Parametric Gröbner basis Computation and Elimination

Deepak Kapur

Department of Computer Science
University of New Mexico
Albuquerque, NM, USA

Joint work with Sun Yao and Dingkang Wang and Yiming Yang

Newton Institute, Cambridge

July 27, 2017

Background

- Gröbner basis was first proposed as a special basis of polynomial ideals by Buchberger (1965), where he also gave an algorithm to construct it.

Background

- Gröbner basis was first proposed as a special basis of polynomial ideals by Buchberger (1965), where he also gave an algorithm to construct it.
- Comprehensive Gröbner system(CGS) and comprehensive Gröbner basis(CGB) were proposed by Weispfenning(1992) for parametric polynomial systems.

Background

- Gröbner basis was first proposed as a special basis of polynomial ideals by Buchberger (1965), where he also gave an algorithm to construct it.
- Comprehensive Gröbner system(CGS) and comprehensive Gröbner basis(CGB) were proposed by Weispfenning(1992) for parametric polynomial systems.
- Parametric Gröbner basis was proposed independently by Kapur (1994).

Main Applications of Comprehensive Gröbner System

1. solving systems of parametric polynomials under various specializations.
2. grouping together structurally similar polynomial systems under various specializations.
3. study the solution structure, such as dimension, leading terms, of a parametric system.
4. automatic geometric theorem proving and geometric theorem discovery.
5. geometric reasoning in model based scene analysis and image understanding.
6. program analysis – automatic generation of loop invariants.
7. analysis of equalities appearing in a problem formulated in the theory of real closed field.

Motivation

Example

Let $F = \{ax^2 + by^2, cx^2 + y^2, ax - cy\}$ where $\{x, y\}$ are unknowns and $\{a, b, c\}$ are parameters. Solve

$$\begin{cases} ax^2 + by^2 = 0, \\ cx^2 + y^2 = 0, \\ ax - cy = 0. \end{cases}$$

for different values of parameters.

Motivation

Example

Let $F = \{ax^2 + by^2, cx^2 + y^2, ax - cy\}$ where $\{x, y\}$ are unknowns and $\{a, b, c\}$ are parameters. Solve

$$\begin{cases} ax^2 + by^2 = 0, \\ cx^2 + y^2 = 0, \\ ax - cy = 0. \end{cases}$$

for different values of parameters.

- A specialization $\sigma_{(1,2,3)}$ deduced by $(1, 2, 3) \in \mathbb{Q}^3$ is to set $a = 1$, $b = 2$ and $c = 3$. $\sigma_{(1,2,3)}(ax^2 + by^2) = x^2 + 2y^2$.

Motivation

Example

Let $F = \{ax^2 + by^2, cx^2 + y^2, ax - cy\}$ where $\{x, y\}$ are unknowns and $\{a, b, c\}$ are parameters. Solve

$$\begin{cases} ax^2 + by^2 = 0, \\ cx^2 + y^2 = 0, \\ ax - cy = 0. \end{cases}$$

for different values of parameters.

- A specialization $\sigma_{(1,2,3)}$ deduced by $(1, 2, 3) \in \mathbb{Q}^3$ is to set $a = 1$, $b = 2$ and $c = 3$. $\sigma_{(1,2,3)}(ax^2 + by^2) = x^2 + 2y^2$. Similarly

  for other polynomials, we get $3x^2 + y^2, x - 3y$.

Motivation

Example

Let $F = \{ax^2 + by^2, cx^2 + y^2, ax - cy\}$ where $\{x, y\}$ are unknowns and $\{a, b, c\}$ are parameters. Solve

$$\begin{cases} ax^2 + by^2 = 0, \\ cx^2 + y^2 = 0, \\ ax - cy = 0. \end{cases}$$

for different values of parameters.

- A specialization $\sigma_{(1,2,3)}$ deduced by $(1, 2, 3) \in \mathbb{Q}^3$ is to set $a = 1$, $b = 2$ and $c = 3$. $\sigma_{(1,2,3)}(ax^2 + by^2) = x^2 + 2y^2$. Similarly

  for other polynomials, we get $3x^2 + y^2, x - 3y$.
- Different specializations lead to different systems.

What is a Gröbner Basis?

Given a polynomial ideal generated by a basis $\{f, g, h\}$, its Gröbner basis is a special basis with very nice properties:

- Polynomials are viewed as simplification rules which simplify polynomials and simplification always terminates.

What is a Gröbner Basis?

Given a polynomial ideal generated by a basis $\{f, g, h\}$, its Gröbner basis is a special basis with very nice properties:

- Polynomials are viewed as simplification rules which simplify polynomials and simplification always terminates.
- Every polynomial in the ideal simplifies to 0 using its Gröbner basis.

What is a Gröbner Basis?

Given a polynomial ideal generated by a basis $\{f, g, h\}$, its Gröbner basis is a special basis with very nice properties:

- Polynomials are viewed as simplification rules which simplify polynomials and simplification always terminates.
- Every polynomial in the ideal simplifies to 0 using its Gröbner basis.
- Every polynomial simplifies to a unique normal form (also called the canonical form) of the polynomial based on the term ordering used.

Properties of Gröbner bases

- Once a term ordering is fixed, the reduced Gröbner basis of an ideal is unique.

Properties of Gröbner bases

- Once a term ordering is fixed, the reduced Gröbner basis of an ideal is unique.
- Using lexicographic ordering on terms, a Gröbner basis has a nice structure from which common zeros of polynomials can be computed.

Properties of Gröbner bases

- Once a term ordering is fixed, the reduced Gröbner basis of an ideal is unique.
- Using lexicographic ordering on terms, a Gröbner basis has a nice structure from which common zeros of polynomials can be computed.
- If a polynomial system has no solution, its Gröbner basis consists of a nonzero constant.

Buchberger's Algorithm for Computing a Gröbner basis

- Define an admissible term ordering: $t \geq 1$, and $t_1 \geq t_2 \implies s * t_1 \geq s * t_2$ for any term s.

Buchberger's Algorithm for Computing a Gröbner basis

- Define an admissible term ordering: $t \geq 1$, and $t_1 \geq t_2 \implies s * t_1 \geq s * t_2$ for any term s.
- Make simplification rules from polynomials by making the largest term to be the left side and the minus of the remaining polynomial to be the right side.

Buchberger's Algorithm for Computing a Gröbner basis

- Define an admissible term ordering: $t \geq 1$, and $t_1 \geq t_2 \implies s * t_1 \geq s * t_2$ for any term s.
- Make simplification rules from polynomials by making the largest term to be the left side and the minus of the remaining polynomial to be the right side.
- Using the above ordering, simplification by polynomials is guaranteed to terminate.

Buchberger's Algorithm for Computing a Gröbner basis

- Define an admissible term ordering: $t \geq 1$, and $t_1 \geq t_2 \implies s * t_1 \geq s * t_2$ for any term s.
- Make simplification rules from polynomials by making the largest term to be the left side and the minus of the remaining polynomial to be the right side.
- Using the above ordering, simplification by polynomials is guaranteed to terminate.
- Generate new rules/polynomials from existing polynomials using **superpositions (S-polynomials)** and simplification to achieve confluence.

Buchberger's Algorithm for Computing a Gröbner basis

- Define an admissible term ordering: $t \geq 1$, and $t_1 \geq t_2 \implies s * t_1 \geq s * t_2$ for any term s.
- Make simplification rules from polynomials by making the largest term to be the left side and the minus of the remaining polynomial to be the right side.
- Using the above ordering, simplification by polynomials is guaranteed to terminate.
- Generate new rules/polynomials from existing polynomials using **superpositions (S-polynomials)** and simplification to achieve confluence.
- Algorithm terminates when no new rules can be generated.

Buchberger's Algorithm for Computing a Gröbner basis

- Define an admissible term ordering: $t \geq 1$, and $t_1 \geq t_2 \implies s * t_1 \geq s * t_2$ for any term s.
- Make simplification rules from polynomials by making the largest term to be the left side and the minus of the remaining polynomial to be the right side.
- Using the above ordering, simplification by polynomials is guaranteed to terminate.
- Generate new rules/polynomials from existing polynomials using **superpositions (S-polynomials)** and simplification to achieve confluence.
- Algorithm terminates when no new rules can be generated.
- Upon termination algorithm gives a Gröbner basis.

Illustration of Gröbner Basis Algorithm

- Multivariate Polynomials: $x^2 - 4x + y^2 = 0$, $xy = 1$.

Illustration of Gröbner Basis Algorithm

- Multivariate Polynomials: $x^2 - 4x + y^2 = 0$, $xy = 1$.

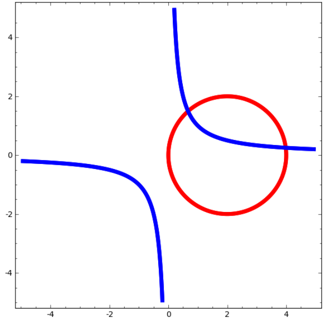
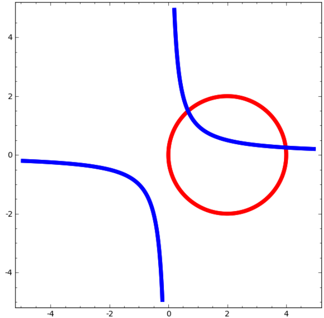


Illustration of Gröbner Basis Algorithm

- Multivariate Polynomials: $x^2 - 4x + y^2 = 0$, $xy = 1$.



