

Equivariant Gröbner Bases

Michael Hanson Morrow

University of Kentucky

2021

The Classical Ideal Membership Problem

Notation

Until specified otherwise, let K be a field and let $R = K[x_1, \dots, x_n]$.

The Classical Ideal Membership Problem

Notation

Until specified otherwise, let K be a field and let $R = K[x_1, \dots, x_n]$.

Recall: Hilbert's Basis Theorem says R is Noetherian, and hence every ideal of R is finitely generated.

The Classical Ideal Membership Problem

Notation

Until specified otherwise, let K be a field and let $R = K[x_1, \dots, x_n]$.

Recall: Hilbert's Basis Theorem says R is Noetherian, and hence every ideal of R is finitely generated.

Question (CIMP)

Given $f \in R$ and an ideal $I \subseteq R$ generated by $g_1, \dots, g_s \in R$, is there a finite algorithm to determine if $f \in I$?

The Classical Ideal Membership Problem

Notation

Until specified otherwise, let K be a field and let $R = K[x_1, \dots, x_n]$.

Recall: Hilbert's Basis Theorem says R is Noetherian, and hence every ideal of R is finitely generated.

Question (CIMP)

Given $f \in R$ and an ideal $I \subseteq R$ generated by $g_1, \dots, g_s \in R$, is there a finite algorithm to determine if $f \in I$?

Some remarks:

- For $n = 1$, $K[x_1]$ is a PID and thus every ideal is of the form $\langle g \rangle$ for some $g \in K[x_1]$. The CIMP is then solved with high school polynomial long division ($f \in \langle g \rangle$ iff $f = gq$ for some $q \in K[x_1]$).

The Classical Ideal Membership Problem

Notation

Until specified otherwise, let K be a field and let $R = K[x_1, \dots, x_n]$.

Recall: Hilbert's Basis Theorem says R is Noetherian, and hence every ideal of R is finitely generated.

Question (CIMP)

Given $f \in R$ and an ideal $I \subseteq R$ generated by $g_1, \dots, g_s \in R$, is there a finite algorithm to determine if $f \in I$?

Some remarks:

- For $n = 1$, $K[x_1]$ is a PID and thus every ideal is of the form $\langle g \rangle$ for some $g \in K[x_1]$. The CIMP is then solved with high school polynomial long division ($f \in \langle g \rangle$ iff $f = gq$ for some $q \in K[x_1]$).
- For $n \geq 2$, $K[x_1, \dots, x_n]$ is not a PID and thus the task becomes more complicated.

Monomial Orders

To deal with polynomial rings in several variables (i.e. $n \geq 2$), we first need to order the monomials.

Monomial Orders

To deal with polynomial rings in several variables (i.e. $n \geq 2$), we first need to order the monomials.

Notation

Let $\text{Mon}(R)$ denote the set of monomials of R (including 1).

Monomial Orders

To deal with polynomial rings in several variables (i.e. $n \geq 2$), we first need to order the monomials.

Notation

Let $\text{Mon}(R)$ denote the set of monomials of R (including 1).

Definition (Monomial Order)

Let $<$ be a total order on $\text{Mon}(R)$. Then $<$ is called a **monomial order** (on $\text{Mon}(R)$) if for any $m_1, m_2, n \in \text{Mon}(R)$ with $n \neq 1$, we have

$$m_1 < m_2 \implies m_1 < nm_1 < nm_2.$$

Monomial Orders

Monomial orders abound. For example, we have:

Definition (Lex/Phonebook Order)

The **lexicographic order** on $\text{Mon}(R)$ is given by letting $x_1 > \cdots > x_n$ and defining $x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n}$ iff the leftmost nonzero entry of $(a_1 - b_1, \dots, a_n - b_n)$ is positive.

Monomial Orders

Monomial orders abound. For example, we have:

Definition (Lex/Phonebook Order)

The **lexicographic order** on $\text{Mon}(R)$ is given by letting $x_1 > \cdots > x_n$ and defining $x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n}$ iff the leftmost nonzero entry of $(a_1 - b_1, \dots, a_n - b_n)$ is positive.

For example, $x_1^2 > x_1 x_2^5$.

Monomial Orders

Monomial orders abound. For example, we have:

Definition (Lex/Phonebook Order)

The **lexicographic order** on $\text{Mon}(R)$ is given by letting $x_1 > \cdots > x_n$ and defining $x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n}$ iff the leftmost nonzero entry of $(a_1 - b_1, \dots, a_n - b_n)$ is positive.

For example, $x_1^2 > x_1 x_2^5$.

