Comprehensive Gröbner Systems and QE

James Davenport

University of Bath

3 December 2019

$\mathcal{J}$=http://people.bath.ac.uk/masjhd/JHD-CA.pdf

JHD's interpretations: notes (A) etc. at end

Example

Consider first the example of $H_1 := \{x + 1, uy + x\} \subset \mathbf{Q}[u, x, y]$. Under any term order with $x < y$, this forms a (zero-dimensional) Gröbner base in $\mathbf{Q}(u)[x, y]$.

However, if we substitute $u = 0$, we get $\{x + 1, x\}$, which is not a Gröbner base at all.

If we consider instead $H_2 := \{x + 1, uy - 1\}$, which is equivalent in $\mathbf{Q}(u)[x, y]$, substituting $u = 0$ gives us $\{x + 1, -1\}$, which is a Gröbner basis (admittedly redundant) equivalent to $\{-1\}$ — no solutions. In fact H_2 is what we want — a Gröbner basis which is comprehensive in the informal sense that it is valid, not only for symbolic u, but for all values of u.

Definition

Definition

Let K be an integral domain, $R = K[u_1, \ldots, u_m]$ and $T = R[x_1, \ldots, x_n]$, and fix an ordering $\prec$ on the monomials in $x_1, \ldots, x_n$. Let G be a finite subset of T. G is said to be a *Comprehensive Gröbner basis* if, for all fields K' and all ring homomorphisms $\sigma : R \to K'$ (extended to homomorphisms $\sigma : T \to K'[x_1, \ldots, x_n]$), $\sigma(G)$ is a Gröbner basis (under $\prec$) in $K'[x_1, \ldots, x_n]$.

It is not obvious that these exist, but they do [Wei92, Theorem 2.7].

At least in principle, K could be $\mathbf{Z}$ and K' could be $\mathbf{F}_p$, but I haven't seen this explored, and most people assume K is a field.

Algebraic Partitions

Definition

Let K be an integral domain, $R = K[u_1, \ldots, u_m]$ and $S \subseteq K^m$. A finite set $\{S_1, \ldots, S_t\}$ of nonempty subsets of S is called an *algebraic partition* of S if it satisfies the following properties

1. $\bigcup_{i=1}^{t} S_i = S$.
2. $S_i \cap S_j = \emptyset$ if $i \neq j$.
3. For each i, $S_i = V_K(I_i^{(1)}) \setminus V_K(I_i^{(2)})$ for some ideals $I_i^{(1)}$, $I_i^{(2)}$ of R, where $V_K(I)$ is $V(I) \cap K^m$.

Each S_i is called a *segment*.

Note the close relationship with triangular sets: S_i would be referred to as a *quasi-variety*. But regular chains deals with very specific quasi-varieties: $V(T) \setminus V(\mathrm{lc}(T))$.
Note that K needn't be algebraically closed: again not much explored until now.

Comprehensive Gröbner System

Definition

Let $\{S_1, \ldots, S_t\}$ be an algebraic partition of $S \subseteq K^m$, let $T = R[x_1, \ldots, x_n]$, and fix an ordering $\prec$ on the monomials in $x_1, \ldots, x_n$. Let F be a finite subset of T. A finite set $\mathcal{G} := \{(S_1, G_1), \ldots, (S_s, G_s)\}$ satisfying the following properties is called a comprehensive Gröbner system (CGS) of F over S with parameters $u_1, \ldots, u_m$ w.r.t. $\leq$:

1. Each G_i is a finite subset of (F);
2. For each $\overline{c} \in S_i$, $G_i(\overline{c}) := \{g(\overline{c}, x_1, \ldots, x_n) | g(\overline{u}, x_1, \ldots, x_n) \in G_i\}$ is a Gröbner basis of the ideal $(F(\overline{c})$ in $C[x_1, \ldots, x_n]$ with respect to $\prec$, where $F(\overline{c}) := \{f(\overline{c}, x_1, \ldots, x_n) | f(\overline{u}, x_1, \ldots, x_n) \in F\}$
3. For each $\overline{c} \in S_i$, $\mathrm{lc}(g)(\overline{c}) \neq 0$ for any element g of G_i.

In addition, if each $G_i(\overline{c})$ is a minimal (reduced) Gröbner basis, G is said to be minimal (reduced). Being monic is not required. The question of local canonicity is discussed in [KY20].