- Computing intersection points of the curves (which is the same as common solutions).

Illustration of Gröbner Basis Algorithm

Example

$$\begin{array}{llll} 1. & y^2 & \rightarrow & -x^2 + 4x \\ 2. & xy & \rightarrow & 1 \end{array}$$

Illustration of Gröbner Basis Algorithm

Example

$$
\begin{array}{llll}
1. & y^2 & \rightarrow & -x^2 + 4x \\
2. & xy & \rightarrow & 1
\end{array}
$$

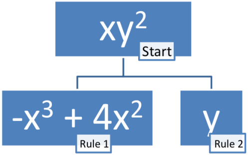
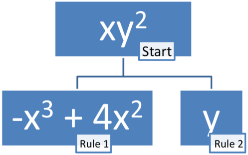


Illustration of Gröbner Basis Algorithm

Example

$$\begin{array}{llll} 1. & y^2 & \to & -x^2 + 4x \\ 2. & xy & \to & 1 \end{array}$$

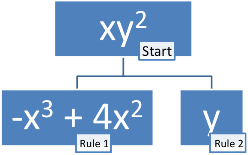


- 3. $y \to -x^3 + 4x^2$.

Illustration of Gröbner Basis Algorithm

Example

$$
\begin{array}{llll}
1. & y^2 & \rightarrow & -x^2 + 4x \\
2. & xy & \rightarrow & 1
\end{array}
$$

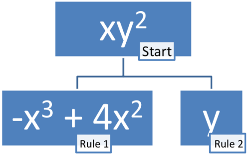


- 3. $y \rightarrow -x^3 + 4x^2$.
- Simplifying the second polynomial: 4. $x^4 - 4x^3 + 1 = 0$.

Illustration of Gröbner Basis Algorithm

Example

$$\begin{array}{llll} 1. & y^2 & \to & -x^2 + 4x \\ 2. & xy & \to & 1 \end{array}$$

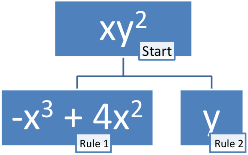


- 3. $y \to -x^3 + 4x^2$.
- Simplifying the second polynomial: 4. $x^4 - 4x^3 + 1 = 0$.
- First polynomial simplifies to 0 using 2 and 3. $\{4.\quad x^4 - 4x^3 + 1, 3.\quad y + x^3 - 4x^2\}$ is a Groebner basis.

Illustration of Gröbner Basis Algorithm

Example

$$\begin{array}{llll} 1. & y^2 & \to & -x^2+4x \\ 2. & xy & \to & 1 \end{array}$$



- 3. $y \to -x^3 + 4x^2$.
- Simplifying the second polynomial: 4. $x^4 - 4x^3 + 1 = 0$.
- First polynomial simplifies to 0 using 2 and 3. $\{4. \quad x^4 - 4x^3 + 1, 3. \quad y + x^3 - 4x^2\}$ is a Groebner basis.
- x and y coordinates of the four intersection points can be obtained from 4th and 3rd polynomials, resp.

Termination of Gröbner basis Algorithm

The process of generating additional rules always terminate because of a very elegant and simple combinatorial result from number theory:

Dickson's Lemma

Every infinite subset of N^k has at least two comparable k-tuples where comparison is done component-wise. $(a, b) \geq (c, d)$ iff $a \geq c \wedge b \geq d$.

Parametric Polynomial Systems

Example

Let $F = \langle ax^2 + by^2, cx^2 + y^2, ax - cy \rangle$ where $\{x, y\}$ are unknowns and $\{a, b, c\}$ are parameters.

$$\begin{cases} ax^2 + by^2 = 0, \\ cx^2 + y^2 = 0, \\ ax - cy = 0. \end{cases}$$

Parametric Polynomial Systems

Example

Let $F = \langle ax^2 + by^2, cx^2 + y^2, ax - cy \rangle$ where $\{x, y\}$ are unknowns and $\{a, b, c\}$ are parameters.

$$\begin{cases} ax^2 + by^2 = 0, \\ cx^2 + y^2 = 0, \\ ax - cy = 0. \end{cases}$$

- Different specializations lead to different systems.
  - The Gröbner basis for $\sigma_{(0,1,0)}(F)$ = (y^2) is $\{y^2\}$.
  - The Gröbner basis for $\sigma_{(1,2,1)}(F)$ = $(x^2 + 2y^2, x^2 + y^2, x - y)$ is $\{x - y, y^2\}$.

Comprehensive (Parametric) Gröbner Basis

A finite set $CGB \subset \langle F \rangle$ is a comprehensive Gröbner basis iff for every specialization σ of parameters, $\sigma(CGB)$ is a Gröbner basis of $\sigma(\langle F \rangle)$.

Comprehensive (Parametric) Gröbner Basis

A finite set $CGB \subset \langle F \rangle$ is a comprehensive Gröbner basis iff for every specialization σ of parameters, $\sigma(CGB)$ is a Gröbner basis of $\sigma(\langle F \rangle)$.

It is desirable to have $CGB \subset \langle F \rangle$.

Comprehensive Gröbner System

- Identify groups of specializations σ's that share the same Gröbner basis for the specialized ideal $\sigma(\langle F \rangle)$.

Comprehensive Gröbner System

- Identify groups of specializations σ's that share the same Gröbner basis for the specialized ideal $\sigma(\langle F \rangle)$.
- For each such set of specialization, compute the respective Gröbner basis.

Algorithms for Computing CGS and CGB

- Algorithms for computing CGS:

Algorithms for Computing CGS and CGB

- Algorithms for computing CGS:
  - Weispfenning (1992, 2003), Kapur (1995), Montes (2002), Wang (2004), Suzuki-Sato (2003, 2006), Nabeshima (2007), Manubens-Montes (2009), Kapur-Sun-Wang (2010, 2011);

Algorithms for Computing CGS and CGB

- Algorithms for computing CGS:
  - Weispfenning (1992, 2003), Kapur (1995), Montes (2002), Wang (2004), Suzuki-Sato (2003, 2006), Nabeshima (2007), Manubens-Montes (2009), Kapur-Sun-Wang (2010, 2011);
- Algorithms for computing CGB:

Algorithms for Computing CGS and CGB

- Algorithms for computing CGS:
  - Weispfenning (1992, 2003), Kapur (1995), Montes (2002), Wang (2004), Suzuki-Sato (2003, 2006), Nabeshima (2007), Manubens-Montes (2009), Kapur-Sun-Wang (2010, 2011);
- Algorithms for computing CGB:
  - Weispfenning (1992, 2003), Suzuki-Sato (2006), Kapur-Sun-Wang (2011), Kapur-Yang (2014), Kapur-Yang (2015).

Algorithms for Computing CGS and CGB

- Algorithms for computing CGS:
  - Weispfenning (1992, 2003), Kapur (1995), Montes (2002), Wang (2004), Suzuki-Sato (2003, 2006), Nabeshima (2007), Manubens-Montes (2009), Kapur-Sun-Wang (2010, 2011);
- Algorithms for computing CGB:
  - Weispfenning (1992, 2003), Suzuki-Sato (2006), Kapur-Sun-Wang (2011), Kapur-Yang (2014), Kapur-Yang (2015).
- Gröbner Cover: Wibmer (2007), Montes-Wibmer (2010).

Comprehensive Gröbner System and Basis

- Comprehensive Gröbner system(CGS): $\{(A_1, G_1), \cdots, (A_l, G_l)\}$ for a finite basis F of a parametric ideal $\langle F \rangle$, where $\mathbb{C}^3 = A_1 \cup \cdots \cup A_l$ and $G_1, \cdots, G_l \subset \mathbb{Q}[a, b, c][x, y]$, s.t. $\sigma_\alpha(G_i)$ is a Gröbner basis for $\langle \sigma_\alpha(F) \rangle$ for $\forall \alpha \in A_i$..

  Each A_i is specified by a finite set of polynomial equality constraints and a finite set of polynomial disequality constraints over the parameters.

$$\{(A_i, G_i)\} = \begin{cases} \mathbb{C}^3 \setminus V(abc - a^2), & \{ax - cy, (bc - a)y^2\} \\ V(a) \setminus V(c), & \{cy, cx^2 + y^2\} \\ V(a, c), & \{y^2\} \\ V(bc - a) \setminus V(ab^2 + ac), & \{ax - cy, (b^2 + c)y^2\} \\ V(bc - a, b^2 + c, ab + c^2, c^3 + a^2) \setminus V(ac), & \{c^2 x + bcy\} \end{cases}$$

Comprehensive Gröbner System and Basis

- Comprehensive Gröbner system(CGS): $\{(A_1, G_1), \cdots, (A_l, G_l)\}$ for a finite basis F of a parametric ideal $\langle F\rangle$, where $\mathbb{C}^3 = A_1 \cup \cdots \cup A_l$ and $G_1, \cdots, G_l \subset \mathbb{Q}[a, b, c][x, y]$, s.t. $\sigma_\alpha(G_i)$ is a Gröbner basis for $\langle\sigma_\alpha(F)\rangle$ for $\forall\alpha \in A_i$..
  Each A_i is specified by a finite set of polynomial equality constraints and a finite set of polynomial disequality constraints over the parameters.

$$\{(A_i, G_i)\} = \begin{cases} \mathbb{C}^3 \setminus V(abc - a^2), & \{ax - cy, (bc - a)y^2\} \\ V(a) \setminus V(c), & \{cy, cx^2 + y^2\} \\ V(a, c), & \{y^2\} \\ V(bc - a) \setminus V(ab^2 + ac), & \{ax - cy, (b^2 + c)y^2\} \\ V(bc - a, b^2 + c, ab + c^2, c^3 + a^2) \setminus V(ac), & \{c^2x + bcy\} \end{cases}$$

- Comprehensive Gröbner basis(CGB): $G \subset \langle F\rangle \subset \mathbb{Q}[a, b, c][x, y]$, s.t. $\sigma_\alpha(G)$ is a Gröbner basis for $\langle\sigma_\alpha(F)\rangle$.

$$G = \{ax - cy, (bc - a)y^2, cx^2 + y^2, (bc - a)xy + (b^2 + c)y^2, abx - bcy\}.$$

A Typical Comprehensive Gröbner System Algorithm

- Compute a Gröbner basis of $\langle F \rangle$ using a block ordering in which parameters are smaller than variables.