Definition

Fix a monomial order $<$ and let $f = c_1 m_1 + \dots + c_s m_s$ where $c_i \in K$, $m_i \in \text{Mon}(R)$, and $m_1 > \cdots > m_s$. Define the **leading term** of f to be $\text{lt}(f) := c_1 m_1$. Similarly, define the **initial monomial** of f to be $\text{in}(f) := m_1$. Finally, if $G \subseteq R$, define

$$\text{in}(G) := \{\text{in}(g) \mid g \in G\},$$

and define the **initial ideal** of G to be $\langle \text{in}(G) \rangle$.

An example:

- Give $\mathbb{Q}[x, y, z]$ the lex order with $x > y > z$ and let $g = 2y^2z^3 + yz^{21}$. Then $\text{in}(g) = y^2z^3$ and $\text{lt}(g) = 2y^2z^3$.

An example:

- Give $\mathbb{Q}[x, y, z]$ the lex order with $x > y > z$ and let $g = 2y^2z^3 + yz^{21}$. Then $\text{in}(g) = y^2z^3$ and $\text{lt}(g) = 2y^2z^3$.

A fundamental property of monomial orders:

Lemma (Dickson's Lemma)

Any monomial order $<$ is a well-order. In other words, any nonempty subset of $\text{Mon}(R)$ has a minimal element with respect to $<$.

Multivariate Division

Using monomial orders, we can define multivariate division with remainder.

Definition (Multivariate Division with Remainder)

Fix a monomial order $<$. Let $G \subseteq R$ and pick $f \in R$. Suppose $f = g + r$ for some $g \in \langle G \rangle$ and some $r \in R$ such that the following hold:

- Either $r = 0$ or $\text{in}(r) \notin \langle \text{in}(G) \rangle$.
- If $g \neq 0$ then $\text{in}(r) < \text{in}(f)$ (and hence $\text{in}(f) = \text{in}(g)$).

Then r is called a **remainder of f upon division by G** .

Multivariate Division

Using monomial orders, we can define multivariate division with remainder.

Definition (Multivariate Division with Remainder)

Fix a monomial order $<$. Let $G \subseteq R$ and pick $f \in R$. Suppose $f = g + r$ for some $g \in \langle G \rangle$ and some $r \in R$ such that the following hold:

- Either $r = 0$ or $\text{in}(r) \notin \langle \text{in}(G) \rangle$.
- If $g \neq 0$ then $\text{in}(r) < \text{in}(f)$ (and hence $\text{in}(f) = \text{in}(g)$).

Then r is called a **remainder of f upon division by G** .

There is an algorithm for computing remainders of f upon division by G .

Theorem (Multivariate Division Algorithm)

Let $<$ be a monomial order, let $G \subseteq R$, and let $f \in R$. Then a remainder of f upon division by G exists and can be computed in finite time.

Remark: remainders of f upon division by G need not be unique.

Multivariate Division

An example of multivariate division:

- Give $\mathbb{R}[x, y]$ the lex order with $x > y$, let $f = x^2y + x$, let $g_1 = x + 1$, and let $g_2 = y - 1$.

Since remainders need not be unique, it may be possible for f to have a nonzero remainder upon division by G , yet $f \in \langle G \rangle$. This is undesirable, so we introduce the following “good” generating set:

Definition

Let $<$ be a monomial order, let $I \subseteq R$ be an ideal, and let $G \subseteq I$. Then G is a **Gröbner basis** for I if $\langle \text{in}(I) \rangle = \langle \text{in}(G) \rangle$.

Since remainders need not be unique, it may be possible for f to have a nonzero remainder upon division by G , yet $f \in \langle G \rangle$. This is undesirable, so we introduce the following “good” generating set:

Definition

Let $<$ be a monomial order, let $I \subseteq R$ be an ideal, and let $G \subseteq I$. Then G is a **Gröbner basis** for I if $\langle \text{in}(I) \rangle = \langle \text{in}(G) \rangle$.

Some remarks:

- As the name suggests, Gröbner bases generate their ideals. In other words, if G is a Gröbner basis for I , then $I = \langle G \rangle$.

Since remainders need not be unique, it may be possible for f to have a nonzero remainder upon division by G , yet $f \in \langle G \rangle$. This is undesirable, so we introduce the following “good” generating set:

Definition

Let $<$ be a monomial order, let $I \subseteq R$ be an ideal, and let $G \subseteq I$. Then G is a **Gröbner basis** for I if $\langle \text{in}(I) \rangle = \langle \text{in}(G) \rangle$.

Some remarks:

- As the name suggests, Gröbner bases generate their ideals. In other words, if G is a Gröbner basis for I , then $I = \langle G \rangle$.
- Every ideal of R has a finite Gröbner basis, since the Noetherianity of R implies that $\langle \text{in}(I) \rangle$ is finitely generated.

