Parametric Gröbner bases

Geometry & applications

Andreas Bøgh Poulsen *201805425*

AARHUS
UNIVERSITET
INSTITUT FOR MATEMATIK

Supervisor: Niels Lauritzen

Contents

Introduction

1 Preliminaries

This project will assume familiarity with ring theory, multivariate polynomials over fields. A familiarity with Gröbner bases will be beneficial, but we will introduce the necesary notations and definitions. Let R be a Noetherian, commutative ring and $X = (x_1, x_2, \ldots, x_n)$ be an ordered collection of symbols. We denote the ring of polynomials in these variables $R[X]$. Given two (disjoint) sets of variables X and Y, we will use $R[X, Y]$ to mean $R[X \cup Y]$, which is naturally isomorphic to $R[X][Y]$. A monomial is a product of variables and a term is a monomial times a coefficient. We denote a monomial as X^v for some $v \in \mathbb{N}^n$.

1.1 · Definition (Monomial order, leading term). A *monomial order* is a total order $<$ on the set of monomials satisfying that $u < v \implies wu < wv$.

Given a monomial order $<$ and a polynomial $f \in R[X]$, the *leading term* of f is the term with the largest monomial w.r.t. $<$ and is denoted by $\mathrm{lt}_<(f)$. If $\mathrm{lt}_<(f) = a \cdot m$ for some monomial m and $a \in R$, then we denote $\mathrm{lm}_<(f) = m$ and $\mathrm{lc}_<(f) = a$. If $<$ is clear from context, it will be omitted.

These definitions naturally extend to sets of polynomials, so given a set of polynomials $F \subset k[X]$, we denote $\mathrm{lm}_<(F) := \{\mathrm{lm}_<(f) \mid f \in F\}$. The above definitions work over a general ring (and we will use that), for from here, we'll work over a field k. With this, we can give the definition of a Gröbner basis.

1.2 · Definition (Gröbner basis). Let $G \subset k[X]$ be a finite set of polynomials and $<$ be a monomial order. We say G is a *Gröbner basis* if $\langle \mathrm{lt}_<(G) \rangle = \mathrm{lt}_<(\langle G \rangle)$

2 Definitions and initial results

The purpose of this project is to study parametric Gröbner bases, so let's introduce those. The bare concept is rather simple.

2.1 · Definition (Parametric Gröbner basis). Let k, k_1 be fields, U and X be collections of variables and $F \subset k[U, X]$ be a finite set of polynomials. A *parametric Gröbner basis* is a finite set of polynomials $G \subset k[U, X]$ such that $\sigma(G)$ is a Gröbner basis of $\langle \sigma(F) \rangle$ for any ring homomorphism $\sigma : k[U] \to k_1$.

We call such a $\sigma : k[U] \to k_1$ a *specialization*. By the linearity of σ, all such ring homomorphisms can be characterized by their image of U. Thus, we can identify $\{\sigma : k[U] \to k_1 \mid \sigma \text{ is a ring hom.}\}$ with the affine space k_1^m when U has m elements. For $\alpha \in k_1^m$ we'll denote the corresponding map

$$\sigma_\alpha(u_i) = \alpha_i \quad \text{for } u_i \in U$$

extended linearly.

When we work with these parametric Gröbner bases, it will be more convenient to have a bit more information attached to them, namely which elements are required for which σ. Since σ is described by an $\alpha \in k_1^m$, we can restrict them using subsets of k_1^m.

2.2 · Definition (Vanishing sets & algebraic sets). Let E be a finite subset of $k[X]$. Then the *vanishing set* of E is $V(E) := \{v \in k^n \mid e(v) = 0 \ \ \forall e \in E\}$.

An *algebraic set* is a set of the form $V(E) \setminus V(N)$ for two finite subsets E and N of $k[X]$.

2.3 · Definition (Gröbner system). Let A be an algebraic set and $G \subset k[U,X]$ be a finite set. Then (A,G) is called a *segment of a Gröbner system* if $\sigma_\alpha(G)$ is a Gröbner basis of $\sigma_\alpha(\langle G\rangle)$ for all $\alpha \in A$. A set $\{(A_1,G_1),\dots,(A_t,G_t)\}$ is called a *Gröbner system* if each (A_i,G_i) is a segment of a Gröbner system.

