GRÖBNER BASIS STRUCTURE OF FINITE SETS OF POINTS

SHUHONG GAO, VIRGÍNIA M. RODRIGUES, AND JEFFREY STROOMER

Abstract. We study the relationship between certain Gröbner bases for zero-dimensional radical ideals, and the varieties defined by the ideals. Such a variety is a finite set of points in an affine n-dimensional space. We are interested in monomial orders that "eliminate" one variable, say z. Eliminating z corresponds to projecting points in n-space to $(n-1)$-space by discarding the z-coordinate. We show that knowing a minimal Gröbner basis under an elimination order immediately reveals some of the geometric structure of the corresponding variety, and knowing the variety makes available information concerning the basis. These relationships can be used to decompose polynomial systems into smaller systems.

1. Introduction

Gröbner bases and elimination are powerful tools for solving polynomial systems. The basic idea is to turn a polynomial system into triangular form and solve it iteratively using linear algebra. There is a rich literature on this and related topics, and the reader is referred to [4, 5, 19] for an excellent exposition. Elimination theory deals mainly with the case where partial solutions can be extended to complete solutions. In general it is difficult to predict in how many ways partial solutions can be extended. In this paper we shed some light on this problem. We study the connection between the structure of certain Gröbner bases and the geometric structure of the solution set (an affine variety) of a zero-dimensional polynomial ideal. We focus on the special but important case when all the solutions are distinct, i.e., when the ideal is radical.

Let $\mathbb{F}$ be any field, let I be a zero-dimensional radical ideal in $\mathbb{F}[x_1, \ldots, x_n]$, and let $\mathcal{P}$ be the set of its zeros in $\overline{\mathbb{F}}^n$, where $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$. Suppose G is a minimal Gröbner basis for I under some monomial order. We would like to have an easy way, involving little computation, to translate information concerning G into information concerning $\mathcal{P}$, and vice-versa.

To make these ideas concrete, let $\pi : \overline{\mathbb{F}}^n \longrightarrow \overline{\mathbb{F}}^{n-1}$ be the projection map

$$\pi(a_1, \cdots, a_{n-1}, a_n) = (a_1, \cdots, a_{n-1}).$$

Date: November 19, 2003.

The first two authors were supported in part by National Science Foundation (NSF) under Grants DMS9970637 and DMS0302549, National Security Agency (NSA) under Grant MDA904-02-1-0067, the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Office of Naval Research (ONR) under Grant N00014-00-1-0565. The second author also gratefully acknowledges the support of CAPES, Brazil.

Let $\mathcal{S} = \pi(\mathcal{P})$ denote the projection of $\mathcal{P}$. The *fibre of* π *in* $\mathcal{P}$ *at a point* $s \in \mathcal{S}$ is $\pi^{-1}(s)$, the set of points in $\mathcal{P}$ that project to s. For simplicity we call this set the *fibre of* s. The *size* of a fibre is its cardinality, and the *fibre size of* s is the size of its fibre. Note $\mathcal{P}$ is a disjoint union of fibres. A point $s \in \mathcal{S}$ corresponds to a partial solution and the fibre size of s indicates the number of ways s can be extended to complete solutions (i.e., to points in $\mathcal{P}$). It is natural to ask the following:

(1) Does a Gröbner basis for I tell the sizes of the fibres in $\mathcal{P}$?
(2) Is it possible to determine from such a Gröbner basis other information, say Gröbner bases for subsets of $\mathcal{S}$ that are projections of fibres of different sizes?

We work with perfect fields. Recall that a field $\mathbb{F}$ is *perfect* if either $\mathbb{F}$ has characteristic 0, or $\mathbb{F}$ has characteristic $p > 0$ and every element in $\mathbb{F}$ has a p-th root in $\mathbb{F}$. Perfect fields include number fields, finite fields, and all algebraically closed fields. We also restrict our attention to elimination orders. A monomial order in $\mathbb{F}[x_1, \ldots, x_n]$ is an *elimination order for* x_n if the monomial x_n is greater than all monomials in $\mathbb{F}[x_1, \ldots, x_{n-1}]$. There is a unique elimination order for x_n that extends any given monomial order on $\mathbb{F}[x_1, \ldots, x_{n-1}]$, say lexicographic or graded lexicographic.

Our main contribution in this paper is the following theorem, which is proved in Section 3.

Theorem. *Let* $\mathbb{F}$ *be a perfect field,* I *a zero-dimensional radical ideal in* $\mathbb{F}[x_1, \ldots, x_n]$*, and* $\mathcal{P}$ *the set of zeros of* I *in* $\overline{\mathbb{F}}^n$*. Assume the fibre sizes in* $\mathcal{P}$ *are* $m_1 > \ldots > m_r > 0$*. Let* G *be any minimal Gröbner basis for* I *under an elimination order for* x_n*. View the elements of* G *as polynomials in* x_n *with coefficients in* $\mathbb{F}[x_1, \ldots, x_{n-1}]$*.*

(1) *The* x_n*-degrees of the polynomials in* G *are exactly the fibre sizes in* $\mathcal{P}$*.*
(2) *For* $1 \leq i \leq r$ *let* G_i *denote the set of the leading coefficients of polynomials in* G *whose* x_n*-degrees are* $< m_i$*, and let* $\mathcal{S}_{\leq i}$ *denote the set of points in* $\mathcal{S} = \pi(\mathcal{P})$ *that are projections of fibres of size* $\geq m_i$*. Then each* G_i *is a Gröbner basis for* $\mathcal{S}_{\leq i}$*.*

This is a strengthening of the classical elimination theory which deals with existence of extension of partial solutions, whereas the above theorem predicts exactly how many extensions exist. We demonstrate this with a simple example. Let $\mathbb{F}$ be any perfect field, and let $G = \{z^2 - z, zy - z, x, y^2 - y\}$. Then G is a Gröbner basis for any monomial order, and the solutions of G are exactly the points $(0, 1, 0)$, $(0, 1, 1)$, and $(0, 0, 0)$. For the variable z, its distinct degrees in G are 2, 1 and 0, and

$$G_1 = \{y - 1, x, y^2 - y\}, \quad G_2 = \{x, y^2 - y\}.$$

Clearly G_1 has one solution, namely $(0, 1)$, which is the projection of a fibre of size 2 by the above theorem. Similarly, G_2 has two solutions, namely $(0, 0)$ and $(0, 1)$, each of which is the projection of a fibre of size ≥ 1. It follows that $(0, 0)$ is the projection of a fibre of size 1. Note these fibre sizes indeed match those of the solution set. This relationship can be used to decompose the polynomial system

G into smaller systems that are easier to solve. We demonstrate this with a more extensive example in Section5.

When the points in $\mathcal{P}$ are known, the x_n-degrees for a minimal Gröbner basis can be found by calculating fibre sizes. In the extreme case where the monomial order is lexicographic, this gives rise to a simple algorithm, presented in Section 4, for constructing the monomial basis of I. The algorithm operates exclusively on the point set and requires no operations in the field aside from tests for equality of field elements. In [3], Cerlienco and Mureddu present an algorithm for computing the monomial basis for I directly from the point set. Our construction is different from theirs and is perhaps more intuitive.

In this paper we do not describe how to calculate a Gröbner basis for a given set of points. Algorithms for doing this (possibly with multiplicity) are described in [2, 6, 7, 16]. Vanishing ideals of finite sets of points also arise in several other applications. See for examples, [12, 18, 20] for coding theory, [8, 9, 10, 11, 15] for multivariate polynomial interpolation and multivariate rational function approximation, [17] for statistics, and [14] for biology.

2. Preliminaries

We refer the reader to the books of Cox, Little and O'Shea ([4] and [5]) for introduction to the theory of Gröbner bases and its applications. Here we mention some notation and basic results needed in later sections. Throughout we write R to denote the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$.