Gröbner bases provide a complete solution to the CIMP.

Theorem

Fix a monomial order $<$, let $I \subseteq R$ be an ideal with Gröbner basis G , and let $f \in R$. Then $f \in I$ iff f has a remainder of zero upon division by G .

Gröbner bases provide a complete solution to the CIMP.

Theorem

Fix a monomial order $<$, let $I \subseteq R$ be an ideal with Gröbner basis G , and let $f \in R$. Then $f \in I$ iff f has a remainder of zero upon division by G .

Proof. (\Leftarrow) If f has a remainder of zero upon division by G , then $f \in \langle G \rangle = I$ by definition of multivariate division.

Gröbner bases provide a complete solution to the CIMP.

Theorem

Fix a monomial order $<$, let $I \subseteq R$ be an ideal with Gröbner basis G , and let $f \in R$. Then $f \in I$ iff f has a remainder of zero upon division by G .

Proof. (\Leftarrow) If f has a remainder of zero upon division by G , then $f \in \langle G \rangle = I$ by definition of multivariate division.

(\Rightarrow) Conversely, suppose $f \in I$, and use multivariate division to write $f = g + r$ for some $g \in \langle G \rangle = I$ and some $r \in R$ with either $r = 0$ or $\text{in}(r) \notin \langle \text{in}(G) \rangle = \langle \text{in}(I) \rangle$. If $r \neq 0$ then $r = f - g \in I$ implies $\text{in}(r) \in \langle \text{in}(I) \rangle$, a contradiction. □

For an ideal $I \subseteq R$ and a subset $G \subseteq I$, how can we determine if G is a Gröbner basis for I ?

For an ideal $I \subseteq R$ and a subset $G \subseteq I$, how can we determine if G is a Gröbner basis for I ?

Theorem (Buchberger's Criterion)

Fix a monomial order $<$. Let $I \subseteq R$ be an ideal and let $G \subseteq I$. For $f, g \in G$ define the **S-pair** of f and g :

$$S(f, g) := \frac{\text{lcm}(\text{in}(f), \text{in}(g))}{\text{lt}(f)} f - \frac{\text{lcm}(\text{in}(f), \text{in}(g))}{\text{lt}(g)} g \in \langle G \rangle.$$

Then G is a Gröbner basis for I iff $S(f, g)$ has a remainder of zero upon division by G for all $f, g \in G$.

Note: the S-pairs $S(f, g)$ and $S(g, f)$ differ only by a sign, so if $S(f, g)$ has a remainder of zero, so does $S(g, f)$.

If G is a finite set then Buchberger's Criterion can be checked algorithmically in finite time. This naturally leads us to a process for computing Gröbner bases for ideals of R .

If G is a finite set then Buchberger's Criterion can be checked algorithmically in finite time. This naturally leads us to a process for computing Gröbner bases for ideals of R .

Theorem (Buchberger's Algorithm)

Fix a monomial order $<$, and let $I \subseteq R$ be an ideal. Then a Gröbner basis for I can be computed in finite time.

An example of Buchberger's Algorithm:

- Give $\mathbb{R}[x, y]$ the lex order with $x > y$. Consider $I = \langle G \rangle$ where $G = \{x^2 + y, xy\}$. Put $g_1 = x^2 + y$ and $g_2 = xy$.

The Equivariant Ideal Membership Problem

We have seen that Gröbner bases solve the CIMP using multivariate division and that we can compute them in finite time using Buchberger's Algorithm. What about infinitely many variables?

The Equivariant Ideal Membership Problem

We have seen that Gröbner bases solve the CIMP using multivariate division and that we can compute them in finite time using Buchberger's Algorithm. What about infinitely many variables?

One naturally proposes the following:

Question

Let K be a field and consider the polynomial ring $K[x_1, x_2, \dots]$ in infinitely many variables. Given $f \in K[x_1, x_2, \dots]$ and an ideal $I \subseteq K[x_1, x_2, \dots]$, is there a finite algorithm to determine if $f \in I$?

The Equivariant Ideal Membership Problem

We have seen that Gröbner bases solve the CIMP using multivariate division and that we can compute them in finite time using Buchberger's Algorithm. What about infinitely many variables?

One naturally proposes the following:

Question

Let K be a field and consider the polynomial ring $K[x_1, x_2, \dots]$ in infinitely many variables. Given $f \in K[x_1, x_2, \dots]$ and an ideal $I \subseteq K[x_1, x_2, \dots]$, is there a finite algorithm to determine if $f \in I$?

Roadblock: $\langle x_1, x_2, \dots \rangle$ is not finitely generated, so $K[x_1, x_2, \dots]$ is not Noetherian.

