Finite Computation of Gröbner Bases for OI-Modules

Michael Hanson Morrow

University of Kentucky

2021

Outline

- Classical motivation

Outline

- Classical motivation
- Preliminary notions
  - The category OI
  - OI-algebras and OI-modules
  - Direct sums and submodules
  - Orbits and generation of submodules

Outline

- Classical motivation
- Preliminary notions
  - The category OI
  - OI-algebras and OI-modules
  - Direct sums and submodules
  - Orbits and generation of submodules
- Gröbner bases
  - Free OI-modules
  - Monomials
  - Initial modules

Outline

- Classical motivation
- Preliminary notions
  - The category OI
  - OI-algebras and OI-modules
  - Direct sums and submodules
  - Orbits and generation of submodules
- Gröbner bases
  - Free OI-modules
  - Monomials
  - Initial modules
- Computation
  - Division Algorithm
  - OI-Factorization Lemma
  - OI-Buchberger's Criterion and Algorithm

Classical Motivation

1. Let K be a field, and let $R = K[x_1, \ldots, x_n]$.

Classical Motivation

1. Let K be a field, and let $R = K[x_1, \ldots, x_n]$.
2. Consider the free R-module R^s for some $s < \infty$.

Classical Motivation

1. Let K be a field, and let $R = K[x_1, \ldots, x_n]$.
2. Consider the free R-module R^s for some $s < \infty$.
3. Let M be a finitely generated submodule of R^s.

Classical Motivation

1. Let K be a field, and let $R = K[x_1, \ldots, x_n]$.
2. Consider the free R-module R^s for some $s < \infty$.
3. Let M be a finitely generated submodule of R^s.
4. Buchberger's Algorithm (see [Eis95, 15.9]) allows one to compute a finite Gröbner basis for M in finite time.

Classical Motivation

1. Let K be a field, and let $R = K[x_1, \ldots, x_n]$.
2. Consider the free R-module R^s for some $s < \infty$.
3. Let M be a finitely generated submodule of R^s.
4. Buchberger's Algorithm (see [Eis95, 15.9]) allows one to compute a finite Gröbner basis for M in finite time.

Question

Consider a sequence of modules $M_0, M_1, M_2, \ldots$ over polynomial rings $P_0, P_1, P_2, \ldots$ respectively. Can we find finitely many finite Gröbner bases $G \subseteq M_i$ such that any module M_j has a finite Gröbner basis expressable in terms of the G if $i \leq j$?

Preliminary Notions: OI-Algebras

- Let $[n] = \{1, \ldots, n\}$ for $n \in \mathbb{N}$ and set $[0] = \varnothing$.
- Let OI denote the category whose objects are $[n]$ for $n \in \mathbb{Z}_{\geq 0}$ and whose morphisms are strictly increasing maps.
- Let K be a field, and denote by K-Alg the category of commutative, associative, unital K-algebras whose morphisms are unital K-algebra homomorphisms.

Preliminary Notions: OI-Algebras

- Let $[n] = \{1, \ldots, n\}$ for $n \in \mathbb{N}$ and set $[0] = \varnothing$.
- Let OI denote the category whose objects are $[n]$ for $n \in \mathbb{Z}_{\geq 0}$ and whose morphisms are strictly increasing maps.
- Let K be a field, and denote by K-Alg the category of commutative, associative, unital K-algebras whose morphisms are unital K-algebra homomorphisms.

Definition

An OI-*algebra* over K is a covariant functor $\mathbf{A} : \mathrm{OI} \longrightarrow K\text{-Alg}$ such that $\mathbf{A}(\varnothing) = K$.

Preliminary Notions: OI-Algebras

- For an object $[n] \in \mathrm{OI}$ and any functor F out of OI, we write F_n instead of $F([n])$.
- We write $\mathrm{Hom}(m, n)$ instead of $\mathrm{Hom}_{\mathrm{OI}}([m], [n])$.

Preliminary Notions: OI-Algebras

- For an object $[n] \in \mathrm{OI}$ and any functor F out of OI, we write F_n instead of $F([n])$.
- We write $\mathrm{Hom}(m,n)$ instead of $\mathrm{Hom}_{\mathrm{OI}}([m],[n])$.

Example

Fix $c \in \mathbb{N}$ and define an OI-algebra $\mathbf{P}$ as follows:

1. For $m \geq 0$ set
$$\mathbf{P}_m = K[x_{i,j} \ : \ i \in [c],\ j \in [m]].$$
2. For $\varepsilon \in \mathrm{Hom}(m,n)$ define
$$\mathbf{P}(\varepsilon) : \mathbf{P}_m \longrightarrow \mathbf{P}_n \quad \text{via} \quad x_{i,j} \longmapsto x_{i,\varepsilon(j)}.$$

Preliminary Notions: OI-Algebras

- For an object $[n] \in \mathrm{OI}$ and any functor F out of OI, we write F_n instead of $F([n])$.
- We write $\mathrm{Hom}(m, n)$ instead of $\mathrm{Hom}_{\mathrm{OI}}([m], [n])$.

Example

Fix $c \in \mathbb{N}$ and define an OI-algebra $\mathbf{P}$ as follows:

1. For $m \geq 0$ set
$$\mathbf{P}_m = K[x_{i,j} \; : \; i \in [c], \; j \in [m]].$$
2. For $\varepsilon \in \mathrm{Hom}(m, n)$ define
$$\mathbf{P}(\varepsilon) : \mathbf{P}_m \longrightarrow \mathbf{P}_n \quad \text{via} \quad x_{i,j} \longmapsto x_{i,\varepsilon(j)}.$$

Example

If $c = 1$, we can think of $\mathbf{P}$ as the sequence
$$K, \; K[x_1], \; K[x_1, x_2], \; K[x_1, x_2, x_3], \; \ldots$$

Preliminary Notions: OI-Modules

- Let K-Vect denote the category of vector spaces over K whose morphisms are K-linear maps.

Preliminary Notions: OI-Modules

- Let K-Vect denote the category of vector spaces over K whose morphisms are K-linear maps.

Definition

An OI-*module* over an OI-algebra $\mathbf{A}$ is a covariant functor $\mathbf{M} : \mathrm{OI} \longrightarrow K\text{-Vect}$ such that:

1. Each $\mathbf{M}_m$ is an $\mathbf{A}_m$-module.
2. For each $\varepsilon \in \mathrm{Hom}(m, n)$ and any $a \in \mathbf{A}_m$, the diagram

$$\begin{array}{ccc} \mathbf{M}_m & \xrightarrow{\mathbf{M}(\varepsilon)} & \mathbf{M}_n \\ {\scriptstyle \cdot a}\downarrow & & \downarrow{\scriptstyle \cdot \mathbf{A}(\varepsilon)(a)} \\ \mathbf{M}_m & \xrightarrow{\mathbf{M}(\varepsilon)} & \mathbf{M}_n \end{array}$$

   commutes.