Fix any monomial order in R. A nonzero polynomial $f \in R$ has a unique leading term $lt(f)$. For any nonempty subset G of R, we denote by $lt(G)$ the set of leading terms of all nonzero polynomials in G, and by $\langle lt(G)\rangle$ the ideal generated by the elements of $lt(G)$.

Every nonzero ideal I of R has a Gröbner basis. A Gröbner basis G for I can be made *minimal* making its polynomials monic and by removing from G any polynomial g with $lt(g) \in \langle lt(G \setminus \{g\})\rangle$ A given ideal can have many minimal Gröbner bases, but each has the same set of leading terms. A minimal Gröbner basis G for I is *reduced* if its elements are reduced with respect to G, i.e., for every $g \in G$ no monomial of g is in $\langle lt(G \setminus \{g\})\rangle$. Any nonzero ideal I of R has a unique reduced Gröbner basis. and radical.

For an n-tuple $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ we write x^α to represent the monomial with exponent vector α: $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. The set

$$B(I) = \{x^\alpha : \alpha \in \mathbb{N}^n \text{ and } x^\alpha \notin lt(I)\}$$

of all monomials not divisible by the leading term of any polynomial in I is called the *monomial basis of* I (with respect to the given monomial order). Its elements are called *basis monomials* (or *standard monomials*). The monomial basis of I forms a basis for the quotient ring R/I as a vector space over the field $\mathbb{F}$, so

$$|B(I)| = dim_{\mathbb{F}}\,(R/I)\,.$$

This implies that for a given ideal I the number of basis monomials is independent of the monomial order.

The set of exponent vectors of the basis monomials is called the *delta set of the ideal I*. We represent it by $\Delta(I)$. Thus

$$\Delta(I) = \{\alpha \in \mathbb{N}^n : x^\alpha \in B(I)\} = \{\alpha \in \mathbb{N}^n : x^\alpha \notin lt(I)\}.$$

Similarly, we define the *delta set of a finite set* $\{f_1, \ldots, f_l\} \subseteq R$ to be the set

$$\Delta(f_1, \ldots, f_l) = \{\alpha \in \mathbb{N}^n : x^\alpha \text{ is not divisible by any } lt(f_i),\ 1 \leq i \leq l\}.$$

The motivation for the choice of names is the following. Consider the set of n-tuples of natural numbers with the partial order $\leq$ induced from the usual order on $\mathbb{N}$, namely $(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n)$ provided $a_i \leq b_i$ for each i. Suppose Δ is a subset of $\mathbb{N}^n$ with the property that whenever $a = (a_1, \ldots, a_n) \in \Delta$ and $b = (b_1, \ldots, b_n) \in \mathbb{N}^n$, with $b \leq a$, then b must also be in Δ. Then Δ is called a *delta set* (or an *order ideal*). It is easy to see that $\Delta(I)$ and $\Delta(f_1, \ldots, f_l)$ as defined above are in fact delta sets in this second sense, since for all $\alpha, \beta \in \mathbb{N}^n$, $x^\alpha \mid x^\beta$ if and only if $\alpha \leq \beta$. It follows that $\Delta(I) \subseteq \Delta(f_1, \ldots, f_l)$ for any $f_1, \ldots, f_l \in I$. Lemma 1 below tells us that the equality holds if and only if $\{f_1, \ldots, f_l\}$ is a Gröbner basis for I. Whenever Δ is a delta set, then $c \in \mathbb{N}^n$ is *co-minimal* for Δ provided c is a minimal element of $\mathbb{N}^n \setminus \Delta$.

We denote by $V(I)$ be the set of common zeros in $\overline{\mathbb{F}}^n$ of the polynomials in the ideal I, i.e.,

$$V(I) = \{p \in \overline{\mathbb{F}}^n : f(p) = 0 \text{ for all } f \in I\}.$$

$V(I)$ is an affine algebraic set, called the *algebraic set determined by I*. It is also known as the *locus of I* or the *variety of I*.

Conversely, let $\mathcal{P}$ be a finite set of distinct points in $\mathbb{F}^n$, where $\mathbb{F}$ is an arbitrary field, and consider the vanishing ideal $\mathbf{I}(\mathcal{P})$ of $\mathcal{P}$ defined by

$$\mathbf{I}(\mathcal{P}) = \{f \in \mathbb{F}[x_1, \ldots, x_n] : f(p) = 0 \text{ for all } p \in \mathcal{P}\}. \tag{1}$$

The common solutions of the polynomials in $\mathbf{I}(\mathcal{P})$ are precisely the points in $\mathcal{P}$. For brevity, when G is a Gröbner basis for $\mathbf{I}(\mathcal{P})$, we say G is a Gröbner basis for $\mathcal{P}$. The following basic results relate the concepts above, whose proofs are straightforward (The last part of Lemma 1 appears in [16, Lemma 3.8, p112].)

Lemma 1. *Let $\mathcal{P} \subseteq \mathbb{F}^n$ and $I = \mathbf{I}(\mathcal{P})$. Then $V(I) = \mathcal{P}$ and $|\Delta(I)| = |\mathcal{P}|$, Further, $\{f_1, \ldots, f_l\} \subset I$ is a Gröbner basis for I if and only if $|\Delta(f_1, \ldots, f_l)| = |\mathcal{P}|$.*

Lemma 2. *Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be finite sets of points in $\mathbb{F}^n$ such that $\mathcal{P}_1 \subseteq \mathcal{P}_2$, and let $I_1 = \mathbf{I}(\mathcal{P}_1)$ and $I_2 = \mathbf{I}(\mathcal{P}_2)$. Then $I_1 \supseteq I_2$ and, under the same monomial order, $\Delta(I_1) \subseteq \Delta(I_2)$ and $\langle lt(I_1)\rangle \supseteq \langle lt(I_2)\rangle$. Moreover, $|\Delta(I_2) \setminus \Delta(I_1)| = |\mathcal{P}_2 \setminus \mathcal{P}_1|$.*

Lemma 1 implies that to obtain a Gröbner basis for $\mathbf{I}(\mathcal{P})$ it suffices to find polynomials $f_1, \ldots, f_l \in I$ such that $|\Delta(f_1, \ldots, f_l)| = |\mathcal{P}|$. Lemma 2 shows how Gröbner bases change when points are added. We also need the following well-known result on polynomial interpolation.

Lemma 3. *For any $n \geq 1$, any distinct points $p_1, p_2, \ldots, p_s \in \mathbb{F}^n$, and any values $r_1, \ldots, r_s \in \mathbb{F}$, there is a polynomial $g \in R$ such that $g(p_i) = r_i$, for $1 \leq i \leq s$. In* *particular, there are polynomials* $g_1, \ldots, g_s \in R$ *such that for all* $1 \le i, j \le s$,

$$g_i(p_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases} \tag{2}$$

3. Structure of Gröbner bases

Our goal in this section is to prove the theorem stated in the introduction. The strategy is the following. Let $\mathbb{F}$ be any field and let $\mathcal{P} \subseteq \mathbb{F}^n$ be a finite nonempty set of points. The fibre structure of $\mathcal{P}$ allows us to construct a Gröbner basis for $\mathbf{I}(\mathcal{P})$. This basis makes it possible to show that every minimal Gröbner basis for a zero-dimensional radical ideal has a particular property. From this the theorem follows.