The Equivariant Ideal Membership Problem

If we allow permutation of indices, $\langle x_1, x_2, \dots \rangle$ is finitely generated “up to symmetry” by x_1 . Let’s formalize this.

The Equivariant Ideal Membership Problem

If we allow permutation of indices, $\langle x_1, x_2, \dots \rangle$ is finitely generated “up to symmetry” by x_1 . Let’s formalize this.

Notation

Let $R = K[x_1, x_2, \dots]$. For $n \in \mathbb{N}$, write $[n] := \{1, \dots, n\}$, and set $[\infty] := \mathbb{N}$.

The Equivariant Ideal Membership Problem

If we allow permutation of indices, $\langle x_1, x_2, \dots \rangle$ is finitely generated “up to symmetry” by x_1 . Let’s formalize this.

Notation

Let $R = K[x_1, x_2, \dots]$. For $n \in \mathbb{N}$, write $[n] := \{1, \dots, n\}$, and set $[\infty] := \mathbb{N}$.

Definition

For $m, n \in \mathbb{N} \cup \{\infty\}$ define

$$\text{Inc}_{m,n} := \{\rho : [m] \rightarrow [n] \mid a < b \implies \rho(a) < \rho(b)\}.$$

The Equivariant Ideal Membership Problem

If we allow permutation of indices, $\langle x_1, x_2, \dots \rangle$ is finitely generated “up to symmetry” by x_1 . Let’s formalize this.

Notation

Let $R = K[x_1, x_2, \dots]$. For $n \in \mathbb{N}$, write $[n] := \{1, \dots, n\}$, and set $[\infty] := \mathbb{N}$.

Definition

For $m, n \in \mathbb{N} \cup \{\infty\}$ define

$$\text{Inc}_{m,n} := \{ \rho : [m] \rightarrow [n] \mid a < b \implies \rho(a) < \rho(b) \}.$$

Definition/Proposition

The set $\text{Inc}_{\infty, \infty}$ of strictly increasing maps on \mathbb{N} forms a monoid under the multiplication $\rho\sigma := \rho \circ \sigma$. Denote this monoid by $\text{Inc}(\mathbb{N})$.

The Equivariant Ideal Membership Problem

From now on, let $\text{Inc}(\mathbb{N})$ act on $R = K[x_1, x_2, \dots]$ via $x_i \mapsto x_{\rho(i)}$ and extending by homomorphisms.

The Equivariant Ideal Membership Problem

From now on, let $\text{Inc}(\mathbb{N})$ act on $R = K[x_1, x_2, \dots]$ via $x_i \mapsto x_{\rho(i)}$ and extending by homomorphisms. For example, if $f = 2x_1^2x_2 + x_5$ and $\rho \in \text{Inc}(\mathbb{N})$ satisfies $\rho(1) = 3$, $\rho(2) = 4$, and $\rho(5) = 21$, then $\rho(f) = 2x_3^2x_4 + x_{21}$.

The Equivariant Ideal Membership Problem

From now on, let $\text{Inc}(\mathbb{N})$ act on $R = K[x_1, x_2, \dots]$ via $x_i \mapsto x_{\rho(i)}$ and extending by homomorphisms. For example, if $f = 2x_1^2x_2 + x_5$ and $\rho \in \text{Inc}(\mathbb{N})$ satisfies $\rho(1) = 3$, $\rho(2) = 4$, and $\rho(5) = 21$, then $\rho(f) = 2x_3^2x_4 + x_{21}$.

Definition

An ideal $I \subseteq R$ is said to be **$\text{Inc}(\mathbb{N})$ -invariant** if $\rho(I) \subseteq I$ for all $\rho \in \text{Inc}(\mathbb{N})$.

The Equivariant Ideal Membership Problem

From now on, let $\text{Inc}(\mathbb{N})$ act on $R = K[x_1, x_2, \dots]$ via $x_i \mapsto x_{\rho(i)}$ and extending by homomorphisms. For example, if $f = 2x_1^2x_2 + x_5$ and $\rho \in \text{Inc}(\mathbb{N})$ satisfies $\rho(1) = 3$, $\rho(2) = 4$, and $\rho(5) = 21$, then $\rho(f) = 2x_3^2x_4 + x_{21}$.

Definition

An ideal $I \subseteq R$ is said to be **$\text{Inc}(\mathbb{N})$ -invariant** if $\rho(I) \subseteq I$ for all $\rho \in \text{Inc}(\mathbb{N})$.