Example Revisited

In the setting of the first example, we partition $\mathbf{Q}$ as $\{S_1 := \{0\}, S_2 := \mathbf{Q} \setminus S_1$. The Gröbner basis corresponding to S_2 is either H_1 or H_2 (or any other variant), and these are Gröbner bases by the gcd Criterion *as long as* the leading term of $uy + x$ is uy. Hence $u = 0$ is a special case, and our polynomials are $\underbrace{uy}_{=0} + x$ and $x + 1$, whose S-polynomial (or indeed reduction) is $\left(\underbrace{uy}_{=0} + x\right) - (x+1) = \underbrace{uy}_{=0} - 1$. So the Gröbner basis corresponding to S_1 is $\{uy - 1\}$.

Note the trick of "remembering" the phantom uy.

Let $\mathcal{F}(S)$ be the defining formula for S.

Computing a Comprehensive Gröbner System is conceptually straightforward: we start with the trivial partition $\{S\}$, and run Buchberger's Algorithm. Every time we have to decide on the zeroness or not of a leading coefficient, either in the $S(g_i, g_j) \stackrel{*}{\to}^G h$ step or in deciding whether $h = 0$ (directly or via the Criteria), and that decision depends on the u_i, i.e. whether a polynomial p in the u_i is zero or not, we split our set $S_i = V_K(I_i^{(1)}) \setminus V_K(I_i^{(2)})$ into $S_{i'} = V_K(I_i^{(1)} \cup \{p\}) \setminus V_K(I_i^{(2)})$ and $S_{i''} = V_K(I_i^{(1)}) \setminus V_K(I_i^{(2)} \cup \{p\})$ and continue Buchberger's Algorithm over each set separately, *but keeping* the apparently zero terms. In practice, the same polynomials p keep cropping up, and substantial ingenuity is needed to reduce or eliminate duplication. Again very similar to Regular Chains in terms of the duplication problem.

How are they connected?

Very simply.

Theorem ([Wei92, Proposition 3.4(i)])

If $\mathcal{G} := \{(S_1, G_1), \ldots, (S_s, G_s)\}$ *is a Comprehensive Gröbner System for* F *over* S, *then* $G' := \bigcup_{i=1}^{s} G_i$ *is a Comprehensive Gröbner Basis for* F *over* S.

"Theorem 1" [FIS15]: from [PRS93]

Let $\sigma(M)$ be the number of positive eigenvalues of M minus the number of negative ones.
Let I be a zero dimensional ideal in a polynomial ring $K[\overline{x}]$ with d roots (counted with multiplicity), $h \in K[\overline{x}]$. There is a $d \times d$ symmetric matrix M_h^I such that

$$\sigma(M_h^I) = \#(\{\overline{c} \in V_{\mathbf{R}}(I) | h(\overline{c}) > 0\}) - \#(\{\overline{c} \in V_{\mathbf{R}}(I) | h(\overline{c}) < 0\}).$$

In particular $\sigma(M_1^I) = \#(V_{\mathbf{R}}(I))$.
The recipe for $M_h^I$is given in [FIS15].
I am not sure what happens if h is zero at a root of I — I think the matrix is singular.

“Lemma 3” [FIS15]

Let I be a zero dimensional ideal and $h_1, \ldots, h_l$ be polynomials of $K[\overline{x}]$. For new variables $\overline{z} = z_1, \ldots, z_l$ let J be an ideal of $K[\overline{x}, \overline{z}]$ defined by $J = I + \langle z_1^2 - h_1, \ldots, z_l^2 - h_l \rangle$. Then the following equation holds.

$$\sigma(M_1^J) = 2^l \#(\{\overline{c} \in V_{\mathbf{R}}(I) | h_1(\overline{c}) > 0, \ldots, h_l(\overline{c}) > 0\}) > 0.$$

JHD notes that M will be a $d2^l \times d2^l$ matrix: the 2^l comes from counting $\pm\sqrt{h_i}$

“Lemma 7” [FIS15]

Let I be a zero dimensional ideal and $h_1, \ldots, h_l$ be polynomials of $K[\overline{x}]$. For new variables $\overline{z} = z_1, \ldots, z_l$ let J be an ideal of $K[\overline{x}, \overline{z}]$ defined by $J = I + \langle z_1 h_1 - 1, \ldots, z_l h_l - 1 \rangle$. Then the following equation holds.