We often refer to $\mathbf{M}$ as an $\mathbf{A}$-*module*.

Preliminary Notions: OI-Modules

Example

Let $d \geq 0$ be an integer, and define an OI-module $\mathbf{F}^{\mathrm{OI},d}$ over $\mathbf{A}$ as follows:

1. For $m \geq 0$, set

$$\mathbf{F}^{\mathrm{OI},d}_m = \bigoplus_{\pi \in \mathrm{Hom}(d,m)} \mathbf{A}_m e_\pi \cong (\mathbf{A}_m)^{\binom{m}{d}}.$$

2. For $\varepsilon \in \mathrm{Hom}(m, n)$ define

$$\mathbf{F}^{\mathrm{OI},d}(\varepsilon) : \mathbf{F}^{\mathrm{OI},d}_m \longrightarrow \mathbf{F}^{\mathrm{OI},d}_n \quad \text{via} \quad e_\pi \longmapsto e_{\varepsilon \circ \pi}.$$

The module $\mathbf{F}^{\mathrm{OI},d}$ is an example of a *free* OI-module over $\mathbf{A}$.

Preliminary Notions: OI-Modules

Example

Let $d \geq 0$ be an integer, and define an OI-module $\mathbf{F}^{\text{OI},d}$ over $\mathbf{A}$ as follows:

1. For $m \geq 0$, set
$$\mathbf{F}^{\text{OI},d}_m = \bigoplus_{\pi \in \text{Hom}(d,m)} \mathbf{A}_m e_\pi \cong (\mathbf{A}_m)^{\binom{m}{d}}.$$
2. For $\varepsilon \in \text{Hom}(m,n)$ define
$$\mathbf{F}^{\text{OI},d}(\varepsilon) : \mathbf{F}^{\text{OI},d}_m \longrightarrow \mathbf{F}^{\text{OI},d}_n \quad \text{via} \quad e_\pi \longmapsto e_{\varepsilon \circ \pi}.$$

The module $\mathbf{F}^{\text{OI},d}$ is an example of a *free* OI-module over $\mathbf{A}$.

Example

If $c = 1$ and $d = 2$, we can think of $\mathbf{F}^{\text{OI},2}$ over $\mathbf{P}$ as the sequence
$$0,\ 0,\ K[x_1, x_2],\ K[x_1, x_2, x_3]^3,\ K[x_1, x_2, x_3, x_4]^6,\ \ldots$$

Preliminary Notions: Direct Sums and Submodules

Definition

A *subset* of an OI-module $\mathbf{M}$ is a subset of $\coprod_{m \geq 0} \mathbf{M}_m$, and therefore an *element* of $\mathbf{M}$ is an element of $\mathbf{M}_m$ for some $m \geq 0$.

Preliminary Notions: Direct Sums and Submodules

Definition

A *subset* of an OI-module $\mathbf{M}$ is a subset of $\coprod_{m \geq 0} \mathbf{M}_m$, and therefore an *element* of $\mathbf{M}$ is an element of $\mathbf{M}_m$ for some $m \geq 0$.

Definition

Let $\mathbf{M}$ and $\mathbf{N}$ be OI-modules over an OI-algebra $\mathbf{A}$.

- The *direct sum* $\mathbf{M} \oplus \mathbf{N}$ of $\mathbf{M}$ and $\mathbf{N}$ is the OI-module given by $(\mathbf{M} \oplus \mathbf{N})_m = \mathbf{M}_m \oplus \mathbf{N}_m$ for $m \geq 0$, and $(\mathbf{M} \oplus \mathbf{N})(\varepsilon) = \mathbf{M}(\varepsilon) \oplus \mathbf{N}(\varepsilon)$ whenever $\varepsilon \in \mathrm{Hom}(m, n)$.

Preliminary Notions: Direct Sums and Submodules

Definition

A *subset* of an OI-module $\mathbf{M}$ is a subset of $\coprod_{m \geq 0} \mathbf{M}_m$, and therefore an *element* of $\mathbf{M}$ is an element of $\mathbf{M}_m$ for some $m \geq 0$.

Definition

Let $\mathbf{M}$ and $\mathbf{N}$ be OI-modules over an OI-algebra $\mathbf{A}$.

- The *direct sum* $\mathbf{M} \oplus \mathbf{N}$ of $\mathbf{M}$ and $\mathbf{N}$ is the OI-module given by $(\mathbf{M} \oplus \mathbf{N})_m = \mathbf{M}_m \oplus \mathbf{N}_m$ for $m \geq 0$, and $(\mathbf{M} \oplus \mathbf{N})(\varepsilon) = \mathbf{M}(\varepsilon) \oplus \mathbf{N}(\varepsilon)$ whenever $\varepsilon \in \mathrm{Hom}(m, n)$.
- We say $\mathbf{M}$ is a *submodule* of $\mathbf{N}$ if $\mathbf{M} \subseteq \mathbf{N}$ and $\mathbf{N}$ induces an $\mathbf{A}$-module structure on $\mathbf{M}$.

Preliminary Notions: Direct Sums and Submodules

Definition

A *subset* of an OI-module $\mathbf{M}$ is a subset of $\coprod_{m \geq 0} \mathbf{M}_m$, and therefore an *element* of $\mathbf{M}$ is an element of $\mathbf{M}_m$ for some $m \geq 0$.

Definition

Let $\mathbf{M}$ and $\mathbf{N}$ be OI-modules over an OI-algebra $\mathbf{A}$.

- The *direct sum* $\mathbf{M} \oplus \mathbf{N}$ of $\mathbf{M}$ and $\mathbf{N}$ is the OI-module given by $(\mathbf{M} \oplus \mathbf{N})_m = \mathbf{M}_m \oplus \mathbf{N}_m$ for $m \geq 0$, and $(\mathbf{M} \oplus \mathbf{N})(\varepsilon) = \mathbf{M}(\varepsilon) \oplus \mathbf{N}(\varepsilon)$ whenever $\varepsilon \in \mathrm{Hom}(m, n)$.
- We say $\mathbf{M}$ is a *submodule* of $\mathbf{N}$ if $\mathbf{M} \subseteq \mathbf{N}$ and $\mathbf{N}$ induces an $\mathbf{A}$-module structure on $\mathbf{M}$.
- For $f \in \mathbf{M}_m$, we say f has *width* m, written $w(f) = m$. We call $\mathbf{M}_m$ the *width m component* of $\mathbf{M}$.