A Typical Comprehensive Gröbner System Algorithm

- Compute a Gröbner basis of $\langle F \rangle$ using a block ordering in which parameters are smaller than variables.
- Does the Gröbner basis include polynomials purely in parameters? If so, for every specialization σ not satisfying any of these parametric polynomials, the Gröbner basis of $\sigma(\langle F \rangle)$ is $\{1\}$, since there are no common solutions.

A Typical Comprehensive Gröbner System Algorithm

- Compute a Gröbner basis of $\langle F \rangle$ using a block ordering in which parameters are smaller than variables.
- Does the Gröbner basis include polynomials purely in parameters? If so, for every specialization σ not satisfying any of these parametric polynomials, the Gröbner basis of $\sigma(\langle F \rangle)$ is $\{1\}$, since there are no common solutions.
- For other specializations (above parametric equalities are assumed to hold), consider other polynomials in the Gröbner basis as polynomials in variables with the coefficients of terms being polynomials in parameters.

A Typical Comprehensive Gröbner System Algorithm

- Compute a Gröbner basis of $\langle F \rangle$ using a block ordering in which parameters are smaller than variables.
- Does the Gröbner basis include polynomials purely in parameters? If so, for every specialization σ not satisfying any of these parametric polynomials, the Gröbner basis of $\sigma(\langle F \rangle)$ is $\{1\}$, since there are no common solutions.
- For other specializations (above parametric equalities are assumed to hold), consider other polynomials in the Gröbner basis as polynomials in variables with the coefficients of terms being polynomials in parameters.
  - For the leading coefficients of the leading terms of these polynomials, perform case analysis assuming the leading coefficients are nonzero as well as zeros.

A Typical Comprehensive Gröbner System Algorithm

- Compute a Gröbner basis of $\langle F \rangle$ using a block ordering in which parameters are smaller than variables.
- Does the Gröbner basis include polynomials purely in parameters? If so, for every specialization σ not satisfying any of these parametric polynomials, the Gröbner basis of $\sigma(\langle F \rangle)$ is $\{1\}$, since there are no common solutions.
- For other specializations (above parametric equalities are assumed to hold), consider other polynomials in the Gröbner basis as polynomials in variables with the coefficients of terms being polynomials in parameters.
  - For the leading coefficients of the leading terms of these polynomials, perform case analysis assuming the leading coefficients are nonzero as well as zeros.
  - Such a case analysis gives possibly many branches.

A Typical Comprehensive Gröbner System Algorithm

- Compute a Gröbner basis of $\langle F \rangle$ using a block ordering in which parameters are smaller than variables.
- Does the Gröbner basis include polynomials purely in parameters? If so, for every specialization σ not satisfying any of these parametric polynomials, the Gröbner basis of $\sigma(\langle F \rangle)$ is $\{1\}$, since there are no common solutions.
- For other specializations (above parametric equalities are assumed to hold), consider other polynomials in the Gröbner basis as polynomials in variables with the coefficients of terms being polynomials in parameters.
  - For the leading coefficients of the leading terms of these polynomials, perform case analysis assuming the leading coefficients are nonzero as well as zeros.
  - Such a case analysis gives possibly many branches.
- Repeat this process until all branches have been generated (i.e., all possible parametric specializations have been considered).

Key Idea of Kapur, Sun and Wang's algorithm (ISSAC 2010)

Among a set of polynomials which are candidates for inclusion in a Gröbner basis of a branch, it suffices to consider only those polynomials whose leading terms in **variables** are minimal and noncomparable to each others (since polynomials with leading comparable terms can be used to simplify each other).

Illustration

Example

Let $F := \{ax^2 + by^2, cx^2 + y^2, ax - cy\} \subset \mathbb{Q}[a, b, c][x, y]$ where $\{x, y\}$ are variables and $\{a, b, c\}$ are parameters.

- Gröbner basis for $\langle F \rangle \subset \mathbb{Q}[x, y, a, b, c]$ w.r.t. $x, y \gg a, b, c$.

$$G = \{ax - cy, (bc - a)y^2, (ab + c^2)y^2, (c^3 + a^2)y^2,$$

$$cxy + by^2, cx^2 + y^2, (b^2 + c)y^3, bxy^2 - y^3\}.$$

Illustration

Example

Let $F := \{ax^2 + by^2, cx^2 + y^2, ax - cy\} \subset \mathbb{Q}[a, b, c][x, y]$ where $\{x, y\}$ are variables and $\{a, b, c\}$ are parameters.

- Gröbner basis for $\langle F \rangle \subset \mathbb{Q}[x, y, a, b, c]$ w.r.t. $x, y \gg a, b, c$.

$$G = \{ax - cy, (bc - a)y^2, (ab + c^2)y^2, (c^3 + a^2)y^2,$$

$$cxy + by^2, cx^2 + y^2, (b^2 + c)y^3, bxy^2 - y^3\}.$$

Let $G_1 := \{ax - cy, (bc - a)y^2\} \subset G$.

Illustration

Example

Let $F := \{ax^2 + by^2, cx^2 + y^2, ax - cy\} \subset \mathbb{Q}[a, b, c][x, y]$ where $\{x, y\}$ are variables and $\{a, b, c\}$ are parameters.

- Gröbner basis for $\langle F \rangle \subset \mathbb{Q}[x, y, a, b, c]$ w.r.t. $x, y \gg a, b, c$.

$$G = \{ax - cy, (bc - a)y^2, (ab + c^2)y^2, (c^3 + a^2)y^2,$$

$$cxy + by^2, cx^2 + y^2, (b^2 + c)y^3, bxy^2 - y^3\}.$$

Let $G_1 := \{ax - cy, (bc - a)y^2\} \subset G$.
Theorem 4.3 in (Kapur et al. 2010) shows $\sigma_\alpha(G_1)$ is a Gröbner basis for $\langle \sigma_\alpha(F) \rangle$ for $\forall \alpha \in A_1 = \mathbb{C}^3 \setminus V(abc - a^2)$, which is the same as $a \neq 0 \wedge (bc - a) \neq 0$.

Then (A_1, G_1) is a branch of CGS for F.

- For other branches of CGS, making leading coefficients of some of these polynomials in G_1 to be nonzero, one by one.

- For other branches of CGS, making leading coefficients of some of these polynomials in G_1 to be nonzero, one by one.

- For other branches of CGS, making leading coefficients of some of these polynomials in G_1 to be nonzero, one by one.
  For example, we can start with $a = 0$.

- For other branches of CGS, making leading coefficients of some of these polynomials in G_1 to be nonzero, one by one.
  For example, we can start with $a = 0$.

  Gröbner basis for $\langle F \cup \{a\} \rangle$ is:

$$G' = \{a, cy, by^2, cx^2 + y^2, y^3\}.$$

- For other branches of CGS, making leading coefficients of some of these polynomials in G_1 to be nonzero, one by one.
  For example, we can start with $a = 0$.

  Gröbner basis for $\langle F \cup \{a\} \rangle$ is:

$$G' = \{a, cy, by^2, cx^2 + y^2, y^3\}.$$

  Let $G_2 := \{cy, cx^2 + y^2\} \subset G'$.

- For other branches of CGS, making leading coefficients of some of these polynomials in G_1 to be nonzero, one by one.
  For example, we can start with $a = 0$.

  Gröbner basis for $\langle F \cup \{a\}\rangle$ is:

$$G' = \{a, cy, by^2, cx^2 + y^2, y^3\}.$$

  Let $G_2 := \{cy, cx^2 + y^2\} \subset G'$.
  By Theorem 4.3 in (Kapur et al. 2010), $\sigma_\alpha(G_2)$ is a Gröbner basis for $\langle \sigma_\alpha(F)\rangle$ for $\forall \alpha \in A_2 = V(a) \setminus V(c)$, which is the case when $a = 0 \wedge c \neq 0$.

- For other branches of CGS, making leading coefficients of some of these polynomials in G_1 to be nonzero, one by one.
  For example, we can start with $a = 0$.