When $n = 1$, the theorem becomes trivial. In this case we write the points in $\mathcal{P}$ as $p_i = a_i$, $1 \le i \le t$. Let G be the set consisting of the single polynomial $(x_1 - a_1) \cdots (x_t - a_t)$. Then $G \subseteq \mathbf{I}(\mathcal{P})$ and its delta set is $\Delta(G) = \{0, 1, \cdots, t-1\}$ which has cardinality $t = |\mathcal{P}|$. Clearly G is a Gröbner basis for $\mathbf{I}(\mathcal{P})$. The degree of the polynomial in G is equal to the number of zeros of I. This is essentially the Fundamental Theorem of Algebra, which says that every polynomial in $\mathbb{C}[x]$ of degree t has t zeros.

Henceforth in this section we assume $n > 1$. Let π be the projection map as defined in the introduction and let $\mathcal{S} = \pi(\mathcal{P}) = \{\pi(p) : p \in \mathcal{P}\} \subseteq \mathbb{F}^{n-1}$ be the projection of $\mathcal{P}$. If the sizes of the fibres in $\mathcal{P}$ are $m_1 > \ldots > m_r > 0$, then $\mathcal{P}$ can be partitioned as

$$\mathcal{P} = \mathcal{P}_1 \cup \ldots \cup \mathcal{P}_r,$$

where each $\mathcal{P}_i$ consists of the fibres of size m_i. This allows us to partition $\mathcal{S}$ as

$$\mathcal{S} = \mathcal{S}_1 \cup \ldots \cup \mathcal{S}_r, \text{ where } \mathcal{S}_i = \pi(\mathcal{P}_i), 1 \le i \le r.$$

It is convenient to let m_{r+1} denote 0. We use $\mathcal{S}_{\le i}$ to denote $S_1 \cup \ldots \cup \mathcal{S}_i$, $\mathcal{P}_{\ge i}$ to denote $\mathcal{P}_i \cup \ldots \cup \mathcal{P}_r$, and so on. Whenever $\mathcal{P}$ is a set of points in $\mathbb{F}^m$, write $\Delta(\mathcal{P})$ as a shorthand for $\Delta(\mathbf{I}(\mathcal{P}))$, a subset of $\mathbb{N}^m$. Given a delta set $\Delta \subset \mathbb{N}^{n-1}$ and a positive integer m, one can build a new delta set $\Delta \otimes m \subset \mathbb{N}^n$ as follows:

$$\Delta \otimes m = \{(a_1, \ldots, a_{n-1}, i) : (a_1, \ldots, a_{n-1}) \in \Delta \text{ and } 0 \le i < m\}.$$

Theorem 4. *Let* $\mathbb{F}$ *be any field and let* $\mathcal{P} \subset \mathbb{F}^n$ *be a finite set with fibre sizes* $m_1 > \ldots > m_r > 0$. *Assume* $\mathcal{P}$ *and* $\mathcal{S}$ *are partitioned as described above. Let* $G_0 = \{1\}$, *and for* $1 \le i \le r$ *let* G_i *be a Gröbner basis for* $\mathcal{S}_{\le i}$. *Then, under an elimination order for* x_n *in* $R = \mathbb{F}[x_1, \cdots, x_n]$, $\mathbf{I}(\mathcal{P})$ *has a Gröbner basis given by*

$$\hat{G} = \bigcup_{i=1}^{r+1} \{f_i \cdot g : g \in G_{i-1}\}, \tag{3}$$

for some $f_i \in R$ *with* $lt(f_i) = x_n^{m_i}$, $1 \le i \le r+1$.

Proof: We first construct the desired polynomials f_i, $1 \le i \le r+1$. We require that f_i vanish on $\mathcal{P}_{\ge i}$ and $lt(f_i) = x_n^{m_i}$. We take $f_{r+1} = 1$, as $\mathcal{P}_{\ge r+1}$ is empty, so assume $1 \le i \le r$. Since the largest fibre in $\mathcal{P}_{\ge i}$ has size m_i, we can partition $\mathcal{P}_{\ge i}$ into m_i subsets $\mathcal{Q}_1 \cup \ldots \cup \mathcal{Q}_{m_i}$ so that every fibre in each $\mathcal{Q}_j$ has size 1. This means the projection map π is one-to-one on each $\mathcal{Q}_j$. By Lemma 3, there is a polynomial $f_j \in \mathbb{F}[x_1, \ldots, x_{n-1}]$ that interpolates $\mathcal{Q}_j$, that is, $x_n - f_j$ vanishes on $\mathcal{Q}_j$. We define f_i to be $\prod_{j=1}^{m_i}(x_n - f_j)$. Then $lt(f_i) = x_n^{m_i}$ and f_j vanishes on $\mathcal{P}_{\geq i}$. Every $g \in G_{i-1}$ vanishes on $\mathcal{S}_{<i}$, hence on $\mathcal{P}_{<i}$, and therefore, $g \cdot f_i$ vanishes on $\mathcal{P}$. This proves $\hat{G}$ in (3) is a subset of $\mathbf{I}(\mathcal{P})$.

Define a delta set Δ as follows:

$$\Delta = \bigcup_{i=1}^{r} \big(\Delta(\mathcal{S}_{\leq i}) \otimes m_i\big).$$

By Lemma 2 and the fact that the m_i decreases with i, one sees that $|\Delta| = |\mathcal{P}|$. By Lemma 1, it suffices to show that whenever $c \in \mathbb{N}^n$ is co-minimal for Δ, the set G in (3) contains a polynomial $h \in \mathbf{I}(\mathcal{P})$ such that $lt(h) = x^c$. Let $c \in \mathbb{N}^n$ be co-minimal for Δ. Then c is of the form $c = (c_1, \ldots, c_{n-1}, m_i)$ for some $1 \leq i \leq r+1$, and $\pi(c) = (c_1, \ldots, c_{n-1})$ is co-minimal for $\Delta(\mathcal{S}_{<i})$. (Here $\mathcal{S}_0$ is empty and corresponds to $G_0 = \{1\}$.) Since G_{i-1} is a Gröbner basis for $\mathcal{S}_{<i}$, there is $g \in G_{i-1}$ with $lt(g) = x_1^{c_1} \cdots x_{n-1}^{c_{n-1}}$. Hence $h = g \cdot f_i$ is in G and $lt(h) = x^c$. This proves that $\hat{G}$ is a (not necessarily minimal) Gröbner basis for $\mathbf{I}(\mathcal{P})$. □

The proof of Theorem 4 actually shows something additional, namely

Corollary 5.

$$\Delta(\mathcal{P}) = \bigcup_{i=1}^{r} \big(\Delta(\mathcal{S}_{\leq i}) \otimes m_i\big).$$

In particular, this asserts that the fibre structures of $\mathcal{P}$ and $\Delta(\mathcal{P})$ are identical, i.e., for each m, the number of fibres of size m in $\mathcal{P}$ equals the number of fibres of the same size in $\Delta(\mathcal{P})$.

The Gröbner basis $\hat{G}$ described in Theorem 4 has two pleasant properties. Suppose we view its elements as polynomials in x_n with coefficients in $\mathbb{F}[x_1, \ldots, x_{n-1}]$. First, the x_n-degrees of the polynomials are exactly the fibre sizes of $\mathcal{P}$. Second, for each fibre size m_i, $1 \leq i \leq r+1$, the leading coefficients of the polynomials having x_n-degree exactly m_i form a Gröbner basis for $\mathcal{S}_{<i}$.

If we reduce $\hat{G}$ or make it minimal, the second property no longer holds, but we can still recover a Gröbner basis for $S_{<i}$ by augmenting the coefficient set with the leading coefficients of the polynomials having x_n-degree smaller than m_i. The interesting fact is that this property holds for every minimal Gröbner basis for $\mathbf{I}(\mathcal{P})$, as we show in Theorem 6 below.