Preliminary Notions: Orbits and Generation

Definition

Let $B \subseteq \mathbf{M}$. Denote by $\langle B \rangle_{\mathbf{M}}$ the smallest submodule of $\mathbf{M}$ containing B. We call it the submodule *generated by* B. If B can be taken finite, then we say $\langle B \rangle_{\mathbf{M}}$ is *finitely generated*.

Preliminary Notions: Orbits and Generation

Definition

Let $B \subseteq \mathbf{M}$. Denote by $\langle B \rangle_{\mathbf{M}}$ the smallest submodule of $\mathbf{M}$ containing B. We call it the submodule *generated by* B. If B can be taken finite, then we say $\langle B \rangle_{\mathbf{M}}$ is *finitely generated*.

Example

- $\mathbf{F}^{\mathrm{OI},d}$ is finitely generated by a single element $e_{\mathrm{id}_{[d]}}$.
- $\mathbf{F}^{\mathrm{OI},d}$ is not isomorphic to a direct sum of copies of $\mathbf{A}$ if $d \geq 1$. This is because $\mathbf{A}_0 = K$ but $\mathbf{F}_0^{\mathrm{OI},d} = 0$ if $d \geq 1$. Thus, there are more free OI-modules over $\mathbf{A}$ than just sums of copies of $\mathbf{A}$.

Preliminary Notions: Orbits and Generation

Definition

Let $B \subseteq \mathbf{M}$. Denote by $\langle B \rangle_{\mathbf{M}}$ the smallest submodule of $\mathbf{M}$ containing B. We call it the submodule *generated by* B. If B can be taken finite, then we say $\langle B \rangle_{\mathbf{M}}$ is *finitely generated*.

Example

- $\mathbf{F}^{\mathrm{OI},d}$ is finitely generated by a single element $e_{\mathrm{id}_{[d]}}$.
- $\mathbf{F}^{\mathrm{OI},d}$ is not isomorphic to a direct sum of copies of $\mathbf{A}$ if $d \geq 1$. This is because $\mathbf{A}_0 = K$ but $\mathbf{F}_0^{\mathrm{OI},d} = 0$ if $d \geq 1$. Thus, there are more free OI-modules over $\mathbf{A}$ than just sums of copies of $\mathbf{A}$.
- Let $c = 1$ and consider $x_1, x_2 \in \mathbf{P}_2$. Then $I = \langle x_1 x_2 \rangle_{\mathbf{P}}$ is an ideal of $\mathbf{P}$ with $I_n = \langle x_i x_j \ : \ 1 \leq i < j \leq n \rangle$.

Preliminary Notions: Orbits and Generation

Definition

Let $B \subseteq \mathbf{M}$ and let $m \geq 0$. The *m-orbit* of an element $b \in B$ is the set

$$\mathrm{Orb}(b, m) = \{\mathbf{M}(\varepsilon)(b) \;:\; \varepsilon \in \mathrm{Hom}(w(b), m)\}.$$

The *m-orbit* of B is then defined to be

$$\mathrm{Orb}(B, m) = \bigcup_{b \in B} \mathrm{Orb}(b, m).$$

Preliminary Notions: Orbits and Generation

Definition

Let $B \subseteq \mathbf{M}$ and let $m \geq 0$. The *m-orbit* of an element $b \in B$ is the set

$$\mathrm{Orb}(b, m) = \{\mathbf{M}(\varepsilon)(b) \;:\; \varepsilon \in \mathrm{Hom}(w(b), m)\}.$$

The *m-orbit* of B is then defined to be

$$\mathrm{Orb}(B, m) = \bigcup_{b \in B} \mathrm{Orb}(b, m).$$

Remark

Let $B \subseteq \mathbf{M}$. Then $\langle B \rangle_{\mathbf{M}}$ can be realized as the submodule of $\mathbf{M}$ given by

$$(\langle B \rangle_{\mathbf{M}})_m = \langle \mathrm{Orb}(B, m) \rangle$$

for $m \geq 0$, where the RHS is generated as an $\mathbf{A}_m$-submodule of $\mathbf{M}_m$.

Preliminary Notions: Summary

- OI is the category of ordered sets $[n]$ with morphisms given by strictly increasing maps.

Preliminary Notions: Summary

- **OI** is the category of ordered sets $[n]$ with morphisms given by strictly increasing maps.
- **P** is an **OI**-algebra over K consisting of polynomial rings with increasingly many variables.

Preliminary Notions: Summary

- OI is the category of ordered sets $[n]$ with morphisms given by strictly increasing maps.
- **P** is an OI-algebra over K consisting of polynomial rings with increasingly many variables.
- $\mathbf{F}^{\mathrm{OI},d}$ is a free OI-module over an OI-algebra **A** that is finitely generated by a single element $e_{\mathrm{id}_{[d]}}$.

Preliminary Notions: Summary

- OI is the category of ordered sets $[n]$ with morphisms given by strictly increasing maps.
- $\mathbf{P}$ is an OI-algebra over K consisting of polynomial rings with increasingly many variables.
- $\mathbf{F}^{\mathrm{OI},d}$ is a free OI-module over an OI-algebra $\mathbf{A}$ that is finitely generated by a single element $e_{\mathrm{id}_{[d]}}$.
- If $\mathbf{M}$ is an OI-module and $B \subseteq \mathbf{M}$, then $\langle B \rangle_{\mathbf{M}}$ is the submodule of $\mathbf{M}$ generated by B.

Preliminary Notions: Summary

- OI is the category of ordered sets $[n]$ with morphisms given by strictly increasing maps.
- $\mathbf{P}$ is an OI-algebra over K consisting of polynomial rings with increasingly many variables.
- $\mathbf{F}^{\mathrm{OI},d}$ is a free OI-module over an OI-algebra $\mathbf{A}$ that is finitely generated by a single element $e_{\mathrm{id}_{[d]}}$.
- If $\mathbf{M}$ is an OI-module and $B \subseteq \mathbf{M}$, then $\langle B \rangle_{\mathbf{M}}$ is the submodule of $\mathbf{M}$ generated by B.
- The m-orbit of an element $b \in B$ is the set of all $\mathbf{M}(\varepsilon)(b)$ where $\varepsilon \in \mathrm{Hom}(w(b), m)$.