$$\#(V_{\mathbf{R}}(J)) = \#(\{\overline{c} \in V_{\mathbf{R}}(I) | h_1(\overline{c}) \neq 0, \ldots, h_l(\overline{c}) \neq 0\}).$$

"Lemma 9" [FIS15]

Let I be a zero dimensional ideal and $h_1, \ldots, h_l$ be polynomials of $K[\overline{x}]$. For new variables $\overline{z} = z_1, \ldots, z_l$ let J be an ideal of $K[\overline{x}, \overline{z}]$ defined by $J = I + \langle z_1^2 - h_1, \ldots, z_l^2 - h_l \rangle$. Then the following equation holds.

$$\sigma(M_1^J) > 0 \Leftrightarrow \#(\{\overline{c} \in V_{\mathbf{R}}(I) | h_1(\overline{c}) \geq 0, \ldots, h_l(\overline{c}) \geq 0\}) > 0.$$

Again a $d2^l \times d2^l$ matrix.

"Lemma 12" [FIS15]

Let M be a real symmetric $d \times d$ matrix and $\chi(x) = x^d + \sum a_i x^i$ be its characteristic polynomial. Let $S_+(M)$ be the number of sign changes in the coefficients of $\chi(x)$, and $S_-(M)$ in $\chi(-x)$. Then S_+ is the number of positive roots of χ, and S_- the number of negative ones.

$$\underbrace{\#(V_{\mathbf{R}}(I)) = \sigma(M_1^I)} > 0 \Leftrightarrow S_+(M_1^I) \neq S_-(M_1^I)$$

We can write $S_+(M_1^I) \neq S_-(M_1^I)$ as a quantifier-free formula in the a_i: call this $I_d(a_{d-1}, \ldots, a_0)$.
No statements made about the complexity of this.

Basic QE setting [FIS15]: MainQE(S, ϕ)

We consider an "innermost block" in this form (C):

$$\exists \overline{x} \begin{pmatrix} f_1(\overline{y}, \overline{x}) = 0 \wedge \cdots f_r(\overline{y}, \overline{x}) = 0 \wedge \\ p_1(\overline{y}, \overline{x}) > 0 \wedge \cdots p_s(\overline{y}, \overline{x}) > 0 \wedge \\ q_1(\overline{y}, \overline{x}) \neq 0 \wedge \cdots q_t(\overline{y}, \overline{x}) \neq 0 \end{pmatrix}$$

$f_i, p_j, q_k \in \mathbf{Q}[\overline{y}, \overline{x}] \setminus \mathbf{Q}[\overline{y}]$.
Let $\overline{z}, \overline{w}$ be new variables with $\overline{z}, \overline{w} \succ \overline{x}$.
Let $\mathcal{G} = (S_i, G_i)$ be a CGS (parameters $\overline{y}$) over S (A) for

$$\{f_1, \ldots, f_r, \underbrace{z_1^2 p_1 - 1, \ldots, z_s^2 p_s - 1}_{\text{forcing positive}}, \underbrace{w_1 q_1 - 1, \ldots, w_t q_t - 1}_{\text{forcing nonzero}}\}$$

Claim

Each G_i will be
$\{f_1', \ldots, f_{r'}', u_1 z_1^2 - p_1', \ldots, u_s z_s^2 - p_s', v_1 w_1 - q_1', \ldots, v_t w_t - q_t'\}$.

Our answer will be $\bigvee_i \Psi_i(S_i, G_i)$: next two slides explain Ψ_i.

G_i zero-dimensional ($\overline{z}, \overline{w}$ irrelevant for dimension)

If $G_i = (1)$ then we return `false`. Otherwise recall
$G_i = \{f'_1, \ldots, f'_{r'}, u_1 z_1^2 - p'_1, \ldots, u_s z_s^2 - p'_s, v_1 w_1 - q'_1, \ldots, v_t w_t - q'_t\}$.
Let $I = \langle f'_1, \ldots, f'_{r'} \rangle$,

$$\chi(x) = \prod_{(e_1,\ldots,e_s)\in\{0,1\}^s} \chi^I_{(p'_1/u_1)^{e_1},\cdots,(p'_s/u_s)^{e_s}}(x) = x^{2^s d} + \sum_0^{2^s d-1} a_i x^i.$$

The answer is $\Psi_i := \mathcal{F}(S_i) \wedge I_{2^s d}(a_i)$.
JHD: at least that's my reconstruction. I can't see where the w_i (the $\neq 0$) terms come in. Also, the subscript of $\chi^I_{\ldots}$, the characteristic polynomial of $M^I_{\ldots}$, is not a polynomial.