  Gröbner basis for $\langle F \cup \{a\} \rangle$ is:

  $$G' = \{a, cy, by^2, cx^2 + y^2, y^3\}.$$

  Let $G_2 := \{cy, cx^2 + y^2\} \subset G'$.
  By Theorem 4.3 in (Kapur et al. 2010), $\sigma_\alpha(G_2)$ is a Gröbner basis for $\langle \sigma_\alpha(F) \rangle$ for $\forall \alpha \in A_2 = V(a) \setminus V(c)$, which is the case when $a = 0 \wedge c \neq 0$.

- $(A_2, G_2) = (V(a) \setminus V(c), \{cy, cx^2 + y^2\})$ is a branch of CGS for F.

- For other branches of CGS, making leading coefficients of some of these polynomials in G_1 to be nonzero, one by one.
  For example, we can start with $a = 0$.

  Gröbner basis for $\langle F \cup \{a\}\rangle$ is:

  $$G' = \{a, cy, by^2, cx^2 + y^2, y^3\}.$$

  Let $G_2 := \{cy, cx^2 + y^2\} \subset G'$.
  By Theorem 4.3 in (Kapur et al. 2010), $\sigma_\alpha(G_2)$ is a Gröbner basis for $\langle \sigma_\alpha(F)\rangle$ for $\forall \alpha \in A_2 = V(a) \setminus V(c)$, which is the case when $a = 0 \wedge c \neq 0$.

- $(A_2, G_2) = (V(a) \setminus V(c), \{cy, cx^2 + y^2\})$ is a branch of CGS for F.

- For other branches of CGS, making leading coefficients of some of these polynomials in G_1 to be nonzero, one by one.

  For example, we can start with $a = 0$.

  Gröbner basis for $\langle F \cup \{a\} \rangle$ is:

$$G' = \{a, cy, by^2, cx^2 + y^2, y^3\}.$$

  Let $G_2 := \{cy, cx^2 + y^2\} \subset G'$.

  By Theorem 4.3 in (Kapur et al. 2010), $\sigma_\alpha(G_2)$ is a Gröbner basis for $\langle \sigma_\alpha(F) \rangle$ for $\forall \alpha \in A_2 = V(a) \setminus V(c)$, which is the case when $a = 0 \wedge c \neq 0$.

- $(A_2, G_2) = (V(a) \setminus V(c), \{cy, cx^2 + y^2\})$ is a branch of CGS for F.

- Similarly, to generate additional branches, make $c = 0$, and so on.

Faithfulness of Comprehensive Gröbner basis

Comprehensive Gröbner system(CGS):

$$\{(A_i, G_i)\} = \begin{cases} \mathbb{C}^3 \setminus V(a(abc-a)), & \{ax-cy, (bc-a)y^2\} \\ V(a) \setminus V(c), & \{cy, cx^2+y^2\} \\ V(a,c), & \{y^2\} \\ V(bc-a) \setminus V(a(b^2+c)), & \{ax-cy, (b^2+c)y^2\} \\ V(bc-a, b^2+c, ab+c^2, c^3+a^2) \setminus V(ac), & \{c^2x+bcy\} \end{cases}$$

Faithfulness of Comprehensive Gröbner basis

Comprehensive Gröbner system(CGS):

$$\{(A_i, G_i)\} = \begin{cases} \mathbb{C}^3 \setminus V(a(abc-a)), & \{ax-cy, (bc-a)y^2\} \\ V(a) \setminus V(c), & \{cy, cx^2+y^2\} \\ V(a,c), & \{y^2\} \\ V(bc-a) \setminus V(a(b^2+c)), & \{ax-cy, (b^2+c)y^2\} \\ V(bc-a, b^2+c, ab+c^2, c^3+a^2) \setminus V(ac), & \{c^2x+bcy\} \end{cases}$$

Comprehensive Gröbner basis(CGB):

$$G = \{ax-cy, (bc-a)y^2, cx^2+y^2, (bc-a)xy+(b^2+c)y^2, abx-bcy\}.$$

Faithfulness of Comprehensive Gröbner basis

Comprehensive Gröbner system(CGS):

$$\{(A_i, G_i)\} = \begin{cases} \mathbb{C}^3 \setminus V(a(abc-a)), & \{ax-cy, (bc-a)y^2\} \\ V(a) \setminus V(c), & \{cy, cx^2+y^2\} \\ V(a,c), & \{y^2\} \\ V(bc-a) \setminus V(a(b^2+c)), & \{ax-cy, (b^2+c)y^2\} \\ V(bc-a, b^2+c, ab+c^2, c^3+a^2) \setminus V(ac), & \{c^2x+bcy\} \end{cases}$$

Comprehensive Gröbner basis(CGB):

$$G = \{ax-cy, (bc-a)y^2, cx^2+y^2, (bc-a)xy+(b^2+c)y^2, abx-bcy\}.$$

- However, cy is not a polynomial in $\langle F \rangle$.

Faithfulness of Comprehensive Gröbner basis

Comprehensive Gröbner system(CGS):

$$\{(A_i, G_i)\} = \begin{cases} \mathbb{C}^3 \setminus V(a(abc-a)), & \{ax - cy, (bc-a)y^2\} \\ V(a) \setminus V(c), & \{cy, cx^2 + y^2\} \\ V(a,c), & \{y^2\} \\ V(bc-a) \setminus V(a(b^2+c)), & \{ax - cy, (b^2+c)y^2\} \\ V(bc-a, b^2+c, ab+c^2, c^3+a^2) \setminus V(ac), & \{c^2x + bcy\} \end{cases}$$

Comprehensive Gröbner basis(CGB):

$$G = \{ax - cy, (bc-a)y^2, cx^2 + y^2, (bc-a)xy + (b^2+c)y^2, abx - bcy\}.$$

- However, cy is not a polynomial in $\langle F \rangle$.
- Faithfulness: G should be a subset of $\langle F \rangle$
  E.g., $cy \notin \langle F \rangle$, so $\sigma_{(1,2,1)}(cy) = y \notin \langle \sigma_{(1,2,1)}(F) \rangle = \langle x - y, y^2 \rangle$.

Tuple Representation of Polynomials

- Faithfulness: G should be a subset of $\langle F \rangle$

  E.g., $cy \notin \langle F \rangle$, so $\sigma_{(1,2,1)}(cy) = y \notin \langle \sigma_{(1,2,1)}(F) \rangle = \langle x - y, y^2 \rangle$.

Tuple Representation of Polynomials

- Faithfulness: G should be a subset of $\langle F \rangle$
  E.g., $cy \notin \langle F \rangle$, so $\sigma_{(1,2,1)}(cy) = y \notin \langle \sigma_{(1,2,1)}(F) \rangle = \langle x - y, y^2 \rangle$.
- If $\{(A_i, G_i)\}$ is a CGS for F and $G_i \subset \langle F \rangle$, then $\bigcup G_i$ is a CGB for F.

Tuple Representation of Polynomials

- Faithfulness: G should be a subset of $\langle F \rangle$
  E.g., $cy \notin \langle F \rangle$, so $\sigma_{(1,2,1)}(cy) = y \notin \langle \sigma_{(1,2,1)}(F) \rangle = \langle x - y, y^2 \rangle$.
- If $\{(A_i, G_i)\}$ is a CGS for F and $G_i \subset \langle F \rangle$, then $\bigcup G_i$ is a CGB for F.
- Objective: find $f \in \langle F \rangle$, s.t. $\sigma_\alpha(f) = \sigma_\alpha(cy)$ for $\forall \alpha \in V(a) \setminus V(c)$.

Tuple Representation of Polynomials

- Faithfulness: G should be a subset of $\langle F \rangle$
  E.g., $cy \notin \langle F \rangle$, so $\sigma_{(1,2,1)}(cy) = y \notin \langle \sigma_{(1,2,1)}(F) \rangle = \langle x - y, y^2 \rangle$.
- If $\{(A_i, G_i)\}$ is a CGS for F and $G_i \subset \langle F \rangle$, then $\bigcup G_i$ is a CGB for F.
- Objective: find $f \in \langle F \rangle$, s.t. $\sigma_\alpha(f) = \sigma_\alpha(cy)$ for $\forall \alpha \in V(a) \setminus V(c)$.
- Split a polynomial into two parts, nonzero part and zero part under a specialization or more precisely, along a branch component.

Tuple Representation of Polynomials

New technique

Given $A_i \subset \mathbb{C}^3$ *and* $f \in \langle F \rangle$,

1. $f = p + \bar{p}, \qquad f \longmapsto (p, \bar{p})$ *s.t.*
2. $\sigma_\alpha(\bar{p}) = 0$ *for* $\forall \alpha \in A_i$.

Tuple Representation of Polynomials

New technique

Given $A_i \subset \mathbb{C}^3$ *and* $f \in \langle F \rangle$,

1. $f = p + \bar{p}, \qquad f \longmapsto (p, \bar{p})$ *s.t.*
2. $\sigma_\alpha(\bar{p}) = 0$ *for* $\forall \alpha \in A_i$.

E.g. $A_2 = V(a) \setminus V(c)$, then $ax - cy \in F \longmapsto (-cy, ax)$.

KSW Algorithm

- CGS / CGB computed by the Kapur-Sun-Wang (2011) algorithm has the following features:
  - Partitions the parameter space into disjoint fewer branches (segments).