Preliminary Notions: Summary

- OI is the category of ordered sets $[n]$ with morphisms given by strictly increasing maps.
- $\mathbf{P}$ is an OI-algebra over K consisting of polynomial rings with increasingly many variables.
- $\mathbf{F}^{\mathrm{OI},d}$ is a free OI-module over an OI-algebra $\mathbf{A}$ that is finitely generated by a single element $e_{\mathrm{id}_{[d]}}$.
- If $\mathbf{M}$ is an OI-module and $B \subseteq \mathbf{M}$, then $\langle B \rangle_{\mathbf{M}}$ is the submodule of $\mathbf{M}$ generated by B.
- The m-orbit of an element $b \in B$ is the set of all $\mathbf{M}(\varepsilon)(b)$ where $\varepsilon \in \mathrm{Hom}(w(b), m)$.

We now turn our attention to Gröbner bases.

Gröbner Bases: Free OI-Modules

Definition

In general, we define a *free* OI-module over $\mathbf{A}$ to be a direct sum $\bigoplus_{\lambda \in \Lambda} \mathbf{F}^{\mathrm{OI}, d_\lambda}$ for integers $d_\lambda \geq 0$.

Gröbner Bases: Free OI-Modules

Definition

In general, we define a *free* OI-module over $\mathbf{A}$ to be a direct sum $\bigoplus_{\lambda \in \Lambda} \mathbf{F}^{\mathrm{OI},d_\lambda}$ for integers $d_\lambda \geq 0$.

Remark

If $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI},d_i}$ is a free OI-module, then

$$\mathbf{F}_m = \bigoplus_{\substack{1 \leq i \leq s \\ \pi \in \mathrm{Hom}(d_i,m)}} \mathbf{A}_m e_{\pi,i} \cong (\mathbf{A}_m)^{\sum_{i=1}^{s} \binom{m}{d_i}} \quad \text{for } m \geq 0.$$

Gröbner Bases: Free OI-Modules

Definition

In general, we define a *free* OI-module over $\mathbf{A}$ to be a direct sum $\bigoplus_{\lambda \in \Lambda} \mathbf{F}^{\mathrm{OI}, d_\lambda}$ for integers $d_\lambda \geq 0$.

Remark

If $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI}, d_i}$ is a free OI-module, then

$$\mathbf{F}_m = \bigoplus_{\substack{1 \leq i \leq s \\ \pi \in \mathrm{Hom}(d_i, m)}} \mathbf{A}_m e_{\pi, i} \cong (\mathbf{A}_m)^{\sum_{i=1}^{s} \binom{m}{d_i}} \quad \text{for } m \geq 0.$$

- $\mathbf{F}$ is generated by the $e_{\mathrm{id}_{[d_i]}, i}$, and we call these elements the *basis elements* of $\mathbf{F}$.

Gröbner Bases: Free OI-Modules

Definition

In general, we define a *free* OI-module over $\mathbf{A}$ to be a direct sum $\bigoplus_{\lambda \in \Lambda} \mathbf{F}^{\mathrm{OI},d_\lambda}$ for integers $d_\lambda \geq 0$.

Remark

If $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI},d_i}$ is a free OI-module, then

$$\mathbf{F}_m = \bigoplus_{\substack{1 \leq i \leq s \\ \pi \in \mathrm{Hom}(d_i,m)}} \mathbf{A}_m e_{\pi,i} \cong (\mathbf{A}_m)^{\sum_{i=1}^{s} \binom{m}{d_i}} \quad \text{for } m \geq 0.$$

- $\mathbf{F}$ is generated by the $e_{\mathrm{id}_{[d_i]},i}$, and we call these elements the *basis elements* of $\mathbf{F}$.
- The $e_{\pi,i} \in \mathbf{F}_m$ are called the *local basis elements* of $\mathbf{F}_m$.

Gröbner Bases: Free OI-Modules

Definition

In general, we define a *free* OI-module over $\mathbf{A}$ to be a direct sum $\bigoplus_{\lambda \in \Lambda} \mathbf{F}^{\mathrm{OI},d_\lambda}$ for integers $d_\lambda \geq 0$.

Remark

If $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI},d_i}$ is a free OI-module, then

$$\mathbf{F}_m = \bigoplus_{\substack{1 \leq i \leq s \\ \pi \in \mathrm{Hom}(d_i,m)}} \mathbf{A}_m e_{\pi,i} \cong (\mathbf{A}_m)^{\sum_{i=1}^{s} \binom{m}{d_i}} \quad \text{for } m \geq 0.$$

- $\mathbf{F}$ is generated by the $e_{\mathrm{id}_{[d_i]},i}$, and we call these elements the *basis elements* of $\mathbf{F}$.
- The $e_{\pi,i} \in \mathbf{F}_m$ are called the *local basis elements* of $\mathbf{F}_m$.
- The second index in $e_{\pi,i}$ is for distinguishing which direct summand the local basis elements come from (we may have $d_i = d_j$ for some $i \neq j$).

Gröbner Bases: Monomials

- From now on, we consider finitely generated free OI-modules $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI},d_i}$ over $\mathbf{P}$.

Definition

A *monomial* in $\mathbf{F}$ is an element of the form

$$x^u e_{\pi,i} \in \mathbf{F}_m$$

where $\pi \in \mathrm{Hom}(d_i, m)$ and x^u is a monomial in $\mathbf{P}_m$. Elements of $\mathbf{F}$ can be expressed as K-linear combinations of monomials.

Gröbner Bases: Monomials

- From now on, we consider finitely generated free OI-modules $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI},d_i}$ over $\mathbf{P}$.

Definition

A *monomial* in $\mathbf{F}$ is an element of the form

$$x^u e_{\pi,i} \in \mathbf{F}_m$$

where $\pi \in \mathrm{Hom}(d_i, m)$ and x^u is a monomial in $\mathbf{P}_m$. Elements of $\mathbf{F}$ can be expressed as K-linear combinations of monomials.

Definition

Let $\mu, \nu \in \mathbf{F}$ be monomials. We say ν is OI-*divisible* by μ if ν is divisible by an element of $\mathrm{Orb}(\mu, w(\nu))$.

Gröbner Bases: Monomials

Definition

A *monomial order* on $\mathbf{F}$ is a total order $<$ on the monomials of $\mathbf{F}$ such that if μ and ν are monomials in $\mathbf{F}_m$ with $\mu < \nu$, then:

1. $\mu < x^p \mu < x^p \nu$ for any monomial $1 \neq x^p \in \mathbf{P}_m$; and
2. $\mu < \mathbf{F}(\varepsilon)(\mu) < \mathbf{F}(\varepsilon)(\nu)$ whenever $\varepsilon \in \mathrm{Hom}(m, n)$ and $m < n$.