$\exists\phi$: $G_i > 0$-dimensional ($\overline{z}, \overline{w}$ irrelevant for dimension)

$\overline{u} :=$ maximal independent variables $(\overline{x}, G_i, \succ)$. (B)
If $\overline{u} = \overline{x}$ return SYNRAC$(\mathcal{F}(S) \wedge \exists\overline{x}\phi)$ [Wei98]
$\overline{x}' := \overline{x} \setminus \overline{u}$; $\phi_1 := \texttt{Free}(\phi, \overline{x}')$; $\phi_2 := \texttt{NonFree}(\phi, \overline{x}')$;
$\varphi := \phi_1 \wedge \text{Recurse}(S_i, \exists\overline{x}'\phi_2)$ (1)
JHD: I think this means φ now only contains $\overline{u}$-variables
Let $\varphi_1 \vee \cdots \vee \varphi_l$ be a disjunctive normal form of φ. (C)
for $1 \leq j \leq l$ **do**
$\varphi_j^{(1)} := \texttt{Free}(\varphi, \overline{u})$; $\varphi_j^{(2)} := \texttt{NonFree}(\varphi_j, \overline{u})$;
$\psi_j := \varphi_j^{(1)} \wedge \text{Recurse}(S_i, \exists\overline{u}\phi_j^{(2)})$ (2)(E)
Return $\Psi := \mathcal{F}(S_i) \wedge (\psi_1 \vee \cdots \vee \psi_l)$
JHD: "Recurse" goes right back to the MainQE, note that call (1) has pushed the $\overline{u}$-variables into being parameters (I think) (D). But somehow S_i gets lost in these recursions: I hope I've added it in the right place. Their Theorem 16 states that this does terminate — far from obvious (F).

JHD notes

- (A) Recursing with S is, I think, my interpolation to make sense of the recursions we'll see later. S initially is $\mathbf{R}^{\#\overline{y}}$.
- (B) There's a lot of freedom here: ML?
- (C) Note that our main recursion is on ϕ in conjunctive normmal form (CNF), whereas here we convert to disjunctive normal form (DNF) and implicitly back at the end of the block. Since CNF$\leftrightarrow$DNF naïvely is exponential, this would provide an exponential blowup at each $\exists/\forall$ boundary, similar to [DH88].
- (D) Therefore this recursion is on strictly fewer variables, since dim > 0.
- (E) Therefore this recursion is on strictly fewer variables, since $\overline{u} \neq \overline{x}$. $\varphi_j^{(1)}$ is free of $\overline{u}$ by construction, and free of $\overline{x}'$ since it comes from ϕ_1, so actually belongs in an outer block. We might ask why such things exist, but they could be generated by the recursion.
- (F) But the two previous notes are probably key.

Bibliography I

J.H. Davenport and J. Heintz.
Real Quantifier Elimination is Doubly Exponential.
J. Symbolic Comp., 5:29–35, 1988.

R. Fukasaku, H. Iwane, and Y. Sato.
Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems.
In D. Robertz, editor, *Proceedings ISSAC 2015*, pages 173–180, 2015.

D. Kapur and Y. Yang.
An Algorithm for Computing a Minimal Comprehensive Gröbner Basis of a Parametric Polynomial System.
https://arxiv.org/abs/2003.07957, 2020.

P. Pedersen, M.-F. Roy, and A. Szpirglas.
Counting Real Zeroes in the Multivariate Case.
In *Proceedings MEGA '92*, pages 203–224, 1993.

Bibliography II

V. Weispfenning.
Comprehensive Gröbner Bases.
J. Symbolic Comp., 14:1–29, 1992.

V. Weispfenning.
A New Approach to Quantifier Elimination for Real Algebra.
Quantifier Elimination and Cylindrical Algebraic Decomposition, pages 376–392, 1998.