Definition ($\text{Inc}(\mathbb{N})$ -orbits)

For $f \in R$ define the **orbit of f** as $\text{Inc}(\mathbb{N})f := \{\rho(f) \mid \rho \in \text{Inc}(\mathbb{N})\}$, and for $G \subseteq R$ define

$$\text{Inc}(\mathbb{N})G := \bigcup_{g \in G} \text{Inc}(\mathbb{N})g.$$

The Equivariant Ideal Membership Problem

Definition

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal. Then I is $\text{Inc}(\mathbb{N})$ -**generated** by a subset $G \subseteq I$ if $I = \langle \text{Inc}(\mathbb{N})G \rangle$. We sometimes write $\langle G \rangle_{\text{Inc}(\mathbb{N})}$ in place of $\langle \text{Inc}(\mathbb{N})G \rangle$. If G can be taken finite, then I is $\text{Inc}(\mathbb{N})$ -**finitely generated** (by G).

The Equivariant Ideal Membership Problem

Definition

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal. Then I is $\text{Inc}(\mathbb{N})$ -**generated** by a subset $G \subseteq I$ if $I = \langle \text{Inc}(\mathbb{N})G \rangle$. We sometimes write $\langle G \rangle_{\text{Inc}(\mathbb{N})}$ in place of $\langle \text{Inc}(\mathbb{N})G \rangle$. If G can be taken finite, then I is $\text{Inc}(\mathbb{N})$ -**finitely generated** (by G).

Example: $\langle x_1, x_2, \dots \rangle = \langle x_1 \rangle_{\text{Inc}(\mathbb{N})}$.

The Equivariant Ideal Membership Problem

Definition

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal. Then I is $\text{Inc}(\mathbb{N})$ -**generated** by a subset $G \subseteq I$ if $I = \langle \text{Inc}(\mathbb{N})G \rangle$. We sometimes write $\langle G \rangle_{\text{Inc}(\mathbb{N})}$ in place of $\langle \text{Inc}(\mathbb{N})G \rangle$. If G can be taken finite, then I is $\text{Inc}(\mathbb{N})$ -**finitely generated** (by G).

Example: $\langle x_1, x_2, \dots \rangle = \langle x_1 \rangle_{\text{Inc}(\mathbb{N})}$.

This leads us to the following version of Noetherianity:

Definition/Proposition

The ring R is $\text{Inc}(\mathbb{N})$ -**Noetherian**, i.e. every $\text{Inc}(\mathbb{N})$ -invariant ideal $I \subseteq R$ is $\text{Inc}(\mathbb{N})$ -finitely generated.

Remark: the above result is due to Cohen (1987) and Aschenbrenner & Hillar (2007).

The Equivariant Ideal Membership Problem

We can now state the Equivariant Ideal Membership Problem (EIMP):

Question (EIMP)

Given $f \in R$ and an $\text{Inc}(\mathbb{N})$ -finitely generated ideal

$I = \langle g_1, \dots, g_s \rangle_{\text{Inc}(\mathbb{N})} \subseteq R$, is there a finite algorithm to determine if $f \in I$?

The Equivariant Ideal Membership Problem

We can now state the Equivariant Ideal Membership Problem (EIMP):

Question (EIMP)

Given $f \in R$ and an $\text{Inc}(\mathbb{N})$ -finitely generated ideal $I = \langle g_1, \dots, g_s \rangle_{\text{Inc}(\mathbb{N})} \subseteq R$, is there a finite algorithm to determine if $f \in I$?

We parallel our development of the classical theory.

Definition ($\text{Inc}(\mathbb{N})$ -Respecting Monomial Order)

Let $<$ be a total order on $\text{Mon}(R)$. Then $<$ is a $\text{Inc}(\mathbb{N})$ -**respecting monomial order** (on $\text{Mon}(R)$) if for any $m_1, m_2 \in \text{Mon}(R)$ we have:

- $m_1 < m_2 \implies m_1 < nm_1 < nm_2$ for all $n \in \text{Mon}(R)$ with $n \neq 1$.
- $m_1 < m_2 \implies m_1 \leq \rho(m_1) < \rho(m_2)$ for all $\rho \in \text{Inc}(\mathbb{N})$.

Inc(\mathbb{N})-Respecting Monomial Orders

Some remarks:

- Inc(\mathbb{N})-respecting monomial orders exist: the lex order with $x_1 > x_2 > \dots$ is an example.

Inc(\mathbb{N})-Respecting Monomial Orders

Some remarks:

- Inc(\mathbb{N})-respecting monomial orders exist: the lex order with $x_1 > x_2 > \dots$ is an example.
- For $f \in R$ we define $\text{in}(f)$ and $\text{lt}(f)$ as we did before.