Gröbner Bases: Monomials

Definition

A *monomial order* on $\mathbf{F}$ is a total order $<$ on the monomials of $\mathbf{F}$ such that if μ and ν are monomials in $\mathbf{F}_m$ with $\mu < \nu$, then:

1. $\mu < x^p\mu < x^p\nu$ for any monomial $1 \neq x^p \in \mathbf{P}_m$; and
2. $\mu < \mathbf{F}(\varepsilon)(\mu) < \mathbf{F}(\varepsilon)(\nu)$ whenever $\varepsilon \in \mathrm{Hom}(m, n)$ and $m < n$.

Example (Lexicographic Order)

Order the monomials in each $\mathbf{P}_m$ lexicographically with $x_{i',j'} < x_{i,j}$ if either $j' < j$ or $j' = j$ and $i' < i$. Define $e_{\rho,j} < e_{\pi,i}$ if $i < j$. For a fixed i, identify a monomial $e_{\pi,i} \in \mathbf{F}_m^{\mathrm{OI},d_i}$ with a vector $(m, \pi(1), \ldots, \pi(d_i)) \in \mathbb{N}^{d_i+1}$ and order such monomials using the lexicographic order on $\mathbb{N}^{d_i+1}$. Finally, for $x^a e_{\pi,i}$ and $x^b e_{\rho,j}$ in $\mathbf{F}$, define $x^b e_{\rho,j} < x^a e_{\pi,i}$ if $e_{\rho,j} < e_{\pi,i}$ or $e_{\pi,i} = e_{\rho,j}$ and $x^b < x^a$ in $\mathbf{P}$.

Gröbner Bases: Monomials

- It turns out that any monomial order on $\mathbf{F}$ is a well-order (see [Nag21, 5.3b] and [NR19, 6.5]).

Gröbner Bases: Monomials

- It turns out that any monomial order on $\mathbf{F}$ is a well-order (see [Nag21, 5.3b] and [NR19, 6.5]).

Definition

Fix a monomial order $<$ on $\mathbf{F}$, and let $f = \sum c_\mu \mu \in \mathbf{F}_m$ for some $m \in \mathbb{N}_0$, some monomials $\mu \in \mathbf{F}_m$ and some coefficients $c_\mu \in K$. If $f \neq 0$:

1. Define its *leading monomial* $\mathrm{lm}(f)$ to be the largest monomial μ that has a nonzero coefficient c_μ.
2. We call c_μ the *leading coefficient* of f, denoted $\mathrm{lc}(f)$.
3. Define the *leading term* of f to be $\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lm}(f)$.

For a subset $E \subseteq \mathbf{F}$, write $\mathrm{lm}(E)$ for the set of all leading monomials of elements of E.

Gröbner Bases: Monomials

- It turns out that any monomial order on $\mathbf{F}$ is a well-order (see [Nag21, 5.3b] and [NR19, 6.5]).

Definition

Fix a monomial order $<$ on $\mathbf{F}$, and let $f = \sum c_\mu \mu \in \mathbf{F}_m$ for some $m \in \mathbb{N}_0$, some monomials $\mu \in \mathbf{F}_m$ and some coefficients $c_\mu \in K$. If $f \neq 0$:

1. Define its *leading monomial* $\mathrm{lm}(f)$ to be the largest monomial μ that has a nonzero coefficient c_μ.
2. We call c_μ the *leading coefficient* of f, denoted $\mathrm{lc}(f)$.
3. Define the *leading term* of f to be $\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lm}(f)$.

For a subset $E \subseteq \mathbf{F}$, write $\mathrm{lm}(E)$ for the set of all leading monomials of elements of E.

- The properties of a monomial order allow one to deduce that $\mathbf{F}(\varepsilon)(\mathrm{lm}(f)) = \mathrm{lm}(\mathbf{F}(\varepsilon)(f))$ for any $f \in \mathbf{F}_m$ and any $\varepsilon \in \mathrm{Hom}(m, n)$ with $m \leq n$.

Gröbner Bases: Initial Modules

Definition

Let $<$ be a monomial order on $\mathbf{F}$. For any submodule $\mathbf{M}$ of $\mathbf{F}$, the *initial module* of $\mathbf{M}$ is

$$\mathrm{in}(\mathbf{M}) = \langle \mathrm{lm}(\mathbf{M}) \rangle_{\mathbf{F}}.$$

A subset $B \subseteq \mathbf{M}$ is called a *Gröbner basis* of $\mathbf{M}$ (w.r.t. $<$) if

$$\mathrm{in}(\mathbf{M}) = \langle \mathrm{lm}(B) \rangle_{\mathbf{F}}.$$

Gröbner Bases: Initial Modules

Definition

Let $<$ be a monomial order on $\mathbf{F}$. For any submodule $\mathbf{M}$ of $\mathbf{F}$, the *initial module* of $\mathbf{M}$ is

$$\text{in}(\mathbf{M}) = \langle \text{lm}(\mathbf{M}) \rangle_{\mathbf{F}}.$$

A subset $B \subseteq \mathbf{M}$ is called a *Gröbner basis* of $\mathbf{M}$ (w.r.t. $<$) if

$$\text{in}(\mathbf{M}) = \langle \text{lm}(B) \rangle_{\mathbf{F}}.$$

Remark

One can simply take $B = \mathbf{M}$, but the more interesting cases are when B is finite.

Gröbner Bases: Summary

- Free OI-modules are sums of $\mathbf{F}^{\mathrm{OI},d_\lambda}$ for integers $d_\lambda \geq 0$.

Gröbner Bases: Summary

- Free OI-modules are sums of $\mathbf{F}^{\mathrm{OI},d_\lambda}$ for integers $d_\lambda \geq 0$.
- We consider finitely generated free OI-modules $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI},d_i}$ over $\mathbf{P}$.

Gröbner Bases: Summary

- Free OI-modules are sums of $\mathbf{F}^{\mathrm{OI},d_\lambda}$ for integers $d_\lambda \geq 0$.
- We consider finitely generated free OI-modules $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI},d_i}$ over $\mathbf{P}$.
- Monomials of $\mathbf{F}$ are elements of the form $x^u e_{\pi,i}$ where x^u is a monomial in $\mathbf{P}$.

