Theta^{-1}(P) \mid P \in \mathcal{P}_\Theta \ \} \bigcup \{ \ \Phi^{-1}(P) \mid P \in \mathcal{P}_\Phi \ \}$. We just need to remove the redundant ones.

5.4 Saturation : $\mathsf{A} = \mathsf{Saturation}$

Suppose I is saturated with respect to $\{x_{i_1}, \ldots, x_{i_j}\}$ then we begin the computation with $V = \{x_{i_1}, \ldots, x_{i_j}\}$. For this problem, we only use the $\mathsf{A}(I : x^\infty)$ branch of the reduction. The base case for this algorithm will be $X \setminus L = V$ (step 6). As Φ preserves saturation (Lemma 18), the ideal is already saturated in this ring. Since the algorithm uses only one branch of the reduction, step 14 is redundant.

6. REFERENCES

[1] A. M. Bigatti, R. Scala, and L. Robbiano. Computing toric ideals. *J. Symb. Comput.*, 27(4):351–365, 1999.

[2] P. Conti and C. Traverso. Büchberger algorithm and integer programming. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 130–139, 1991.

[3] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e.* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[4] D. Eisenbud. *Commutative Algebra with a View toward Algebraic Geometry.* Springer Verlag, New York, 1995.

[5] D. Eisenbud and B. Sturmfels. Binomial ideals. *Duke Mathematical Journal*, 84(1):1–45, 1996.

[6] W. Fulton. *Introduction to toric varieties*, volume 131 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 1993.

[7] D. Geiger, C. Meek, and B. Sturmfels. On the toric algebra of graphical models. *The Annals of Statistics*, 34(3):1463–1492, 2006.

[8] R. Gilmer. *Commutative semigroup rings.* University of Chicago Press, Chicago, Illinois, 1984.

[9] R. Hemmecke and P. N. Malkin. Computing generating sets of lattice ideals and markov bases of lattices. *Journal of Symbolic Computation*, 44(10):1463–1476, 2009.

[10] S. Hosten and B. Sturmfels. Grin: An implementation of Gröbner bases for integer programming. *Integer Programming and Combinatorial Optimization*, 1995.

[11] D. Kesh and S. K. Mehta. A saturation algorithm for homogeneous binomial ideals. In *COCOA*, pages 357–371, 2011.

[12] B. Sturmfels. *Gröbner Bases and Convex Polytopes*, volume 8 of *University Lecture Series.* American Mathematical Society, December 1995.

[13] S. R. Tayur, R. R. Thomas, and N. R. Natraj. An algebraic geometry algorithm for scheduling in the presence of setups and correlated demands. *Mathematical Programming*, 69(3):369–401, 1995.

[14] R. Thomas and R. Weismantel. Truncated gröbner bases for integer programming. *Applicable Algebra in Engineering, Communication and Computing*, 8(4):241–256, 4 1997.

[15] R. R. Thomas. A geometric büchberger algorithm for integer programming. *Mathematics of Operations Research*, 20:864–884, 1995.

[16] R. Urbaniak, R. Weismantel, and G. M. Ziegler. A variant of the Buchberger algorithm for integer programming. *SIAM J. Discret. Math.*, 10(1):96–108, 1997.