For an $f \in R$ viewed as a polynomial in x_n with coefficients in $\mathbb{F}[x_1, \ldots, x_{n-1}]$, we write $deg_{x_n}(f)$ to represent the degree of f in x_n, and $lt_{x_n}(f)$ to represent its leading term, which is a polynomial in $\mathbb{F}[x_1, \ldots, x_{n-1}]$. Let G be a Gröbner basis for $\mathbf{I}(\mathcal{P})$ and suppose the distinct degrees in x_n of the polynomials in G are $m_1 > \cdots > m_r > 0 = m_{r+1}$. For $1 \leq i \leq r$, define

$$G_i = \{lt_{x_n}(g) : g \in G \text{ and } deg_{x_n}(g) < m_i\} \subseteq \mathbb{F}[x_1, \ldots, x_{n-1}]. \tag{4}$$

We say that G has the *fibre property* for x_n provided the following hold: (a) $m_1, \cdots, m_r$ are exactly the sizes of the fibres in $\mathcal{P}$, and (b) for $1 \leq i \leq r$, G_i is a Gröbner basis for points in $\mathcal{S}$ that are projections of fibres of size $\geq m_i$. This means, in particular, that G_r is a Gröbner basis for $\mathcal{S}$. Note G_r consists of those polynomials in G that do not contain x_n. Certainly, one can define the fibre property for any other variable, and the following theorem holds similarly.

Theorem 6. *Let $\mathbb{F}$ be any field and $\mathcal{P} \subseteq \mathbb{F}^n$ a finite nonempty set. With respect to an elimination order for x_n in R, every minimal Gröbner basis for $\mathbf{I}(\mathcal{P})$ has the fibre property for x_n.*

Proof: First note that Gröbner basis $\hat{G}$ from Theorem 4 has the fibre property. The minimal Gröbner basis obtained from $\hat{G}$ by removing polynomials whose leading terms are divisible by other polynomials in G still has the fibre property (as the ideals generated by the sets $\hat{G}_i$ remain the same). Hence we may assume that there is a minimal Gröbner basis for $\mathbf{I}(\mathcal{P})$ having the fibre property.

Next we show that basis reduction does not change the fibre property. Let G be any minimal Gröbner basis with the fibre property. Since no leading term of a minimal Gröbner basis divides another leading term, a typical reduction is of the form:

$$g' = g + q \cdot h,$$

where $g, h \in G$, $q \in R$, and $lt(q \cdot h) < lt(g)$. Note $g' \in \mathbf{I}(\mathcal{P})$ and $lt(g') = lt(g)$. Write G' to denote the set that results when g is replaced by g' in G. Then G' is also a minimal Gröbner basis for $\mathbf{I}(\mathcal{P})$. Suppose we can show that G' has the fibre property. Then every minimal Gröbner basis for $\mathbf{I}(\mathcal{P})$ has the fibre property, because G can be reduced to the unique reduced Gröbner basis using a sequence of such replacements, and every minimal basis can be generated from the reduced basis by reversing reduction (which is again a sequence of such replacements). Therefore it suffices to prove G' has the fibre property.

What remains is to show that whenever $1 \le i \le r$, the set G'_i is a Gröbner basis for $\mathbf{I}(\mathcal{S}_{\le i})$. It suffices to prove that, for each i, we have $\langle G'_i \rangle = \mathbf{I}(\mathcal{S}_{\le i})$, and $\langle lt(G'_i) \rangle = \langle lt(\mathbf{I}(\mathcal{S}_{\le i})) \rangle$. For any $f \in R$, we have $deg_{x_n}(f) = deg_{x_n}(lt(f))$. In particular, this means $deg_{x_n}(g') = deg_{x_n}(lt(g')) = deg_{x_n}(lt(g)) = deg_{x_n}(g)$. Also, $lt(lt_{x_n}(f)) = lt_{x_n}(lt(f))$, hence $lt(lt_{x_n}(g')) = lt_{x_n}(lt(g')) = lt_{x_n}(lt(g)) = lt(lt_{x_n}(g))$.

If $lt_{x_n}(g') = lt_{x_n}(g)$, then $G'_i = G_i$, so assume $lt_{x_n}(g') \neq lt_{x_n}(g)$. Then $lt_{x_n}(g') = lt_{x_n}(g) + lt_{x_n}(q) \cdot lt_{x_n}(h)$. Suppose $deg_{x_n}(g) = deg_{x_n}(g') = m_{j+1}$. If $i > j$, then $G'_i = G_i$, so assume $i \le j$. Since $lt(h) < lt(g)$ we must have $deg_{x_n}(h) \le m_{j+1}$, and because G has the fibre property, $lt_{x_n}(g)$ and $lt_{x_n}(h)$ both kill $\mathcal{S}_{\le i}$. This means $lt_{x_n}(g')$ does as well, so G'_i kills $\mathcal{S}_{\le i}$. Since $lt_{x_n}(g) = lt_{x_n}(g') - lt_{x_n}(q) \cdot lt_{x_n}(h)$, we have $\langle G'_i \rangle = \langle G_i \rangle = \mathbf{I}(\mathcal{S}_{\le i})$. Moreover, $lt(G'_i) = lt(G_i)$, which means $\langle lt(G'_i) \rangle = \langle lt(G_i) \rangle = \langle lt(\mathbf{I}(\mathcal{S}_{\le i})) \rangle$. $\square$

Finally, we prove the theorem described in the introduction. For convenience, we restate it here.

Theorem 7. *Let $\mathbb{F}$ be a perfect field, let I be a zero-dimensional radical ideal in $\mathbb{F}[x_1, \ldots, x_n]$, and let $\mathcal{P}$ be the set of zeros of I in $\overline{\mathbb{F}}^n$. Assume the fibre sizes in $\mathcal{P}$ are $m_1 > \ldots > m_r$. Let G be any minimal Gröbner basis for I under an elimination order for x_n. View the elements of G as polynomials in x_n with coefficients in $\mathbb{F}[x_1, \ldots, x_{n-1}]$.*

(1) *The x_n-degrees of the polynomials in G are exactly the fibre sizes in $\mathcal{P}$.*
(2) *For each i, $1 \leq i \leq r$, let G_i be defined in (4) and let $\mathcal{S}_{\leq i}$ be defined as above. Then G_i is a Gröbner basis for $\mathcal{S}_{\leq i}$.*

Proof: Let $\mathbf{I}(\mathcal{P})$ be the vanishing ideal of $\mathcal{P}$ in $\overline{\mathbb{F}}[x_1, \ldots, x_n]$. Then $I \subseteq \mathbf{I}(\mathcal{P})$. By Theorem 6 it suffices to prove that I and $\mathbf{I}(\mathcal{P})$ have the same reduced Gröbner basis. To show this we employ Theorem 3.7.19 in [13, p253], which asserts that when $\mathbb{F}$ is perfect, the cardinality of $\mathcal{P}$ is equal to $\dim_{\mathbb{F}} R/I$. So for any Gröbner basis G of I, $\Delta(G) = \dim_{\mathbb{F}} R/I = |\mathcal{P}|$, thus G is also a Gröbner basis for $\mathbf{I}(\mathcal{P})$. The claim follows as the reduced Gröbner basis for any ideal is unique. □

When $\mathbb{F}$ is not perfect, a radical ideal $I \subset \mathbb{F}[x_1, \cdots, x_n]$ may have a zero of multiplicity > 1, so the dimension of $\mathbb{F}[x]/I$ is greater than $|\mathcal{P}|$, the number of distinct zeros of I. In this case, I and $\mathbf{I}(\mathcal{P})$ do not have the same reduced Gröbner basis. For a simple example, consider $\mathbb{F} = \mathbb{F}_2(u)$ where u is transcendental over $\mathbb{F}_2$, and let $I = \langle x^2 - u \rangle$, a zero-dimensional radical ideal in $\mathbb{F}[x]$. I has only one zero in $\overline{\mathbb{F}}$, while $\mathbb{F}[x]/I$ has dimension two.