Gröbner Bases: Summary

- Free OI-modules are sums of $\mathbf{F}^{\mathrm{OI},d_\lambda}$ for integers $d_\lambda \geq 0$.
- We consider finitely generated free OI-modules $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI},d_i}$ over $\mathbf{P}$.
- Monomials of $\mathbf{F}$ are elements of the form $x^u e_{\pi,i}$ where x^u is a monomial in $\mathbf{P}$.
- Monomial orders are total orders that respect multiplication and are preserved by $\mathbf{F}(\varepsilon)$ whenever $\varepsilon \in \mathrm{Hom}(m, n)$.

Gröbner Bases: Summary

- Free OI-modules are sums of $\mathbf{F}^{\mathrm{OI},d_\lambda}$ for integers $d_\lambda \geq 0$.
- We consider finitely generated free OI-modules $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI},d_i}$ over $\mathbf{P}$.
- Monomials of $\mathbf{F}$ are elements of the form $x^u e_{\pi,i}$ where x^u is a monomial in $\mathbf{P}$.
- Monomial orders are total orders that respect multiplication and are preserved by $\mathbf{F}(\varepsilon)$ whenever $\varepsilon \in \mathrm{Hom}(m, n)$.
- If $\mathbf{M}$ is a submodule of $\mathbf{F}$, then a subset $B \subseteq \mathbf{M}$ is a Gröbner basis of $\mathbf{M}$ (with respect to some monomial order) if $\mathrm{in}(\mathbf{M}) = \langle \mathrm{lm}(B) \rangle_{\mathbf{F}}$.

Gröbner Bases: Summary

- Free OI-modules are sums of $\mathbf{F}^{\mathrm{OI},d_\lambda}$ for integers $d_\lambda \geq 0$.
- We consider finitely generated free OI-modules $\mathbf{F} = \bigoplus_{i=1}^{s} \mathbf{F}^{\mathrm{OI},d_i}$ over $\mathbf{P}$.
- Monomials of $\mathbf{F}$ are elements of the form $x^u e_{\pi,i}$ where x^u is a monomial in $\mathbf{P}$.
- Monomial orders are total orders that respect multiplication and are preserved by $\mathbf{F}(\varepsilon)$ whenever $\varepsilon \in \mathrm{Hom}(m,n)$.
- If $\mathbf{M}$ is a submodule of $\mathbf{F}$, then a subset $B \subseteq \mathbf{M}$ is a Gröbner basis of $\mathbf{M}$ (with respect to some monomial order) if $\mathrm{in}(\mathbf{M}) = \langle \mathrm{lm}(B) \rangle_{\mathbf{F}}$.

We're now ready to look at computation of Gröbner bases.

Computation: Division Algorithm

- Our main tool for doing computation is the division algorithm.

Definition

Let $B \subseteq \mathbf{F}$ and pick $f \in \mathbf{F}_m$. Suppose $f = \sum a_i f_i + r$ for some $a_i \in \mathbf{P}_m$, some $f_i \in \mathrm{Orb}(B, m)$ and some $r \in \mathbf{F}_m$ such that:

1. either $r = 0$ or $\mathrm{lm}(r)$ is not OI-divisible by any element of $\mathrm{lm}(B)$;
2. $\mathrm{lm}(r) < \mathrm{lm}(f)$ whenever $r \neq f$ and $f, r \neq 0$; and
3. $\mathrm{lm}(a_i f_i) \leq \mathrm{lm}(f)$ whenever $a_i f_i, f \neq 0$.

Then r is called a *remainder of f modulo B*.

Computation: Division Algorithm

- Our main tool for doing computation is the division algorithm.

Definition

Let $B \subseteq \mathbf{F}$ and pick $f \in \mathbf{F}_m$. Suppose $f = \sum a_i f_i + r$ for some $a_i \in \mathbf{P}_m$, some $f_i \in \mathrm{Orb}(B, m)$ and some $r \in \mathbf{F}_m$ such that:

1. either $r = 0$ or $\mathrm{lm}(r)$ is not OI-divisible by any element of $\mathrm{lm}(B)$;
2. $\mathrm{lm}(r) < \mathrm{lm}(f)$ whenever $r \neq f$ and $f, r \neq 0$; and
3. $\mathrm{lm}(a_i f_i) \leq \mathrm{lm}(f)$ whenever $a_i f_i, f \neq 0$.

Then r is called a *remainder of f modulo B*.

Remark

If f has a remainder of zero modulo B, then $f \in \langle B \rangle_{\mathbf{F}}$.

Computation: Division Algorithm

- Our main tool for doing computation is the division algorithm.

Definition

Let $B \subseteq \mathbf{F}$ and pick $f \in \mathbf{F}_m$. Suppose $f = \sum a_i f_i + r$ for some $a_i \in \mathbf{P}_m$, some $f_i \in \operatorname{Orb}(B, m)$ and some $r \in \mathbf{F}_m$ such that:

1. either $r = 0$ or $\operatorname{Im}(r)$ is not OI-divisible by any element of $\operatorname{Im}(B)$;
2. $\operatorname{Im}(r) < \operatorname{Im}(f)$ whenever $r \neq f$ and $f, r \neq 0$; and
3. $\operatorname{Im}(a_i f_i) \leq \operatorname{Im}(f)$ whenever $a_i f_i, f \neq 0$.

Then r is called a *remainder of f modulo B*.

Remark

If f has a remainder of zero modulo B, then $f \in \langle B \rangle_{\mathbf{F}}$.

Algorithm (Division Algorithm)

A remainder of $f \in \mathbf{F}_m$ modulo $B \subseteq \mathbf{F}$ can be computed in finite time.

Computation: Division Algorithm

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$, and let $B = \{x_1^2 e_{\mathrm{id}_{[1]}}, x_2^2 e_\rho + x_1 x_2 e_\rho\}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

Computation: Division Algorithm

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$, and let $B = \{x_1^2 e_{\mathrm{id}_{[1]}}, x_2^2 e_\rho + x_1 x_2 e_\rho\}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

- Let $b_1 = x_1^2 e_{\mathrm{id}_{[1]}}$ and let $b_2 = x_2^2 e_\rho + x_1 x_2 e_\rho$.

Computation: Division Algorithm

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$, and let $B = \{x_1^2 e_{\mathrm{id}_{[1]}}, x_2^2 e_\rho + x_1 x_2 e_\rho\}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

- Let $b_1 = x_1^2 e_{\mathrm{id}_{[1]}}$ and let $b_2 = x_2^2 e_\rho + x_1 x_2 e_\rho$.
- Fix the lex order $<$ on $\mathbf{F}$. Then $\mathrm{lm}(b_1) = x_1^2 e_{\mathrm{id}_{[1]}}$ and $\mathrm{lm}(b_2) = x_2^2 e_\rho$.