Inc(\mathbb{N})-Respecting Monomial Orders

Some remarks:

- Inc(\mathbb{N})-respecting monomial orders exist: the lex order with $x_1 > x_2 > \dots$ is an example.
- For $f \in R$ we define $\text{in}(f)$ and $\text{lt}(f)$ as we did before.
- $1 < n$ for all $n \in \text{Mon}(R)$ with $n \neq 1$.

Some remarks:

- Inc(\mathbb{N})-respecting monomial orders exist: the lex order with $x_1 > x_2 > \dots$ is an example.
- For $f \in R$ we define $\text{in}(f)$ and $\text{lt}(f)$ as we did before.
- $1 < n$ for all $n \in \text{Mon}(R)$ with $n \neq 1$.
- For $\rho \in \text{Inc}(\mathbb{N})$ and $f \in R$ we have $\text{in}(\rho(f)) = \rho(\text{in}(f))$.

Inc(\mathbb{N})-Respecting Monomial Orders

Some remarks:

- Inc(\mathbb{N})-respecting monomial orders exist: the lex order with $x_1 > x_2 > \dots$ is an example.
- For $f \in R$ we define $\text{in}(f)$ and $\text{lt}(f)$ as we did before.
- $1 < n$ for all $n \in \text{Mon}(R)$ with $n \neq 1$.
- For $\rho \in \text{Inc}(\mathbb{N})$ and $f \in R$ we have $\text{in}(\rho(f)) = \rho(\text{in}(f))$.

An equivariant version of Dickson's Lemma:

Proposition

Any Inc(\mathbb{N})-respecting monomial order $<$ is a well-order.

Note: the above proposition follows from the Inc(\mathbb{N})-Noetherianity of R .

Inc(\mathbb{N})-Division Algorithm

Definition (Inc(\mathbb{N})-Division)

Fix an Inc(\mathbb{N})-respecting monomial order $<$. Let $G \subseteq R$ and pick $f \in R$. Suppose $f = g + r$ for some $g \in \langle G \rangle_{\text{Inc}(\mathbb{N})}$ and some $r \in R$ such that the following hold:

- Either $r = 0$ or $\text{in}(r) \notin \langle \text{in}(G) \rangle_{\text{Inc}(\mathbb{N})}$.
- if $g \neq 0$ then $\text{in}(r) < \text{in}(f)$ (and hence $\text{in}(f) = \text{in}(g)$).

Then r is called a **remainder of f upon Inc(\mathbb{N})-division by G** .

Inc(\mathbb{N})-Division Algorithm

Definition (Inc(\mathbb{N})-Division)

Fix an Inc(\mathbb{N})-respecting monomial order $<$. Let $G \subseteq R$ and pick $f \in R$. Suppose $f = g + r$ for some $g \in \langle G \rangle_{\text{Inc}(\mathbb{N})}$ and some $r \in R$ such that the following hold:

- Either $r = 0$ or $\text{in}(r) \notin \langle \text{in}(G) \rangle_{\text{Inc}(\mathbb{N})}$.
- if $g \neq 0$ then $\text{in}(r) < \text{in}(f)$ (and hence $\text{in}(f) = \text{in}(g)$).

Then r is called a **remainder of f upon Inc(\mathbb{N})-division by G** .

An algorithm for computing remainders of f upon Inc(\mathbb{N})-division by G :

Theorem (Inc(\mathbb{N})-Division Algorithm)

Fix an Inc(\mathbb{N})-respecting monomial order $<$, let $G \subseteq R$ and let $f \in R$. Then a remainder of f upon Inc(\mathbb{N})-division by G can be computed in finite time.

Equivariant Gröbner Bases

Remark: the $\text{Inc}(\mathbb{N})$ -division algorithm works the same as classical multivariate division, where we divide by $\text{Inc}(\mathbb{N})G$ rather than just G . It terminates in finite time since $\text{Inc}(\mathbb{N})$ -respecting monomial orders are well-orders.

Remark: the $\text{Inc}(\mathbb{N})$ -division algorithm works the same as classical multivariate division, where we divide by $\text{Inc}(\mathbb{N})G$ rather than just G . It terminates in finite time since $\text{Inc}(\mathbb{N})$ -respecting monomial orders are well-orders.

We now introduce our primary object of study.

Definition

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal. A subset $G \subseteq I$ is an $\text{Inc}(\mathbb{N})$ -**equivariant Gröbner basis** for I if the set $\text{Inc}(\mathbb{N})G$ forms a Gröbner basis for I in the usual sense, i.e. if $\langle \text{in}(I) \rangle = \langle \text{in}(G) \rangle_{\text{Inc}(\mathbb{N})}$.