4. Construction of monomial bases

When a Gröbner basis for an ideal $I \subseteq R$ is known, one can easily obtain the leading terms of a minimal Gröbner basis for I, the monomial basis for I, and the delta set $\Delta(I)$. Recall that the monomial basis is the set of monomials that are not divisible by any of the leading terms of the polynomials in the minimal basis, and $\Delta(I)$ consists of the exponents $\alpha \in \mathbb{N}^n$ for which x^α is in the monomial basis.

In this section we show that when the order is lexicographic and the ideal is $\mathbf{I}(\mathcal{P})$, one does not need to know a Gröbner basis to obtain the delta set. More precisely, we give a construction of $\Delta(\mathbf{I}(\mathcal{P}))$ that depends only on the structure of the points, and does no computations in the field aside from comparisons for equality. From the delta set one can easily obtain the monomial basis and the leading terms of a minimal Gröbner basis.

Any nonempty finite set of points $\mathcal{P} \subseteq \mathbb{F}^n$ can be represented as a rooted tree $T(\mathcal{P})$ of height n in a natural way: the nodes on each path from the root to a leaf are labeled with the coordinates of a point. The root receives no label, its children are labeled with the first coordinates of the points, their children with the second coordinates, and so forth. If two points have the same k leading coordinates, then their corresponding paths coincide until level $k+1$. (We regard the root as being at level zero.) Note $T(\mathcal{P})$ contains $|\mathcal{P}|$ leaves, all at level n. When $n = 1$, then $T(\mathcal{P})$ consists of a root and $|\mathcal{P}|$ children, each labeled with the unique coordinate of a point.

As an example, let $\mathcal{P}$ consists of the following 13 points in $\mathbb{Z}^4$: $(1,1,2,3)$, $(1,1,2,4)$, $(1,1,2,5)$, $(1,2,1,1)$, $(1,2,1,2)$, $(1,2,2,1)$, $(1,2,2,2)$, $(3,1,1,2)$, $(3,1,2,2)$, $(3,1,2,3)$, $(3,3,1,1)$, $(3,4,1,1)$, and $(3,4,1,2)$. Then $T(\mathcal{P})$ is the tree of Figure 1.

Every subtree of $T(\mathcal{P})$ is, in effect, $T(\mathcal{Q})$ for a set $\mathcal{Q}$ of points obtained from $\mathcal{P}$ by discarding leading coordinates. To make this explicit, suppose S is the

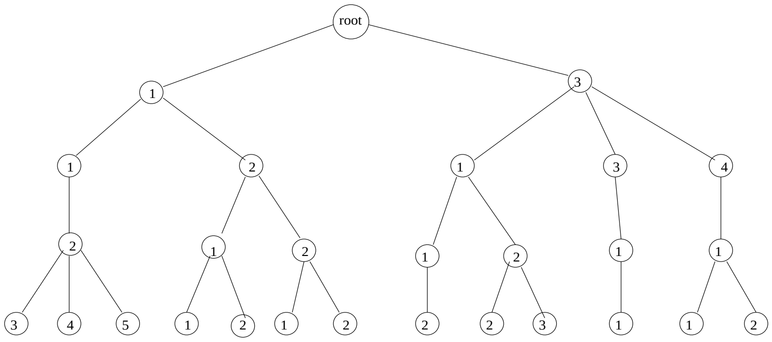

FIGURE 1. Tree $T(\mathcal{P})$ representing 13 points in $\mathbb{Z}^4$

subtree of $T(\mathcal{P})$ corresponding to those points from $\mathcal{P}$ whose first k coordinates are $(a_1, \ldots, a_k)$. Then (ignoring the label on its root), S is $T(\mathcal{Q})$, where $\mathcal{Q} = \{(a_{k+1}, \ldots, a_n) \in \mathbb{F}^{n-k} : (a_1, \ldots, a_k, \ldots, a_n) \in \mathcal{P}\}$. Clearly, whenever S is a subtree of $T(\mathcal{P})$, the corresponding point set $\mathcal{Q}$ can be can be recovered from S. We write $P(S)$ to denote the recovered set.

As before, we use $\Delta(\mathcal{P})$ as a shorthand for $\Delta(\mathbf{I}(\mathcal{P}))$. There is a recursive algorithm to produce $\Delta(\mathcal{P})$ directly from $T(\mathcal{P})$. Before we describe it, we explain what it means to merge delta sets.

Let $\Delta_1, \ldots, \Delta_k \subseteq \mathbb{N}^{n-l}$ be delta sets. For any point $a = (a_2, \ldots, a_n) \in \mathbb{N}^{n-1}$, let $\delta(a)$ denote the number of delta sets Δ_i that contain a. Then to *merge* the Δ_i is to form the delta set $\Delta \subseteq \mathbb{N}^n$ consisting of all points $(j, a_2, \ldots, a_n)$, where $0 \leq j < \delta(a_2, \ldots, a_n)$.

The algorithm to construct $\Delta(\mathcal{P})$ is the following:

(1) Construct $T(\mathcal{P})$ from $\mathcal{P}$.
(2) If $n = 1$ then $\Delta(\mathcal{P})$ is $\{0, 1, \ldots, |\mathcal{P}| - 1\}$.
(3) Otherwise, let the subtrees of the root node of $T(\mathcal{P})$ be $S_1, \ldots, S_k$, and assume this algorithm has recursively constructed each $\Delta(P(S_i))$. Then $\Delta(\mathcal{P})$ is produced by merging the $\Delta(P(S_i))$, $1 \leq i \leq k$.

To illustrate this algorithm, we show how to produce a delta set from the tree $T(\mathcal{P})$ of Figure 1. For each node at the next-to-last level $n - 1$ of $T(\mathcal{P})$ we build the corresponding delta set. For a given node, this set is $\{0, 1, \ldots, t - 1\}$, where t is the number of children for the node. Next, for each node at level $n - 2$ we form the delta set by merging the delta sets for its children. We continue in this fashion, forming the delta sets for level k nodes by merging child delta sets from level $k + 1$. At the end, we produce the delta set for the root node of $T(\mathcal{P})$, which, as we prove in Theorem 8, is $\Delta(\mathcal{P})$. This process is shown in Figure 2 below. In the figure, we represent delta sets as trees. The top row shows the level $n - 1$ delta sets, next row the level $n - 2$ delta sets, and so on. The bottommost row shows the level 0 delta set, i.e., $\Delta(\mathcal{P})$. Arrows connecting the rows indicate which delta sets are merged to form the sets in the next row. Expressed as a set, the final delta set $\Delta(\mathcal{P})$ is $\{(0,0,0,0),\ (0,0,0,1),\ (0,0,0,2),\ (0,0,1,0),\ (0,0,1,1),\ (0,1,0,0),$ $(0,1,0,1),\ (0,2,0,0),\ (1,0,0,0),\ (1,0,0,1),\ (1,0,1,0),\ (1,1,0,0),\ (1,1,0,1)\}$.