Computation: Division Algorithm

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$, and let $B = \{x_1^2 e_{\mathrm{id}_{[1]}}, x_2^2 e_\rho + x_1 x_2 e_\rho\}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

- Let $b_1 = x_1^2 e_{\mathrm{id}_{[1]}}$ and let $b_2 = x_2^2 e_\rho + x_1 x_2 e_\rho$.
- Fix the lex order $<$ on $\mathbf{F}$. Then $\mathrm{lm}(b_1) = x_1^2 e_{\mathrm{id}_{[1]}}$ and $\mathrm{lm}(b_2) = x_2^2 e_\rho$.
- We wish to compute a remainder of $f = x_1 x_2^2 e_\rho + x_2 e_\pi$ modulo B where $\pi : [1] \longrightarrow [2]$ is given by $\pi(1) = 1$.

Computation: Division Algorithm

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$, and let $B = \{x_1^2 e_{\mathrm{id}_{[1]}}, x_2^2 e_\rho + x_1 x_2 e_\rho\}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

- Let $b_1 = x_1^2 e_{\mathrm{id}_{[1]}}$ and let $b_2 = x_2^2 e_\rho + x_1 x_2 e_\rho$.
- Fix the lex order $<$ on $\mathbf{F}$. Then $\mathrm{lm}(b_1) = x_1^2 e_{\mathrm{id}_{[1]}}$ and $\mathrm{lm}(b_2) = x_2^2 e_\rho$.
- We wish to compute a remainder of $f = x_1 x_2^2 e_\rho + x_2 e_\pi$ modulo B where $\pi : [1] \longrightarrow [2]$ is given by $\pi(1) = 1$.
- We have $\mathrm{lm}(f) = x_1 x_2^2 e_\rho = x_1 \mathbf{F}(\rho)(\mathrm{lm}(b_1))$ so we define $r = f - x_1 \mathbf{F}(\rho)(b_1) = x_2 e_\pi$.

Computation: Division Algorithm

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$, and let $B = \{x_1^2 e_{\mathrm{id}_{[1]}}, x_2^2 e_\rho + x_1 x_2 e_\rho\}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

- Let $b_1 = x_1^2 e_{\mathrm{id}_{[1]}}$ and let $b_2 = x_2^2 e_\rho + x_1 x_2 e_\rho$.
- Fix the lex order $<$ on $\mathbf{F}$. Then $\mathrm{lm}(b_1) = x_1^2 e_{\mathrm{id}_{[1]}}$ and $\mathrm{lm}(b_2) = x_2^2 e_\rho$.
- We wish to compute a remainder of $f = x_1 x_2^2 e_\rho + x_2 e_\pi$ modulo B where $\pi : [1] \longrightarrow [2]$ is given by $\pi(1) = 1$.
- We have $\mathrm{lm}(f) = x_1 x_2^2 e_\rho = x_1 \mathbf{F}(\rho)(\mathrm{lm}(b_1))$ so we define $r = f - x_1 \mathbf{F}(\rho)(b_1) = x_2 e_\pi$.
- Since $\mathrm{lm}(r) = x_2 e_\pi$ is not OI-divisible by either $\mathrm{lm}(b_1)$ or $\mathrm{lm}(b_2)$, we are done, and r is a remainder of f modulo B.

Computation: Division Algorithm

Example (Continued)

- Since $\text{Im}(f) = x_1 x_2^2 e_\rho = x_1 \text{Im}(b_2)$, we could have also defined $r = f - x_1 b_2 = -x_1^2 x_2 e_\rho + x_2 e_\pi$.

Computation: Division Algorithm

Example (Continued)

- Since $\text{lm}(f) = x_1 x_2^2 e_\rho = x_1 \text{lm}(b_2)$, we could have also defined $r = f - x_1 b_2 = -x_1^2 x_2 e_\rho + x_2 e_\pi$.
- Since $\text{lm}(r) = -x_1^2 x_2 e_\rho$ is not OI-divisible by either $\text{lm}(b_1) = x_1^2 e_{\text{id}_{[1]}}$ or $\text{lm}(b_2) = x_2^2 e_\rho$, we are done, and r is a remainder of f modulo B.

Computation: Division Algorithm

Example (Continued)

- Since $\text{lm}(f) = x_1x_2^2e_\rho = x_1\text{lm}(b_2)$, we could have also defined $r = f - x_1b_2 = -x_1^2x_2e_\rho + x_2e_\pi$.
- Since $\text{lm}(r) = -x_1^2x_2e_\rho$ is not OI-divisible by either $\text{lm}(b_1) = x_1^2e_{\text{id}_{[1]}}$ or $\text{lm}(b_2) = x_2^2e_\rho$, we are done, and r is a remainder of f modulo B.
- As we can see, remainders modulo B need not be unique.

Computation: Division Algorithm

- The division algorithm pairs nicely with Gröbner bases.

Proposition

Let $\mathbf{M}$ *be a submodule of* $\mathbf{F}$ *with Gröbner basis* $B \subseteq \mathbf{M}$*. Then:*

- *if* $f \in \mathbf{M}$*, applying the division algorithm to* f *will result in a remainder of zero modulo* B*.*

Computation: Division Algorithm

- The division algorithm pairs nicely with Gröbner bases.

Proposition

Let $\mathbf{M}$ *be a submodule of* $\mathbf{F}$ *with Gröbner basis* $B \subseteq \mathbf{M}$*. Then:*

- *if* $f \in \mathbf{M}$*, applying the division algorithm to* f *will result in a remainder of zero modulo* B*.*
- B *generates* $\mathbf{M}$*, i.e.* $\mathbf{M} = \langle B \rangle_{\mathbf{F}}$*.*

Computation: OI-Factorization

- With a division algorithm, we can start working toward a criterion for determining when a set forms a Gröbner basis.

Computation: OI-Factorization

- With a division algorithm, we can start working toward a criterion for determining when a set forms a Gröbner basis.
- The following result will be crucial for finiteness arguments.