Equivariant Gröbner Bases

Remark: the $\text{Inc}(\mathbb{N})$ -division algorithm works the same as classical multivariate division, where we divide by $\text{Inc}(\mathbb{N})G$ rather than just G . It terminates in finite time since $\text{Inc}(\mathbb{N})$ -respecting monomial orders are well-orders.

We now introduce our primary object of study.

Definition

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal. A subset $G \subseteq I$ is an $\text{Inc}(\mathbb{N})$ -**equivariant Gröbner basis** for I if the set $\text{Inc}(\mathbb{N})G$ forms a Gröbner basis for I in the usual sense, i.e. if $\langle \text{in}(I) \rangle = \langle \text{in}(G) \rangle_{\text{Inc}(\mathbb{N})}$.

- As usual, $\text{Inc}(\mathbb{N})$ -equivariant Gröbner bases generate their ideals.
- Every $\text{Inc}(\mathbb{N})$ -invariant ideal of R has a finite $\text{Inc}(\mathbb{N})$ -equivariant Gröbner basis since R is $\text{Inc}(\mathbb{N})$ -Noetherian.

We now have a complete solution to the EIMP:

Theorem

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal with $\text{Inc}(\mathbb{N})$ -equivariant Gröbner basis G . Then for $f \in R$ we have $f \in I$ if and only if f has a remainder of zero upon $\text{Inc}(\mathbb{N})$ -division by G .

We now have a complete solution to the EIMP:

Theorem

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal with $\text{Inc}(\mathbb{N})$ -equivariant Gröbner basis G . Then for $f \in R$ we have $f \in I$ if and only if f has a remainder of zero upon $\text{Inc}(\mathbb{N})$ -division by G .

The question now becomes: how can we compute $\text{Inc}(\mathbb{N})$ -equivariant Gröbner bases?

Equivariant Gröbner Bases

We now have a complete solution to the EIMP:

Theorem

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal with $\text{Inc}(\mathbb{N})$ -equivariant Gröbner basis G . Then for $f \in R$ we have $f \in I$ if and only if f has a remainder of zero upon $\text{Inc}(\mathbb{N})$ -division by G .

The question now becomes: how can we compute $\text{Inc}(\mathbb{N})$ -equivariant Gröbner bases?

Theorem (Equivariant Buchberger's Criterion)

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal and let $G \subseteq I$. Then G is an $\text{Inc}(\mathbb{N})$ -equivariant Gröbner basis for I if and only if the S-pair $S(\sigma(f), \tau(g))$ has a remainder of zero upon $\text{Inc}(\mathbb{N})$ -division by G for all $f, g \in G$ and all $\sigma, \tau \in \text{Inc}(\mathbb{N})$.

Remark: this is just the usual Buchberger's Criterion applied to $\text{Inc}(\mathbb{N})G$.

Roadblock: since $\text{Inc}(\mathbb{N})G$ is infinite, it is not clear if one can check the Equivariant Buchberger's Criterion in finite time.

Roadblock: since $\text{Inc}(\mathbb{N})G$ is infinite, it is not clear if one can check the Equivariant Buchberger's Criterion in finite time.

We will remedy this using the following crucial result:

Theorem

Let $m, n \in \mathbb{N}$, and let $\sigma : [m] \rightarrow \mathbb{N}$ and $\tau : [n] \rightarrow \mathbb{N}$ be strictly increasing maps. Then there are maps $\rho \in \text{Inc}(\mathbb{N})$, $\sigma' \in \text{Inc}_{m, m+n}$, and $\tau' \in \text{Inc}_{n, m+n}$ such that

$$\rho \circ \sigma' = \sigma \quad \text{and} \quad \rho \circ \tau' = \tau.$$

Equivariant Gröbner Bases

An example:

- Consider the maps $\sigma : [3] \rightarrow \mathbb{N}$ and $\tau : [4] \rightarrow \mathbb{N}$ given by

| | | | |
|-------------|---|---|---|
| i | 1 | 2 | 3 |
| $\sigma(i)$ | 2 | 5 | 9 |

and

| | | | | |
|-----------|---|---|---|----|
| i | 1 | 2 | 3 | 4 |
| $\tau(i)$ | 1 | 2 | 4 | 11 |

Equivariant Gröbner Bases

An example:

- Consider the maps $\sigma : [3] \rightarrow \mathbb{N}$ and $\tau : [4] \rightarrow \mathbb{N}$ given by

| | | | |
|-------------|---|---|---|
| i | 1 | 2 | 3 |
| $\sigma(i)$ | 2 | 5 | 9 |

 and

| | | | | |
|-----------|---|---|---|----|
| i | 1 | 2 | 3 | 4 |
| $\tau(i)$ | 1 | 2 | 4 | 11 |