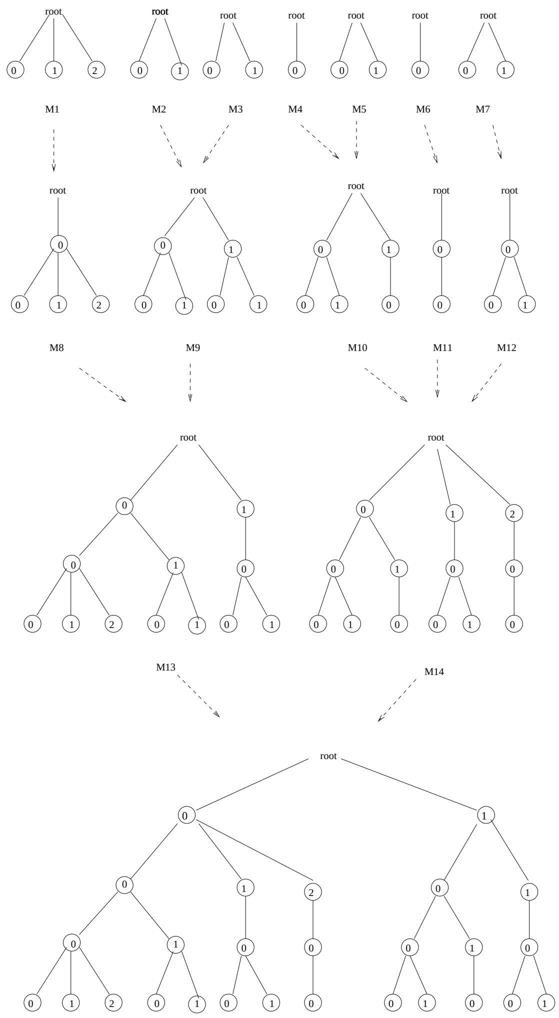

FIGURE 2. Merging delta sets to form $\Delta(\mathcal{P})$

Now we prove that the algorithm produces the correct result.

Theorem 8. *The delta set Δ the algorithm constructs equals $\Delta(\mathcal{P})$.*

Proof: Recall that Corollary 5 asserts

$$\Delta(\mathcal{P}) = \bigcup_{i=1}^{r} \big(\Delta(\mathcal{S}_{\leq i}) \otimes m_i\big). \tag{5}$$

In particular, $\mathcal{P}$ and $\Delta(\mathcal{P})$ have identical fibre structures, i.e., given m, the number of fibres of size m in $\mathcal{P}$ equals the number of fibres of the same size in $\Delta(\mathcal{P})$. Our strategy is to show that Δ equals the set on the right hand side of (5) above. We use the following facts:

(1) In a delta set, each fibre of size m consists of points whose trailing coordinates are $0, \ldots, m-1$.
(2) The set Δ contains the same number of points as does $\mathcal{P}$.
(3) Suppose $\mathcal{P}'$ is obtained from $\mathcal{P}$ by discarding one point, and let Δ' be the delta set the algorithm constructs from $T(\mathcal{P}')$. Then $\Delta' \subseteq \Delta$.
(4) The fibre structures of Δ and $\mathcal{P}$ are identical.

Facts (1) and (2) are obvious, and (3) follows from a straightforward induction on n. We prove (4) in Lemma 9 below.

Our proof is by simultaneous induction on n and $|\mathcal{P}|$, with the cases $n = 1$ and $|\mathcal{P}| = 1$ being clear. Assume first that $\mathcal{P}$ contains points p_1 and p_2 belonging to fibres of different sizes. For $i = 1, 2$ let $\mathcal{P}_i = \mathcal{P} \setminus \{p_i\}$ and let Δ_i be the set the algorithm constructs for $T(\mathcal{P}_i)$. Note the Δ_i cannot be identical because their fibre structures differ. Since $|\Delta| = |\mathcal{P}|$ and, for each i, $\Delta_i \subseteq \Delta$ and $|\Delta_i| = |\mathcal{P}| - 1$, it follows that $\Delta = \Delta_1 \cup \Delta_2$. Similar reasoning shows $\Delta(\mathcal{P}) = \Delta(\mathcal{P}_1) \cup \Delta(\mathcal{P}_2)$. The induction hypothesis on $|\mathcal{P}|$ implies $\Delta_i = \Delta(\mathcal{P}_i)$ for each i, so

$$\Delta = \Delta_1 \cup \Delta_2 = \Delta(\mathcal{P}_1) \cup \Delta(\mathcal{P}_2) = \Delta(\mathcal{P}).$$

This reduces the problem to the case where every fibre in $\mathcal{P}$ has the same size, say m.

Suppose $m > 1$. Let p be a point in $\mathcal{P}$, let $\mathcal{P}' = \mathcal{P} \setminus \{p\}$, and let Δ' be the delta set the algorithm constructs for $T(\mathcal{P}')$. The fibre structures of Δ' and $\mathcal{P}'$ agree, so Δ' contains exactly one fibre of size $m-1$, and Δ is obtained from Δ' by adding one point to this fibre. Similarly, $\Delta(\mathcal{P}')$ contains exactly one fibre of size $m-1$, and $\Delta(\mathcal{P})$ is obtained from $\Delta(\mathcal{P}')$ by adding one point to this fibre. In each case, the added point has $m-1$ as its last coordinate. Using the induction hypothesis on $|\mathcal{P}|$ we have $\Delta' = \Delta(\mathcal{P}')$, so $\Delta = \Delta(\mathcal{P})$.

Finally, suppose $m = 1$. The structure theorem tells us

$$\Delta(\mathcal{P}) = \Delta(\mathcal{S}) \otimes 1.$$

Note $T(\mathcal{S})$ is obtained by discarding each leaf node from $T(\mathcal{P})$. When $m = 1$, the last coordinate of every point in Δ is 0. A moment's reflection about the algorithm reveals that in this case, the last coordinate essentially plays no role when sets are merged. To make this precise, let Δ' denote the delta set the algorithm produces for $T(\mathcal{S})$. Then Δ is obtained by appending a trailing 0 to each point in Δ', i.e., $\Delta = \Delta' \otimes 1$. Since, by the induction hypothesis on n we have $\Delta' = \Delta(\mathcal{S})$, it follows that $\Delta = \Delta(\mathcal{P})$. □

To complete Theorem 8, the following remains to be shown:

Lemma 9. *The fibre structures of Δ and $\mathcal{P}$ are identical.*

Proof: The proof is by induction on $|\mathcal{P}|$, with the case $|\mathcal{P}| = 1$ being obvious. Suppose the smallest fibre in $\mathcal{P}$ has size m, and write $\mathcal{P}'$ for the set that results when a point from such a fibre is discarded. Let Δ' denote the delta set the algorithm produces for $T(\mathcal{P}')$. By the induction hypothesis, Δ' and $\mathcal{P}'$ have identical fibre structures. If $m > 1$, then Δ' contains exactly one fibre of size $m-1$. Since Δ is produced by adding a point to this fibre, the fibre structures of Δ and $\mathcal{P}$ are identical. If $m = 1$, then Δ contains one more fibre of size one than does Δ', so again the fibre structures of Δ and $\mathcal{P}$ are identical. $\square$

Corollary 10. *Let Δ be the delta set constructed by the algorithm for $T(\mathcal{P})$. The set $\{x^\alpha : \alpha \in \Delta\}$ is the monomial basis for the vanishing ideal of $\mathcal{P}$ with respect to the lexicographic order in R.*

The algorithm provides a way, with respect to the lexicographic order, to calculate the leading terms of each minimal Gröbner basis for $\mathbf{I}(\mathcal{P})$. Recall that $c \in \mathbb{N}^n$ is co-minimal for the delta set $D \subseteq \mathbb{N}^n$ if it is a minimal element of $\mathbb{N}^n \setminus D$.

Corollary 11. *Again let Δ be the delta set constructed by the algorithm for $T(\mathcal{P})$. The set of leading terms of every minimal Gröbner basis for the vanishing ideal of $\mathcal{P}$, with respect to the lexicographic order, is given by*

$$\{x^c : c \text{ is co-minimal for } \Delta\}.$$

5. Decomposing polynomial systems and an example

In this section we first show how our structure theorem can be used to decompose a system of equations into smaller systems, then illustrate the method with a nontrivial example.