KSW Algorithm

- CGS / CGB computed by the Kapur-Sun-Wang (2011) algorithm has the following features:
  - Partitions the parameter space into disjoint fewer branches (segments).
  - Output is **faithful**, i.e. all polynomials in CGS and CGB are in the input ideal,

KSW Algorithm

- CGS / CGB computed by the Kapur-Sun-Wang (2011) algorithm has the following features:
  - Partitions the parameter space into disjoint fewer branches (segments).
  - Output is **faithful**, i.e. all polynomials in CGS and CGB are in the input ideal,
  - is efficient (Montes, 2012).

KSW Algorithm

- CGS / CGB computed by the Kapur-Sun-Wang (2011) algorithm has the following features:
  - Partitions the parameter space into disjoint fewer branches (segments).
  - Output is **faithful**, i.e. all polynomials in CGS and CGB are in the input ideal,
  - is efficient (Montes, 2012).
  - CGS is *minimal*, i.e.,

KSW Algorithm

- CGS / CGB computed by the Kapur-Sun-Wang (2011) algorithm has the following features:
  - Partitions the parameter space into disjoint fewer branches (segments).
  - Output is **faithful**, i.e. all polynomials in CGS and CGB are in the input ideal,
  - is efficient (Montes, 2012).
  - CGS is *minimal*, i.e.,
    - for any branch and any specialization in this branch, the corresponding GB is a **minimal** Gröbner basis of the specialization of the input ideal.

KSW Algorithm

- CGS / CGB computed by the Kapur-Sun-Wang (2011) algorithm has the following features:
  - Partitions the parameter space into disjoint fewer branches (segments).
  - Output is **faithful**, i.e. all polynomials in CGS and CGB are in the input ideal,
  - is efficient (Montes, 2012).
  - CGS is *minimal*, i.e.,
    - for any branch and any specialization in this branch, the corresponding GB is a **minimal** Gröbner basis of the specialization of the input ideal.
    - for every branch, the set of leading terms of the corresponding GB remains the same under any specialization in this branch, i.e. the GB is **stable**.

Modified KSW's Algorithm and CGB Computation

- The new technique is applied to the algorithm in (Kapur et al. 2010) to compute comprehensive Gröbner bases.

Exa.	heuristics(Reduce)	Suzuki-Sato(Risa/Asir)	New(Singular)
F6	0.590	*error*	0.310
F8	$>$ 1h	0.6708	0.650
S1	$>$ 1h	*error*	0.120
S2	10.520	*error*	0.165
S3	28.845	$>$ 1h	4.515
S4	50.180	$>$ 1h	5.410
S5	329.169	$>$ 1h	18.034
P3P	$>$ 1h	$>$ 1h	14.440

Modified KSW's Algorithm and CGB Computation

- The new technique is applied to the algorithm in (Kapur et al. 2010) to compute comprehensive Gröbner bases.

Exa.	heuristics(Reduce)	Suzuki-Sato(Risa/Asir)	New(Singular)
F6	0.590	*error*	0.310
F8	$>$ 1h	0.6708	0.650
S1	$>$ 1h	*error*	0.120
S2	10.520	*error*	0.165
S3	28.845	$>$ 1h	4.515
S4	50.180	$>$ 1h	5.410
S5	329.169	$>$ 1h	18.034
P3P	$>$ 1h	$>$ 1h	14.440

- ANY algorithm for computing CGS can use this new technique to compute CGB.

Modified KSW Algorithm

- CGS / CGB computed by the Kapur-Sun-Wang (2011) algorithm has the following features:
  - Partitions the parameter space into **disjoint** fewer branches (segments).
  - Output is **faithful**, i.e. all polynomials in CGS and CGB are in the input ideal,
  - is efficient (Montes, 2012).
  - CGS is *minimal*, i.e.,
    - for any branch and any specialization in this branch, the corresponding GB is a **minimal** Gröbner basis of the specialization of the input ideal.
    - for every branch, the set of leading terms of the corresponding GB remains the same under any specialization in this branch, i.e. the GB is **stable**.

Modified KSW Algorithm

- CGS / CGB computed by the Kapur-Sun-Wang (2011) algorithm has the following features:
  - Partitions the parameter space into **disjoint** fewer branches (segments).
  - Output is **faithful**, i.e. all polynomials in CGS and CGB are in the input ideal,
  - is efficient (Montes, 2012).
  - CGS is *minimal*, i.e.,
    - for any branch and any specialization in this branch, the corresponding GB is a **minimal** Gröbner basis of the specialization of the input ideal.
    - for every branch, the set of leading terms of the corresponding GB remains the same under any specialization in this branch, i.e. the GB is **stable**.
  - CGB is made monic in $K[U, X]$, i.e. $LC_U(CGB)$ are monic.

Example 1

Example

Given an ideal
$I = \langle -2ux^2 - vxy, -4vy^2 + (-2u + 2v) \subseteq \rangle K[u, v][x, y]$ and a lexicographical term order $>$ with $x > y \gg u > v$.

Example 1

Example

Given an ideal $I = \langle -2ux^2 - vxy, -4vy^2 + (-2u+2v) \subseteq \rangle K[u,v][x,y]$ and a lexicographical term order $>$ with $x > y \gg u > v$.

By the KSW algorithm, a CGS and CGB of I w.r.t. $>$ are:

	branch	basis	LT
1	$u \neq 0 \wedge v \neq 0$	$\{vy^2 + (\frac{1}{2}u - \frac{1}{2}v), ux^2 + \frac{1}{2}vxy\}$	$\{y^2, x^2\}$
2	$v = 0 \wedge u \neq 0$	$\{vy^2 + (\frac{1}{2}u - \frac{1}{2}v)\}$	$\{1\}$
3	$u = 0 \wedge v = 0$	$\{\}$	$\{\}$
4	$u = 0 \wedge v \neq 0$	$\{vy^2 + (\frac{1}{2}u - \frac{1}{2}v), ux^2y + (-\frac{1}{4}u + \frac{1}{4}v)x\}$	$\{y^2, x\}$

Example 1

Example

Given an ideal
$I = \langle -2ux^2 - vxy, -4vy^2 + (-2u + 2v) \subseteq \rangle K[u, v][x, y]$ and a lexicographical term order $>$ with $x > y \gg u > v$.

By the KSW algorithm, a CGS and CGB of I w.r.t. $>$ are:

	branch	basis	LT
1	$u \neq 0 \wedge v \neq 0$	$\{vy^2 + (\frac{1}{2}u - \frac{1}{2}v), ux^2 + \frac{1}{2}vxy\}$	$\{y^2, x^2\}$
2	$v = 0 \wedge u \neq 0$	$\{vy^2 + (\frac{1}{2}u - \frac{1}{2}v)\}$	$\{1\}$
3	$u = 0 \wedge v = 0$	$\{\}$	$\{\}$
4	$u = 0 \wedge v \neq 0$	$\{vy^2 + (\frac{1}{2}u - \frac{1}{2}v), ux^2y + (-\frac{1}{4}u + \frac{1}{4}v)x\}$	$\{y^2, x\}$

$$CGB = \{vy^2 + (\frac{1}{2}u - \frac{1}{2}v), \quad ux^2 + \frac{1}{2}vxy, \quad ux^2y + (-\frac{1}{4}u + \frac{1}{4}v)x\}$$

Example 1

Example

Given an ideal $I = \langle -2ux^2 - vxy, -4vy^2 + (-2u + 2v) \subseteq \rangle K[u, v][x, y]$ and a lexicographical term order $>$ with $x > y \gg u > v$.

By the KSW algorithm, a CGS and CGB of I w.r.t. $>$ are:

	branch	basis	LT
1	$u \neq 0 \wedge v \neq 0$	$\{vy^2 + (\frac{1}{2}u - \frac{1}{2}v), ux^2 + \frac{1}{2}vxy\}$	$\{y^2, x^2\}$
2	$v = 0 \wedge u \neq 0$	$\{vy^2 + (\frac{1}{2}u - \frac{1}{2}v)\}$	$\{1\}$
3	$u = 0 \wedge v = 0$	$\{\}$	$\{\}$
4	$u = 0 \wedge v \neq 0$	$\{vy^2 + (\frac{1}{2}u - \frac{1}{2}v), ux^2y + (-\frac{1}{4}u + \frac{1}{4}v)x\}$	$\{y^2, x\}$

$$CGB = \{vy^2 + (\frac{1}{2}u - \frac{1}{2}v), \quad ux^2 + \frac{1}{2}vxy, \quad ux^2y + (-\frac{1}{4}u + \frac{1}{4}v)x\}$$

A branch is represented by $(E = \{e_1, \ldots, e_k\}, N = \{n\})$, which defines the set of specializations $V(E) - V(N)$.

GB vs. CGB

	Gröbner Basis	**Comprehensive Gröbner**
minimal	Proper subsets not GB	Proper subsets not CGB.
monic	$LC(g) = 1$	$LC(g)$ is monic.
reduced	polynomials in normal form	
canonical	GB is reduced.	

Minimality and Uniqueness for CGB

- **Minimality** – no proper subset of CGB is a CGB of I on S.

Minimality and Uniqueness for CGB

- **Minimality** – no proper subset of *CGB* is a CGB of I on S.
- **Uniqueness** – *CGB* is uniquely determined by I and $>$.

Minimality and Uniqueness for CGB

- **Minimality** – no proper subset of *CGB* is a CGB of I on S.
- **Uniqueness** – *CGB* is uniquely determined by I and $>$.
- How do various existing constructions of CGS / CGB fare?