2.4 · Example. *Let $X = \{x,y\}$ and $U = \{u\}$ and consider the polynomials $f(x,y,u) = ux^2+x$ and $g(x,y,u) = xy+1$. When $u \neq 0$, a Gröbner basis of $\langle f,g\rangle$ could be $(y-u, ux+1)$, whatever u may be.* TODO

Skriv om Kalkbrener

2.5 · Definition (Leading coefficient w.r.t. variables). Let $f \in k[U][X]$. Then the leading term of f is denoted $\mathrm{lt}_U(f)$, the leading coefficient is $\mathrm{lc}_U(f)$ and the leading monomial is $\mathrm{lm}_U(f)$. These notations are also used when $f \in k[U,X]$, just viewing f as a polynomial in $k[U][X]$.

Note that $\mathrm{lc}_U(f) \in k[U]$, i.e. the leading term is a polynomial in $k[U]$ times a monomial in X.

From this point, we assume that the monomial order on $k[U,X]$ satisfies $x > u$ for all $x \in X$ and $u \in U$. This monomial order restricts to a monomial order on $k[X]$, denoted by $<_X$. Note that this assumption is not too restrictive, as both the lexicographic, reverse lexicographic and graded versions of those satisfies this assumption.

2.6 · Lemma. *Let G be a Gröbner basis of an ideal $\langle F\rangle$ w.r.t. $<$, let $\alpha \in k_1^m$ and set $G_\alpha := \{\sigma_\alpha(g) \in G \mid \sigma_\alpha(\mathrm{lc}_U(g)) \neq 0\} = \{g_1,g_2,\dots,g_l\} \subset k_1[X]$. Then G_α is a Gröbner basis of the ideal $\langle\sigma_\alpha(F)\rangle$ w.r.t. $<_X$ if and only if $\sigma_\alpha(g)$ is reducible to 0 modulo G_α for every $g \in G$.*

Proof. To we written after Kalkbrener □

We will use this lemma in a slightly different formulation:

2.7 · Lemma. *Let $G = \{g_1,g_2,\dots,g_k\}$ be a Gröbner basis of an ideal $\langle F\rangle$ in $k[U,X]$ w.r.t $<$ and let $\alpha \in k_1^m$. If $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for each $g \in G \setminus (G \cap k[U])$, then $\sigma_\alpha(G)$ is a Gröbner basis of $\langle\sigma_\alpha(F)\rangle$.*

Proof. Let $G_\alpha = \{\sigma_\alpha(g) \mid \sigma_\alpha(\mathrm{lc}_U(g)) \neq 0\}$. If there is any $g \in G$, such that $\sigma_\alpha(g) \in k_1 \setminus \{0\}$, then $g \in G \cap k[U]$ since $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for all $g \in G \setminus K[U]$. Furthermore, since $g \in \langle F\rangle$, we get that $\langle\sigma_\alpha(F)\rangle = k_1[X]$ and $\sigma_\alpha(G)$ is a Gröbner basis.

If there is no such g, then $\alpha \in V(G \cap k[U])$. Take any $g \in G$. If $\sigma_\alpha(g) \in G_\alpha$, then $\mathrm{lt}(\sigma_\alpha(g)) = \sigma_\alpha(\mathrm{lc}_U(g)) \cdot \mathrm{lm}_U(g)$ since $x > u$ for all $x \in X$ and $u \in U$. Thus, $\sigma_\alpha(g)$ is reducible to 0 modulo G_α, since it's leading term is divisible by its own leading term. On the other hand, if $\sigma_\alpha(g) \notin G_\alpha$, then $\sigma_\alpha(g) = 0$, so is immediately reducible to zero. Thus $\sigma_\alpha(G)$ is a Gröbner basis of $\langle \sigma_\alpha(F) \rangle$ by lemma 2.6. □

With lemma 2.6 in mind, we can start constructing Gröbner systems. Let G be a reduced Gröbner basis of an ideal $\langle F \rangle \subset k[U, X]$, and let $H = \{\mathrm{lc}_U(g) \mid g \in G \setminus k[U]\}$. Then $\left(k_1^m \setminus \bigcup_{h \in H} V(h), G\right)$ is a segment of a Gröbner system. Thus, to make a Gröbner system, we need to find segments covering $\bigcup_{h \in H} V(h) = V(\mathrm{lcm}\{h \mid h \in H\})$.

If we take G to be a reduced Gröbner basis, then $h \notin \langle F \rangle$ for any $h \in H$ since then the corresponding leading term would be divisible by a leading term in G. This is not allowed when G is reduced. Hence, we can find a Gröbner basis G_1 of $F \cup \{h\}$, which will then form a segment $(k_1^m \setminus \bigcup_{h \in H_1} V(h), G_1)$ where $H_1 = \{\mathrm{lc}_U(g) \mid g \in G_1\}$. Since $k[U, X]$ is Noetherian, this will eventually stop, forming a Gröbner system.

This leads us to the first algorithm.