Let $\mathbb{F}$ be a perfect field, let I be a zero-dimensional radical ideal in $\mathbb{F}[x_1, \ldots, x_n]$, and let $\mathcal{P}$ be the solution set in $\overline{\mathbb{F}}^n$. Suppose we have computed a Gröbner basis G for I under an elimination order for x_n. Let the distinct degrees of polynomials in G in x_n be $m_1 > \cdots > m_r > 0$. For $1 \le i \le r$, let G_i be the set

$$G_i = \{lt_{x_n}(g) : g \in G \text{ and } deg_{x_n}(g) < m_i\} \subseteq \mathbb{F}[x_1, \ldots, x_{n-1}]. \tag{6}$$

Let $J_1 = \langle G_1 \rangle$, and for $2 \le i \le r$ let J_i be a Gröbner basis for the ideal quotient $(\langle G_i \rangle : \langle G_{i-1} \rangle)$. Recall that for two ideals I, J in R, $(I : J)$ is defined to be

$$(I : J) = \{h \in R : hg \in I \text{ for all } g \in J\}.$$

Theorem 12. *For each $1 \le i \le r$, J_i is a Gröbner basis for the points in $\mathcal{S} = \pi(\mathcal{P})$ that are projections of fibres of size exactly m_i.*

Proof: By Theorem 6 the assertion is true for $J_1 = \langle G_1 \rangle$, so assume $i > 1$. Each G_i is a Gröbner basis for the points in $\mathcal{S}$ that are projections of fibres of size $\ge m_i$. Note that each ideal $\langle G_i \rangle$ is radical and zero-dimensional, as are the ideal quotients $(\langle G_i \rangle : \langle G_{i-1} \rangle)$. The zeros of $(\langle G_i \rangle : \langle G_{i-1} \rangle)$ are precisely the zeros of G_i that are not zeros of G_{i-1}, i.e., the points in $\mathcal{S}$ that are projections of fibres of size exactly m_i. $\square$

As an application of the above theorem, we consider an example from [19] concerning Nash equilibrium. The example describes a game with three players named Adam, Bob, and Carl. Each player has two pure strategies, and each plays his strategies with particular probabilities. Let a (respectively, b and c) be the probability that Adam (respectively, Bob and Carl) plays his first strategy. Obviously, $1 - a$ is the probability Adam plays his second, and similarly for Bob and Carl. The payoff for each player depends on the probabilities a, b, c via a payoff matrix.

A vector (a, b, c) is called a *Nash equilibrium* if no player can increase his payoff by changing his strategy (i.e., by changing the value of a, b, or c) while the other players keep their strategies fixed. The problem is to find all Nash equilibria for a given payoff matrix. Let x, y, and z denote the payoffs for Adam, Bob, and Carl respectively. For the game in [19, Section 6.2], the variables a, b, c, x, y, z must satisfy the following equations:

$$\begin{aligned}
a[x - 6b(1-c) - 11(1-b)c - (1-b)(1-c)] &= 0,\\
(1-a)[x - 6bc - 4b(1-c) - 6(1-b)c - 8(1-b)(1-c)] &= 0,\\
b[y - 12ac - 7a(1-c) - 6(1-a)c - 8(1-a)(1-c)] &= 0,\\
(1-b)[y - 10ac - 12a(1-c) - 8(1-a)c - (1-a)(1-c)] &= 0,\\
c[z - 11ab - 11a(1-b) - 3(1-a)b - 3(1-a)(1-b)] &= 0,\\
(1-c)[z - 14a(1-b) - 2(1-a)b - 7(1-a)(1-b)] &= 0.
\end{aligned}$$

For a valid solution, a, b, and c must take values in the interval $[0, 1]$, and the expressions in square brackets above must be nonnegative. It is shown in [19] that there are 16 solutions. We show below how Theorem 12 can be used to decompose the above polynomial system into smaller ones.

Let I be the ideal in $\mathbb{Q}[a, b, c, x, y, z]$ generated by the six polynomials in the above equations. By [19], I is in fact a zero-dimensional radical ideal. We compute the reduced Gröbner basis for I under the lexicographic order with $z > y > x > c > b > a$. The basis polynomials are listed below:

$$\begin{aligned}
g_1 &= z - 9cba - 5cb - ca + 4c + 9ba + 5b - 7a - 7,\\
g_2 &= y - 16cba + 9cb + 9ca - 7c + 12ba - 7b - 11a - 1,\\
g_3 &= x + 20cba - 4cb - 12ca + 2c - 9ba + 4b + 7a - 8,
\end{aligned}$$

$$\begin{aligned}
g_4 &= 45199440c^2 + (-62777000b^2 + 62777000b + 579451165ab^2 - 678659660a^3\\
&\quad +478183955a - 1290811744ab - 45199440 - 747553276a^2b + 146706560ba^4\\
&\quad +288499641a^2 - 88023936a^4 + 278457899a^2b^2 + 1905583540a^3b\\
&\quad -871834144b^2a^3)c - 293364085a - 202536477a^2b^2 - 1069473161a^3b\\
&\quad -66017952ba^4 - 523660995ab^2 + 392507815a^3 + 784474280ab\\
&\quad +351016833a^2b + 51347296a^4 - 150491026a^2 + 726197472b^2a^3,\\
g_5 &= (315b^2 - 512a^2b + 512ab - 315b)c - 384a^2b^2 + 404ab^2 - 245b^2 + 512a^2b\\
&\quad -532ab + 245b,\\
g_6 &= 8112(a^2 - a)c + 3500a^3 - 22232a^2 + 144900b^3a^2 - 179025b^3a - 13125b^3\\
&\quad +67200b^2a^3 - 264260a^2b^2 + 230810ab^2 + 23625b^2 - 7700a^3b + 82864a^2b\\
&\quad -74789ab - 10500b + 18732a,
\end{aligned}$$

$$
\begin{aligned}
g_7 &= 2075920b^3 + (-3736656 + 3077199a^3 - 3502876a^2 + 1641573a)b^2 + \\
&\quad (1660736 - 3661514a^3 + 2666801a^2 - 221183a)b - 332185a^3 + 1660925a^2 \\
&\quad -1328740a, \\
g_8 &= 5365293087(a^2 - a)b - 2920910449088a^5 + 2317354275384a^4 \\
&\quad -230893240320a^7 + 1520311154688a^6 + 18879018760a - 734785390742a^3 \\
&\quad +30044631318a^2, \\
g_9 &= 92160a^8 - 664704a^7 + 1547888a^6 - 1663252a^5 + 886352a^4 - 207367a^3 \\
&\quad +5255a^2 + 3668a.
\end{aligned}
$$

We see that x, y, z are completely determined by a, b, c, and g_1, g_2, g_3 give the interpolation polynomials, so we need only find all solutions (a, b, c). Consider the elimination ideals

$$I_1 = I \cap \mathbb{Q}[a], \quad I_2 = I \cap \mathbb{Q}[a, b], \quad I_3 = I \cap \mathbb{Q}[a, b, c].$$

Since we used the lexicographic order with $c > b > a$, we automatically get a Gröbner basis for each:

$$I_1 = \langle g_9 \rangle, \quad I_2 = \langle g_7, g_8, g_9 \rangle, \quad I_3 = \langle g_4, \ldots, g_9 \rangle.$$

We first decompose I_2 using Theorem 12 under the projection $(a, b) \mapsto a$. The degrees of b in $\{g_7, g_8, g_9\}$ are $3 > 1 > 0$, hence the fibre size of a zero a of I_1 is either 1 or 3. The zeros with fibre size 3 are determined by

$$\left\langle a^2 - a, g_9 \right\rangle = \left\langle a^2 - a \right\rangle,$$

hence the quotient ideal

$$(I_1 : \left\langle a^2 - a \right\rangle) = \langle h_9 \rangle$$

where

$$
\begin{aligned}
h_9 &= g_9/(a^2 - a) \\
&= 92160a^6 - 572544a^5 + 975344a^4 - 687908a^3 + 198444a^2 - 8923a - 3668
\end{aligned}
$$

determines the zeros with fibre size 1. Therefore, the fibres in $V(I_2)$ of size 3 are determined by

$$J_1 = \left\langle a^2 - a, g_7 \right\rangle = \left\langle a^2 - a, h_7 \right\rangle,$$

where

$$
\begin{aligned}
h_7 &= g_7 \bmod (a^2 - a) \\
&= 2075920b^3 + 1215896b^2 a - 3736656b^2 - 1215896ba + 1660736b.
\end{aligned}
$$