Minimality and Uniqueness for CGB

- **Minimality** – no proper subset of *CGB* is a CGB of *I* on *S*.
- **Uniqueness** – *CGB* is uniquely determined by *I* and $>$.
- How do various existing constructions of CGS / CGB fare?
  - GRGB (Weispfenning, 1992) – neither minimal nor unique.

Minimality and Uniqueness for CGB

- **Minimality** – no proper subset of *CGB* is a CGB of I on S.
- **Uniqueness** – *CGB* is uniquely determined by I and $>$.
- How do various existing constructions of CGS / CGB fare?
  - GRGB (Weispfenning, 1992) – neither minimal nor unique.
  - CCGB (Weispfenning, 2003) – uniquely determined but not algorithmic independent; minimality not guaranteed.

Minimality and Uniqueness for CGB

- **Minimality** – no proper subset of *CGB* is a CGB of *I* on *S*.
- **Uniqueness** – *CGB* is uniquely determined by *I* and $>$.
- How do various existing constructions of CGS / CGB fare?
  - GRGB (Weispfenning, 1992) – neither minimal nor unique.
  - CCGB (Weispfenning, 2003) – uniquely determined but not algorithmic independent; minimality not guaranteed.
  - SACGB (Suzuki & Sato, 2006) – neither minimal nor unique.

Minimality and Uniqueness for CGB

- **Minimality** – no proper subset of *CGB* is a CGB of *I* on *S*.
- **Uniqueness** – *CGB* is uniquely determined by *I* and $>$.
- How do various existing constructions of CGS / CGB fare?
  - GRGB (Weispfenning, 1992) – neither minimal nor unique.
  - CCGB (Weispfenning, 2003) – uniquely determined but not algorithmic independent; minimality not guaranteed.
  - SACGB (Suzuki & Sato, 2006) – neither minimal nor unique.
  - MCCGS (Manubens & Montes, 2007) – number of branches is minimum; CGS is not faithful, thus no CGB is constructed.

Minimality and Uniqueness for CGB

- **Minimality** – no proper subset of *CGB* is a CGB of I on S.
- **Uniqueness** – *CGB* is uniquely determined by I and $>$.
- How do various existing constructions of CGS / CGB fare?
    - GRGB (Weispfenning, 1992) – neither minimal nor unique.
    - CCGB (Weispfenning, 2003) – uniquely determined but not algorithmic independent; minimality not guaranteed.
    - SACGB (Suzuki & Sato, 2006) – neither minimal nor unique.
    - MCCGS (Manubens & Montes, 2007) – number of branches is minimum; CGS is not faithful, thus no CGB is constructed.
    - Gröbner Cover (Montes & Wibmer, 2010) – canonical in terms of regular functions in $\mathcal{O}(U)[X]$; the system is still not faithful.

Minimality and Uniqueness for CGB

- **Minimality** – no proper subset of CGB is a CGB of I on S.
- **Uniqueness** – CGB is uniquely determined by I and $>$.
- How do various existing constructions of CGS / CGB fare?
  - GRGB (Weispfenning, 1992) – neither minimal nor unique.
  - CCGB (Weispfenning, 2003) – uniquely determined but not algorithmic independent; minimality not guaranteed.
  - SACGB (Suzuki & Sato, 2006) – neither minimal nor unique.
  - MCCGS (Manubens & Montes, 2007) – number of branches is minimum; CGS is not faithful, thus no CGB is constructed.
  - Gröbner Cover (Montes & Wibmer, 2010) – canonical in terms of regular functions in $\mathcal{O}(U)[X]$; the system is still not faithful.
  - KSWCGB (KSW, 2011) – neither minimal nor unique.

Minimality and Uniqueness for CGB

- **Minimality** – no proper subset of CGB is a CGB of I on S.
- **Uniqueness** – CGB is uniquely determined by I and $>$.
- How do various existing constructions of CGS / CGB fare?
  - GRGB (Weispfenning, 1992) – neither minimal nor unique.
  - CCGB (Weispfenning, 2003) – uniquely determined but not algorithmic independent; minimality not guaranteed.
  - SACGB (Suzuki & Sato, 2006) – neither minimal nor unique.
  - MCCGS (Manubens & Montes, 2007) – number of branches is minimum; CGS is not faithful, thus no CGB is constructed.
  - Gröbner Cover (Montes & Wibmer, 2010) – canonical in terms of regular functions in $\mathcal{O}(U)[X]$; the system is still not faithful.
  - KSWCGB (KSW, 2011) – neither minimal nor unique.
- Starting with KSWCGB, compute a minimal CGB (MCGB), with a goal of achieving the canonical CGB (CGB) which is both minimal and reduced.

Compute a Minimal Comprehensive Gröbner Basis

- Main idea:

Compute a Minimal Comprehensive Gröbner Basis

- Main idea:
    - Compute *CGB* and *CGS* of a given ideal $I \subseteq K[U][X]$ w.r.t. $>$ using KSW algorithm;

Compute a Minimal Comprehensive Gröbner Basis

- Main idea:
  - Compute *CGB* and *CGS* of a given ideal $I \subseteq K[U][X]$ w.r.t. $>$ using KSW algorithm;
  - Remove non-essential (redundant) polynomials from *CGB*;

Compute a Minimal Comprehensive Gröbner Basis

- Main idea:
  - Compute *CGB* and *CGS* of a given ideal $I \subseteq K[U][X]$ w.r.t. $>$ using KSW algorithm;
  - Remove non-essential (redundant) polynomials from *CGB*;
  - Simplify essential polynomials while maintaining the CGBness.

Compute a Minimal Comprehensive Gröbner Basis

- Main idea:
  - Compute *CGB* and *CGS* of a given ideal $I \subseteq K[U][X]$ w.r.t. $>$ using KSW algorithm;
  - Remove non-essential (redundant) polynomials from *CGB*;
  - Simplify essential polynomials while maintaining the CGBness.
- Result: a CGB of I which contains only essential polynomials, i.e. a minimal CGB of I.

Essential Polynomial with respect to a CGB

- **Redundant** polynomial $f \in CGB$ such that $CGB \backslash \{f\}$ is still a CGB of the same ideal.

Essential Polynomial with respect to a CGB

- **Redundant** polynomial $f \in CGB$ such that $CGB \backslash \{f\}$ is still a CGB of the same ideal.
- **Covering** a subset C of $CGB - \{f\}$ is a covering of (or *covers*) f in a branch A, iff $LT(\sigma(f))$ can be simplified by $LT(\sigma(S))$ under $\forall \sigma \in A$.

Essential Polynomial with respect to a CGB

- **Redundant** polynomial $f \in CGB$ such that $CGB \backslash \{f\}$ is still a CGB of the same ideal.
- **Covering** a subset C of $CGB - \{f\}$ is a covering of (or *covers*) f in a branch A, iff $LT(\sigma(f))$ can be simplified by $LT(\sigma(S))$ under $\forall \sigma \in A$.
- **Intuition:**

Essential Polynomial with respect to a CGB

- **Redundant** polynomial $f \in CGB$ such that $CGB \backslash \{f\}$ is still a CGB of the same ideal.
- **Covering** a subset C of $CGB - \{f\}$ is a covering of (or *covers*) f in a branch A, iff $LT(\sigma(f))$ can be simplified by $LT(\sigma(S))$ under $\forall \sigma \in A$.
- **Intuition:**
  - $f \in CGB$ is redundant (**non-essential**) w.r.t. CGB, iff f has a corresponding covering by $CGB - \{f\}$ in each partition of the given parameter space.

Essential Polynomial with respect to a CGB

- **Redundant** polynomial $f \in CGB$ such that $CGB \backslash \{f\}$ is still a CGB of the same ideal.
- **Covering** a subset C of $CGB - \{f\}$ is a covering of (or *covers*) f in a branch A, iff $LT(\sigma(f))$ can be simplified by $LT(\sigma(S))$ under $\forall \sigma \in A$.
- **Intuition:**
  - $f \in CGB$ is redundant (**non-essential**) w.r.t. CGB, iff f has a corresponding covering by $CGB - \{f\}$ in each partition of the given parameter space.
  - $f \in CGB$ is **essential** w.r.t. CGB, iff there is subset B of the parameter space, such that f has no covering by $CGB - \{f\}$ in B.

Example 2

Example

Give an ideal $I = \langle f = uy + x, g = vz + x + 1\rangle \subseteq K[v,u][z,y,x]$ and a lexicographical term order with $z > y > x \gg v > u$.

Example 2

Example

Give an ideal $I = \langle f = uy + x, g = vz + x + 1 \rangle \subseteq K[v, u][z, y, x]$ and a lexicographical term order with $z > y > x \gg v > u$.

- The CGB by Weispfenning's algorithm (2003) is

$$CGB = \{f, g, h, -h\}$$

where $h = \boxed{g - f} = vz - uy + 1$.

$$RGB = \{f, g\}$$

Example 2

Example

Give an ideal $I = \langle f = uy + x, g = vz + x + 1\rangle \subseteq K[v, u][z, y, x]$ and a lexicographical term order with $z > y > x \gg v > u$.

- The CGB by Weispfenning's algorithm (2003) is

$$CGB = \{f, g, h, -h\}$$

where $h = \boxed{g - f} = vz - uy + 1$.

$$RGB = \{f, g\}$$

  - Obviously, one of h and $-h$ is non-essential.