- Pick $\rho \in \text{Inc}(\mathbb{N})$ satisfying

| | | | | | | | |
|-----------|---|---|---|---|---|---|---|
| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| $\rho(i)$ | | | | | | | |

- Now define $\sigma' : [3] \rightarrow [7]$ and $\tau' : [4] \rightarrow [7]$ via

| | | | |
|--------------|---|---|---|
| i | 1 | 2 | 3 |
| $\sigma'(i)$ | | | |

 and

| | | | | |
|------------|---|---|---|---|
| i | 1 | 2 | 3 | 4 |
| $\tau'(i)$ | | | | |

Definition

For $f \in R$, define the **width** of f to be the largest index of any variable appearing in f . Denote this by $w(f)$. Since f is a polynomial, this quantity always exists and is finite.

Definition

For $f \in R$, define the **width** of f to be the largest index of any variable appearing in f . Denote this by $w(f)$. Since f is a polynomial, this quantity always exists and is finite.

Example: $w(x_1^2 + 3x_4^9 + x_{12}^6 x_5) = 12$.

Definition

For $f \in R$, define the **width** of f to be the largest index of any variable appearing in f . Denote this by $w(f)$. Since f is a polynomial, this quantity always exists and is finite.

Example: $w(x_1^2 + 3x_4^9 + x_{12}^6 x_5) = 12$. We now have the following version of the Equivariant Buchberger's Criterion that can be checked in finite time:

Theorem

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal. Then a subset $G \subseteq I$ is an $\text{Inc}(\mathbb{N})$ -equivariant Gröbner basis for I if and only if the S-pair $S(\sigma(f), \tau(g))$ has a remainder of zero upon $\text{Inc}(\mathbb{N})$ -division by G for all $f, g \in G$, all $\sigma \in \text{Inc}_{w(f), w(f)+w(g)}$, and all $\tau \in \text{Inc}_{w(g), w(f)+w(g)}$.

Why does this work?

Why does this work?

Given any $S(\bar{\sigma}(f), \bar{\tau}(g))$ for $f, g \in G$ and $\bar{\sigma}, \bar{\tau} \in \text{Inc}(\mathbb{N})$, we can rewrite the S-pair as

$$S(\bar{\sigma}(f), \bar{\tau}(g)) = S(\rho(\sigma(f)), \rho(\tau(g))) = \rho(S(\sigma(f), \tau(g)))$$

for some $\rho \in \text{Inc}(\mathbb{N})$, some $\sigma \in \text{Inc}_{w(f), w(f)+w(g)}$ and some $\tau \in \text{Inc}_{w(g), w(f)+w(g)}$ by our earlier result.

Since $S(\sigma(f), \tau(g))$ is assumed to have remainder zero upon $\text{Inc}(\mathbb{N})$ -division by G , so will $S(\bar{\sigma}(f), \bar{\tau}(g))$.

We can now formulate a finite Equivariant Buchberger's Algorithm which works the same as in the classical case, except we need to check more (but still finitely many) S -pairs now.

Theorem (Equivariant Buchberger's Algorithm)

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal. Then a finite $\text{Inc}(\mathbb{N})$ -equivariant Gröbner basis for I exists and can be computed in finite time.




We can now formulate a finite Equivariant Buchberger's Algorithm which works the same as in the classical case, except we need to check more (but still finitely many) S -pairs now.

Theorem (Equivariant Buchberger's Algorithm)

Let $I \subseteq R$ be an $\text{Inc}(\mathbb{N})$ -invariant ideal. Then a finite $\text{Inc}(\mathbb{N})$ -equivariant Gröbner basis for I exists and can be computed in finite time.

Remarks:

- Essentially the same process as the classical Buchberger's Algorithm.
- Terminates since R is $\text{Inc}(\mathbb{N})$ -Noetherian.
- Each step is a finite check since for $f, g \in G$, the sets $\text{Inc}_{w(f), w(f)+w(g)}$ and $\text{Inc}_{w(g), w(f)+w(g)}$ are finite.

-  Daniel E. Cohen. Closure relations, Buchberger's algorithm, and polynomials in infinitely many variables. In *Computation theory and logic*, volume 270 of *Lect. Notes Comput. Sci.*, pages 78–87, 1987.
-  Matthias Aschenbrenner and Christopher J. Hillar. Finite generation of symmetric ideals. *Trans. Amer. Math. Soc.*, 359(11):5171–5192, 2007.
-  Christopher J. Hillar, Seth Sullivant, Finite Gröbner bases in infinite dimensional polynomial rings and applications, *Advances in Mathematics*, Volume 229, Issue 1, 2012, Pages 1-25, ISSN 0001-8708, <https://doi.org/10.1016/j.aim.2011.08.009>.