The fibres of size 1 in $V(I_2)$ are determined by

$$J_2 = \langle h_9, h_8 \rangle$$

where

$$
\begin{aligned}
h_8 &= \frac{g_8}{a^2 - a} = 5365293087b - 230893240320a^5 + 1289417914368a^4 \\
&\quad -1631492534720a^3 + 685861740664a^2 - 48923650078a - 18879018760.
\end{aligned}
$$

Therefore I_3 is decomposed into two subsystems

$$I_{33} = \langle g_4, g_5, g_6, J_1 \rangle, \quad I_{31} = \langle g_4, g_5, g_6, J_2 \rangle$$

corresponding to the fibres in $V(I_2)$ of sizes 3 and 1 respectively.

To further decompose I_{31} and I_{33}, we consider the projection $(a, b, c) \mapsto (a, b)$. A Gröbner basis for I_{31} under the lexicographic order with $c > b > a$ is

$$I_{31} = \langle h_9, h_8, h_6 \rangle$$

where

$$\begin{aligned} h_6 &= 75261732c + 11664829440a^5 - 65873451456a^4 + 86189973480a^3 \\ &\quad -38220173498a^2 + 3337199141a + 790000183. \end{aligned}$$

Since there is only one nonzero degree for c, I_{31} is not decomposable using Theorem 12. A Gröbner basis for I_{33} is

$$\begin{aligned} g_{31} &= 1782c^2 - 1782c - 235b^2a - 1925b^2 + 235ba + 1925b, \\ g_{32} &= 63(b^2 - b)c + 4b^2a - 49b^2 - 4ba + 49b, \\ g_{33} &= 70b^3 + 41b^2a - 126b^2 - 41ba + 56b, \\ g_{34} &= a^2 - a. \end{aligned}$$

Here c has two nonzero degrees, so I_{33} can be decomposed. In fact, the (a, b) with fibre size 2 are determined by

$$\left\langle b^2 - b, g_{33}, g_{34} \right\rangle = \left\langle b^2 - b, a^2 - a \right\rangle,$$

with the corresponding equation for c being $c^2 - c$ ($= g_{31}$ modulo $\left\langle b^2 - b, a^2 - a \right\rangle$), and the (a, b) with fibre size 1 are determined by

$$\left(\langle g_{33}, g_{34} \rangle : \left\langle b^2 - b, a^2 - a \right\rangle \right) = \left\langle a^2 - a, 70b + 41a - 56 \right\rangle,$$

with the corresponding c determined by $63c + 4a - 49 = g_{32}/(b^2 - b)$.

Therefore the original polynomial system I is decomposed into three subsystems:

$$\begin{aligned} &\left\langle g_1, g_2, g_3, c^2 - c, b^2 - b, a^2 - a \right\rangle, \\ &\left\langle g_1, g_2, g_3, 63c + 4a - 49, 70b + 41a - 56, a^2 - a \right\rangle, \\ &\langle g_1, g_2, g_3, I_{31} \rangle = \langle g_1, g_2, g_3, h_6, h_8, h_9 \rangle. \end{aligned}$$

The first two systems are easy to solve: the first has 8 solutions and the second two solutions. To further decompose the third system, one employs other tools, say factoring the univariate polynomial

$$h_9 = (12a - 7)(a - 4)(10a + 1)(2a - 1)(384a^2 - 472a + 131),$$

which gives 6 solutions. This gives all the 16 solutions for I.

References

[1] J. Abbott, A. Bigatti, M. Kreuzer and L. Robbiano, Computing ideals of points, *J. Symbolic Comput.* **30** (2000), 341-356.

[2] B. Buchberger and H. M. Möller, The construction of multivariate polynomials with preassigned zeros, *Computer Algebra, (Marseille, 1982)*, 24-31, *Lecture Notes in Comput. Sci.*, 144, Springer, Berlin-New York, 1982.

[3] L. Cerlienco and M. Mureddu, From algebraic sets to monomial linear bases by means of combinatorial algorithms, *Discrete Math.* **139** (1995), 73-87.

[4] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 2nd edition, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1996.
[5] D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics **185**, Springer-Verlag, New York, 1998.
[6] G-L. Feng and X. Giraud, Fast algorithms in Sudan decoding procedure for Reed-Solomon codes, preprint.
[7] J. Farr and S. Gao, Computing Gröbner bases for vanishing ideals of finite sets of points, in preparation.
[8] J. Farr and S. Gao, Computing general Padé approximations via Gröbner bases, in preparation.
[9] P. Fitzpatrick and J. Flynn, A Gröbner basis technique for Padé approximation, *J. Symbolic Comput.* **24** (1997), 575-589.
[10] P. Fitzpatrick and H. O'Keeffe, Gröbner basis solutions of constrained interpolation problems, Fourth special issue on linear systems and control, *Linear Algebra Appl.* **351/352** (2002), 533-551.
[11] M. Gasca and T. Sauer, Polynomial interpolation in several variables, *Adv. Comput. Math.* **12** (2000), 377-410.
[12] V. Guruswami and M. Sudan, Improved decoding of Reed-Solomon codes and algebraic-geometry codes, *IEEE Transactions on Information Theory*, **45** (1999), no. 6, 1757–1767.
[13] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra*, 1, Springer-Verlag, Berlin, 2000.
[14] R. Laubenbacher, J. Shah, and B. Stigler, A computational algebra approach to the identification of gene regulatory networks, *Proc. Third International Congress on Systems Biology*, Stockholm, Sweden, 2002.
[15] J. B. Little, D. Ortiz, R. Ortiz-Rosado, R. Pablo and K. Rios-Soto, Some remarks on Fitzpatrick and Flynn's Gröbner basis technique for Padé approximation, *J. Symbolic Computing* **35** (2003), 451-461.
[16] M. G. Marinari, H.M. Möller and T. Mora, Gröbner bases of ideals defined by functionals with an application to ideals of projective points, *Appl. Algebra Engrg. Comm. Comput.* **4** (1993), no. 2, 103-145.
[17] G. Pistone, E. Riccomagno, H. P. Wynn, *Algebraic Statistics: Computational Commutative Algebra in Statistics*, Monographs on Statistics & Applied Probability 89, Chapman & Hall/CRC, 2000.
[18] S. Sakata, On fast interpolation method for Guruswami-Sudan list decoding of one-point algebraic-geometry codes, *Proc. AAECC-14* (S. Boztas and I.E. Shparlinski, Eds.), LNCS 2227, pp. 172-182, 2001. Cambridge, 1998.
[19] B. Sturmfels, *Solving Systems of Polynomial Equations*, CBMS 97, AMS, 2002.
[20] M. Sudan, Decoding of Reed Solomon codes beyond the error-correction bound, *Journal of Complexity*, **13** (1997), no. 1, 180–193.

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, USA *E-mail address*: sgao@ces.clemson.edu

Faculdade de Matemática, PUCRS, Av. Ipiranga, 6681, Porto Alegre, RS 90619-900, Brazil, *E-mail address*: virginia@pucrs.br

Xilinx, Inc., 3100 Logic Drive, Longmont, Colorado 80503, USA, *E-mail address*: jeff.stroomer@xilinx.com