Example 2

Example

Give an ideal $I = \langle f = uy + x, g = vz + x + 1 \rangle \subseteq K[v,u][z,y,x]$ and a lexicographical term order with $z > y > x \gg v > u$.

- The CGB by Weispfenning's algorithm (2003) is

$$CGB = \{f, g, h, -h\}$$

where $h = \boxed{g - f} = vz - uy + 1$.

$$RGB = \{f, g\}$$

  - Obviously, one of h and $-h$ is non-essential.
- Check for essentiality in general can be nontrivial.

Example 2

Example

Give an ideal $I = \langle f = uy + x, g = vz + x + 1 \rangle \subseteq K[v,u][z,y,x]$ and a lexicographical term order with $z > y > x \gg v > u$.

- The CGB by Weispfenning's algorithm (2003) is

$$CGB = \{f, g, h, -h\}$$

where $h = \boxed{g - f} = vz - uy + 1$.

$$RGB = \{f, g\}$$

  - Obviously, one of h and $-h$ is non-essential.
- Check for essentiality in general can be nontrivial.
  - $CGB' = \{f, g, g - f\}$ is a CGB of I. Is $g - f$ redundant or essential?

Example 2

Example

Give an ideal $I = \langle f = uy + x, g = vz + x + 1 \rangle \subseteq K[v, u][z, y, x]$ and a lexicographical term order with $z > y > x \gg v > u$.

- The CGB by Weispfenning's algorithm (2003) is

$$CGB = \{f, g, h, -h\}$$

where $h = \boxed{g - f} = vz - uy + 1$.

$$RGB = \{f, g\}$$

  - Obviously, one of h and $-h$ is non-essential.
- Check for essentiality in general can be nontrivial.
  - $CGB' = \{f, g, g - f\}$ is a CGB of I. Is $g - f$ redundant or essential?
  - For $\sigma : u = v = 0$, $\sigma(I) = \langle x, x + 1 \rangle$, implying $1 \in \sigma(I)$. Neither $\sigma(f)$ nor $\sigma(g)$ can reduce it to 0, implying that $h = g - f$ is essential ($\sigma(h) = 1$).

Essentiality Check with CGS

- When *CGB* and *CGS* are computed by the KSW algorithm,

Essentiality Check with CGS

- When *CGB* and *CGS* are computed by the KSW algorithm,
- Given $f \in CGB$, to check if f is essential (w.r.t. *CGB*):
  - **Goal:** find a non-empty subset B of the parameter space such that f has no covering by $CGB - \{f\}$ in B.

Essentiality Check with CGS

- When CGB and CGS are computed by the KSW algorithm,
- Given $f \in CGB$, to check if f is essential (w.r.t. CGB):
  - **Goal:** find a non-empty subset B of the parameter space such that f has no covering by $CGB - \{f\}$ in B.

Essentiality Check with CGS

- When *CGB* and *CGS* are computed by the KSW algorithm,
- Given $f \in CGB$, to check if f is essential (w.r.t. *CGB*):
  - **Goal:** find a non-empty subset B of the parameter space such that f has no covering by $CGB - \{f\}$ in B.
  - Only need to consider branches of the form $(A_i, G_i) \in CGS$ with $f \in G_i$.

Essentiality Check with CGS

- When CGB and CGS are computed by the KSW algorithm,
- Given $f \in CGB$, to check if f is essential (w.r.t. CGB):
  - **Goal:** find a non-empty subset B of the parameter space such that f has no covering by $CGB - \{f\}$ in B.
  - Only need to consider branches of the form $(A_i, G_i) \in CGS$ with $f \in G_i$.
  - For any branch (A_j, G_j) with $f \notin G_j$, there is no need to check if f is covered by $G_j \subseteq CGB - \{f\}$ since A_j, A_i are disjoint.

Essentiality Check with CGS

- When CGB and CGS are computed by the KSW algorithm,
- Given $f \in CGB$, to check if f is essential (w.r.t. CGB):
  - **Goal:** find a non-empty subset B of the parameter space such that f has no covering by $CGB - \{f\}$ in B.
  - Only need to consider branches of the form $(A_i, G_i) \in CGS$ with $f \in G_i$.
  - For any branch (A_j, G_j) with $f \notin G_j$, there is no need to check if f is covered by $G_j \subseteq CGB - \{f\}$ since A_j, A_i are disjoint.

Essentiality Check with CGS

- When *CGB* and *CGS* are computed by the KSW algorithm,
- Given $f \in CGB$, to check if f is essential (w.r.t. CGB):
  - **Goal:** find a non-empty subset B of the parameter space such that f has no covering by $CGB - \{f\}$ in B.
  - Only need to consider branches of the form $(A_i, G_i) \in CGS$ with $f \in G_i$.
  - For any branch (A_j, G_j) with $f \notin G_j$, there is no need to check if f is covered by $G_j \subseteq CGB - \{f\}$ since A_j, A_i are disjoint.
  - In each branch $(A_i, G_i), f \in G_i$: look for a covering of f by $CGB - G_i$ in A_i (i.e. under all specializations in A_i):
    - a) $\boldsymbol{\sigma_i(G_i)}$ **is minimal for** $\forall \boldsymbol{\sigma_i} \in \mathbf{A_i}$: enough to check if $LT(\sigma_i(f)) \in LT(\sigma_i(CGB - G_i))$.
    - b1) If there is no such a covering in A_i, then f is essential w.r.t. CGB, and the algorithm terminates.
    - b2) Otherwise, check the next branch where f appears in the corresponding Gröbner basis.

Essentiality Check with CGS

- When CGB and CGS are computed by the KSW algorithm,
- Given $f \in CGB$, to check if f is essential (w.r.t. CGB):
  - **Goal:** find a non-empty subset B of the parameter space such that f has no covering by $CGB - \{f\}$ in B.
  - Only need to consider branches of the form $(A_i, G_i) \in CGS$ with $f \in G_i$.
  - For any branch (A_j, G_j) with $f \notin G_j$, there is no need to check if f is covered by $G_j \subseteq CGB - \{f\}$ since A_j, A_i are disjoint.
  - In each branch $(A_i, G_i), f \in G_i$: look for a covering of f by $CGB - G_i$ in A_i (i.e. under all specializations in A_i):
    - a) $\sigma_\mathbf{i}(\mathbf{G_i})$ is minimal for $\forall \sigma_\mathbf{i} \in \mathbf{A_i}$: enough to check if $LT(\sigma_i(f)) \in LT(\sigma_i(CGB - G_i))$.
    - b1) If there is no such a covering in A_i, then f is essential w.r.t. CGB, and the algorithm terminates.
    - b2) Otherwise, check the next branch where f appears in the corresponding Gröbner basis.
  - If f has a covering in each of such branches, then f is non-essential (redundant).

Example 3

Example

$I = \langle ux^2 - 2y + (4u+4v)z, (-2u+2v)x^2 - 2y + 3vz \rangle$, and a lex. term order $>$ with $x > y > z \gg u > v$.

Example 3

Example

$I = \langle ux^2 - 2y + (4u+4v)z, (-2u+2v)x^2 - 2y + 3vz \rangle$, and a lex. term order $>$ with $x > y > z \gg u > v$.

First, compute CGS and CGB using the KSW algorithm:

	branch	basis	LT
1	$3u - 2v \neq 0 \wedge v \neq 0$	$\{g_1, g_2\}$	$\{y, x^2\}$
2	$v = 0 \wedge u \neq 0$	$\{g_2, g_5\}$	$\{y, x^2\}$
3	$u = 0 \wedge v = 0$	$\{g_2\}$	$\{y\}$
4	$3u - 2v = 0 \wedge v \neq 0$	$\{g_5, g_4\}$	$\{z, x^2\}$

Example 3

Example

$I = \langle ux^2 - 2y + (4u+4v)z, (-2u+2v)x^2 - 2y + 3vz\rangle$, and a lex. term order $>$ with $x > y > z \gg u > v$.

First, compute CGS and CGB using the KSW algorithm:

	branch	basis	LT
1	$3u - 2v \neq 0 \wedge v \neq 0$	$\{g_1, g_2\}$	$\{y, x^2\}$
2	$v = 0 \wedge u \neq 0$	$\{g_2, g_5\}$	$\{y, x^2\}$
3	$u = 0 \wedge v = 0$	$\{g_2\}$	$\{y\}$
4	$3u - 2v = 0 \wedge v \neq 0$	$\{g_5, g_4\}$	$\{z, x^2\}$

$$\begin{aligned} CGB = \{g_1 &= (u - (2/3)v)y + (-(4/3)u^2 - (1/2)uv + (4/3)v^2)z, \\ g_2 &= vx^2 - 3y + (4u + (11/2)v)z, \\ g_4 &= (u - (40/49)v)x^2 + (22/49)y + ((36/49)u - (24/49)v)z, \\ g_5 &= (u - (2/3)v)x^2 + ((4/3)u + (1/3)v)z\} \end{aligned}$$

Example 3 (contd.)

Example

	branch	basis	LT
1	$3u - 2v \neq 0 \wedge v \neq 0$	$\{g_1, g_2\}$	$\{y, x^2\}$
2	$v = 0 \wedge u \neq 0$	$\{g_2, g_5\}$	$\{y, x^2\}$
3	$u = 0 \wedge v = 0$	$\{g_2\}$	$\{y\}$
4	$3u - 2v = 0 \wedge v \neq 0$	$\{g_5, g_4\}$	$\{z, x^2\}$

$$
\begin{aligned}
CGB = \{g_1 &= (u - (2/3)v)y + (-(4/3)u^2 - (1/2)uv + (4/3)v^2)z, \\
g_2 &= vx^2 - 3y + (4u + (11/2)v)z, \\
g_4 &= (u - (40/49)v)x^2 + (22/49)y + ((36/49)u - (24/49)v \\
g_5 &= (u - (2/3)v)x^2 + ((4/3)u + (1/3)v)z\}
\end{aligned}
$$

- g_5 appears in A_2 with LT x^2: g_4 covers it with LT x^2;
- g_5 appears in A_4 with LT z: g_1 covers it with LT z.

When a Polynomial Is Non-Essential

- $f \in CGB$ is non-essential w.r.t. CGB:
  - Update CGS by substituting f's covering for each occurrence of f;
  - Remove f from CGB.
- In Example 3, g_5 is non-essential w.r.t. CGB:

Example

	branch	basis	LT
1	$3u - 2v \neq 0 \wedge v \neq 0$	$\{g_1, g_2\}$	$\{y, x^2\}$
2	$v = 0 \wedge u \neq 0$	$\{g_2, g_4\}$	$\{y, x^2\}$
3	$u = 0 \wedge v = 0$	$\{g_2\}$	$\{y\}$
4	$3u - 2v = 0 \wedge v \neq 0$	$\{g_1, g_4\}$	$\{z, x^2\}$

$$
\begin{aligned}
CGB = \{g_1 &= (u - (2/3)v)y + (-(4/3)u^2 - (1/2)uv + (4/3)v^2)z, \\
g_2 &= vx^2 - 3y + (4u + (11/2)v)z, \\
g_4 &= (u - (40/49)v)x^2 + (22/49)y + ((36/49)u - (24/49)v)z\}
\end{aligned}
$$

Example 3 (contd.)

Example

	branch	basis	LT
1	$3u - 2v \neq 0 \wedge v \neq 0$	$\{g_1, g_2\}$	$\{y, x^2\}$
2	$v = 0 \wedge u \neq 0$	$\{g_2, g_4\}$	$\{y, x^2\}$
3	$u = 0 \wedge v = 0$	$\{g_2\}$	$\{y\}$
4	$3u - 2v = 0 \wedge v \neq 0$	$\{g_1, g_4\}$	$\{z, x^2\}$

$$CGB = \{g_1 = (u - (2/3)v)y + (-(4/3)u^2 - (1/2)uv + (4/3)v^2)z,$$

$$g_2 = vx^2 - 3y + (4u + (11/2)v)z,$$

$$g_4 = (u - (40/49)v)x^2 + (22/49)y + ((36/49)u - (24/49)v$$

- g_4 appears in A_2 with LT x^2: $CGB - G_2 = \{g_1\}$ doesn't cover g_4 in A_2.

Example 3 (result)

Finally, we achieve a minimal CGB of I w.r.t. $>$:

$$
\begin{aligned}
M = \{g_1 &= (u - (2/3)v)y + (-(4/3)u^2 - (1/2)uv + (4/3)v^2)z,\\
g_2 &= vx^2 - 3y + (4u + (11/2)v)z,\\
g_3 &= ux^2 - 2y + (4u + 4v)z\}.
\end{aligned}
$$

GB vs. CGB

	Gröbner Basis	**Comprehensive Gröbner**
minimal	Proper subsets not GB	Proper subsets not CGB
monic	$LC(g) = 1$	$LC(g)$ is monic.
reduced	polynomials in normal form	simplification violates CGBness
canonical	*GB* is reduced.	*CGB* is minimal and reduced

Towards a Canonical CGB (CCGB)

- There can be multiple MCGBs of the same parametric ideal.
  - In Example 3, besides M, it's easy to check that both

    $$M_1 = \{g_1, g_2, g_4\}$$

    and

    $$M_2 = \{g_1, g_2, g_5\}$$

    are MCGBs of I.
- These MCGBs are comparable using the set ordering w.r.t. $>$:

  $$M < M_1 < M_2,$$

  since $g_1 < g_2 < g_3 < g_4 < g_5$.
- The least MCGB under the set ordering w.r.t. $>$ since this is a total ordering.

Existence of a Canonical CGB

- A term ordering is a well-ordering implying a polynomial ordering is a well-ordering leading to a well-ordering on finite subsets of polynomials. Hence all CGB's can be ordered and the least element is a canonical CGB.

Existence of a Canonical CGB

- A term ordering is a well-ordering implying a polynomial ordering is a well-ordering leading to a well-ordering on finite subsets of polynomials. Hence all CGB's can be ordered and the least element is a canonical CGB.
- For each specialization σ of a parametric ideal I, for every minimal headterm of specialized polynomials in $\sigma(I)$, pick the least polynomial in I which under σ has this headterm. Let S be the set of all such polynomials.

Existence of a Canonical CGB

- A term ordering is a well-ordering implying a polynomial ordering is a well-ordering leading to a well-ordering on finite subsets of polynomials. Hence all CGB's can be ordered and the least element is a canonical CGB.
- For each specialization σ of a parametric ideal I, for every minimal headterm of specialized polynomials in $\sigma(I)$, pick the least polynomial in I which under σ has this headterm. Let S be the set of all such polynomials.

$$S = \bigcup_{\sigma} \{\text{the least } p \in I \mid LT(\sigma(p)) \text{ is minimal} \in LT(\sigma(I))$$

Lemma: *S is finite and is a CGB.*

Existence of a Canonical CGB

S may have redundant polynomials which are not essential. After such redundant polynomials have been removed by performing the essentiality check in the descending order, the result C is unique and the least CGB among all CGBs.

Existence of a Canonical CGB

S may have redundant polynomials which are not essential. After such redundant polynomials have been removed by performing the essentiality check in the descending order, the result C is unique and the least CGB among all CGBs.

Theorem (Kapur, JSSC 2017) *Let $C \subseteq S$ be a subset of polynomials after removing from S all redundant polynomials in the descending order. C is the least CGB among all CGBs of I and is unique.*

A completion Procedure for cgb MCGB directly from a parametric basis

See Kapur and Yang in ISSAC 2016,

Future Work

- An algorithmic construction of a canonical comprehensive Gröbner basis.

Future Work

- An algorithmic construction of a canonical comprehensive Gröbner basis.
- Can the above be computed using completion like approach?

Future Work

- An algorithmic construction of a canonical comprehensive Gröbner basis.
- Can the above be computed using completion like approach?
- Use of parametric computations to speed up quantifier elimination over the real closed field, in conjunction of sum of square heuristics ($\Sigma_{u=1}^{k} {p_u}^2 = 0 \implies p_i = 0$ over the reals.

Future Work

- An algorithmic construction of a canonical comprehensive Gröbner basis.
- Can the above be computed using completion like approach?
- Use of parametric computations to speed up quantifier elimination over the real closed field, in conjunction of sum of square heuristics ($\Sigma_{u=1}^{k} {p_u}^2 = 0 \implies p_i = 0$ over the reals.
- Is there a similar uniqueness property for a comprehensive Gröbner system associated with a parametric ideal?

Future Work

- An algorithmic construction of a canonical comprehensive Gröbner basis.
- Can the above be computed using completion like approach?
- Use of parametric computations to speed up quantifier elimination over the real closed field, in conjunction of sum of square heuristics ($\Sigma_{u=1}^{k} {p_u}^2 = 0 \implies p_i = 0$ over the reals.
- Is there a similar uniqueness property for a comprehensive Gröbner system associated with a parametric ideal?
- Issue of generating certificates?

CGS/CGB based heuristics for Theory of Real Closed Field

- Analyze polynomial equalities and generating segments on free variables Use that the starting point for every quantifier-free subformula.

CGS/CGB based heuristics for Theory of Real Closed Field

- Analyze polynomial equalities and generating segments on free variables Use that the starting point for every quantifier-free subformula.
- A goal: Develop a sufficiently large set of heuristics for performing quantifier elimination on polynomial equalities and inequalities.

CGS/CGB based heuristics for Theory of Real Closed Field

- Analyze polynomial equalities and generating segments on free variables Use that the starting point for every quantifier-free subformula.
- A goal: Develop a sufficiently large set of heuristics for performing quantifier elimination on polynomial equalities and inequalities.
- Two subclasses of interest: (i) Geometry formulations in Euclidean Geometry, (ii) Program and hybrid system analysis.

CGS/CGB based heuristics for Theory of Real Closed Field

- Analyze polynomial equalities and generating segments on free variables Use that the starting point for every quantifier-free subformula.
- A goal: Develop a sufficiently large set of heuristics for performing quantifier elimination on polynomial equalities and inequalities.
- Two subclasses of interest: (i) Geometry formulations in Euclidean Geometry, (ii) Program and hybrid system analysis.
- Integrate into an SMT solver.

CGS/CGB based heuristics for Theory of Real Closed Field

- Analyze polynomial equalities and generating segments on free variables Use that the starting point for every quantifier-free subformula.
- A goal: Develop a sufficiently large set of heuristics for performing quantifier elimination on polynomial equalities and inequalities.
- Two subclasses of interest: (i) Geometry formulations in Euclidean Geometry, (ii) Program and hybrid system analysis.
- Integrate into an SMT solver.
- Study its effectiveness.