OI-Factorization Lemma (M-Nagel)

Let $\sigma \in \mathrm{Hom}(k_1, m)$ *and* $\tau \in \mathrm{Hom}(k_2, m)$ *for some* $k_1, k_2, m \in \mathbb{N}$ *with* $k_1, k_2 \leq m$. *Then for* $\ell = |\mathrm{im}(\sigma) \cup \mathrm{im}(\tau)|$, *there are maps* $\widetilde{\sigma} \in \mathrm{Hom}(k_1, \ell)$, $\widetilde{\tau} \in \mathrm{Hom}(k_2, \ell)$ *and* $\rho \in \mathrm{Hom}(\ell, m)$ *such that*

$$\sigma = \rho \circ \widetilde{\sigma} \quad \textit{and} \quad \tau = \rho \circ \widetilde{\tau}.$$

Computation: OI-Factorization

Example

Let $\sigma : [2] \longrightarrow [6]$ and $\tau : [3] \longrightarrow [6]$ be given by

i	1	2
$\sigma(i)$	3	6

and

i	1	2	3
$\tau(i)$	2	5	6

Computation: OI-Factorization

Example

Let $\sigma : [2] \longrightarrow [6]$ and $\tau : [3] \longrightarrow [6]$ be given by

i	1	2
$\sigma(i)$	3	6

and

i	1	2	3
$\tau(i)$	2	5	6

Then $\mathrm{im}(\sigma) \cup \mathrm{im}(\tau) = \{2, 3, 5, 6\}$ so we define $\rho : [4] \longrightarrow [6]$ via

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

Computation: OI-Factorization

Example

Let $\sigma : [2] \longrightarrow [6]$ and $\tau : [3] \longrightarrow [6]$ be given by

i	1	2
$\sigma(i)$	3	6

and

i	1	2	3
$\tau(i)$	2	5	6

Then $\mathrm{im}(\sigma) \cup \mathrm{im}(\tau) = \{2, 3, 5, 6\}$ so we define $\rho : [4] \longrightarrow [6]$ via

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

Finally, we define $\widetilde{\sigma} : [2] \longrightarrow [4]$ and $\widetilde{\tau} : [3] \longrightarrow [4]$ via

i	1	2
$\widetilde{\sigma}(i)$		

and

i	1	2	3
$\widetilde{\tau}(i)$			

Computation: OI-Factorization

Example

Let $\sigma : [2] \longrightarrow [6]$ and $\tau : [3] \longrightarrow [6]$ be given by

i	1	2
$\sigma(i)$	3	6

and

i	1	2	3
$\tau(i)$	2	5	6

Then $\mathrm{im}(\sigma) \cup \mathrm{im}(\tau) = \{2, 3, 5, 6\}$ so we define $\rho : [4] \longrightarrow [6]$ via

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

Finally, we define $\widetilde{\sigma} : [2] \longrightarrow [4]$ and $\widetilde{\tau} : [3] \longrightarrow [4]$ via

i	1	2
$\widetilde{\sigma}(i)$	2	

and

i	1	2	3
$\widetilde{\tau}(i)$			

Computation: OI-Factorization

Example

Let $\sigma : [2] \longrightarrow [6]$ and $\tau : [3] \longrightarrow [6]$ be given by

i	1	2
$\sigma(i)$	3	6

and

i	1	2	3
$\tau(i)$	2	5	6

Then $\mathrm{im}(\sigma) \cup \mathrm{im}(\tau) = \{2, 3, 5, 6\}$ so we define $\rho : [4] \longrightarrow [6]$ via

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

Finally, we define $\widetilde{\sigma} : [2] \longrightarrow [4]$ and $\widetilde{\tau} : [3] \longrightarrow [4]$ via

i	1	2
$\widetilde{\sigma}(i)$	2	4

and

i	1	2	3
$\widetilde{\tau}(i)$			

Computation: OI-Factorization

Example

Let $\sigma : [2] \longrightarrow [6]$ and $\tau : [3] \longrightarrow [6]$ be given by

i	1	2
$\sigma(i)$	3	6

and

i	1	2	3
$\tau(i)$	2	5	6

Then $\mathrm{im}(\sigma) \cup \mathrm{im}(\tau) = \{2, 3, 5, 6\}$ so we define $\rho : [4] \longrightarrow [6]$ via

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

Finally, we define $\widetilde{\sigma} : [2] \longrightarrow [4]$ and $\widetilde{\tau} : [3] \longrightarrow [4]$ via

i	1	2
$\widetilde{\sigma}(i)$	2	4

and

i	1	2	3
$\widetilde{\tau}(i)$	1		

Computation: OI-Factorization

Example

Let $\sigma : [2] \longrightarrow [6]$ and $\tau : [3] \longrightarrow [6]$ be given by

i	1	2
$\sigma(i)$	3	6

and

i	1	2	3
$\tau(i)$	2	5	6

Then $\mathrm{im}(\sigma) \cup \mathrm{im}(\tau) = \{2, 3, 5, 6\}$ so we define $\rho : [4] \longrightarrow [6]$ via

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

Finally, we define $\widetilde{\sigma} : [2] \longrightarrow [4]$ and $\widetilde{\tau} : [3] \longrightarrow [4]$ via

i	1	2
$\widetilde{\sigma}(i)$	2	4

and

i	1	2	3
$\widetilde{\tau}(i)$	1	3	

Computation: OI-Factorization

Example

Let $\sigma : [2] \longrightarrow [6]$ and $\tau : [3] \longrightarrow [6]$ be given by

i	1	2
$\sigma(i)$	3	6

and

i	1	2	3
$\tau(i)$	2	5	6

Then $\text{im}(\sigma) \cup \text{im}(\tau) = \{2, 3, 5, 6\}$ so we define $\rho : [4] \longrightarrow [6]$ via

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

Finally, we define $\widetilde{\sigma} : [2] \longrightarrow [4]$ and $\widetilde{\tau} : [3] \longrightarrow [4]$ via

i	1	2
$\widetilde{\sigma}(i)$	2	4

and

i	1	2	3
$\widetilde{\tau}(i)$	1	3	4

Computation: OI-Factorization

Example

Let $\sigma : [2] \longrightarrow [6]$ and $\tau : [3] \longrightarrow [6]$ be given by

i	1	2
$\sigma(i)$	3	6

and

i	1	2	3
$\tau(i)$	2	5	6

Then $\operatorname{im}(\sigma) \cup \operatorname{im}(\tau) = \{2, 3, 5, 6\}$ so we define $\rho : [4] \longrightarrow [6]$ via

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

Finally, we define $\widetilde{\sigma} : [2] \longrightarrow [4]$ and $\widetilde{\tau} : [3] \longrightarrow [4]$ via

i	1	2
$\widetilde{\sigma}(i)$	2	4

and

i	1	2	3
$\widetilde{\tau}(i)$	1	3	4

One checks that $\sigma = \rho \circ \widetilde{\sigma}$ and $\tau = \rho \circ \widetilde{\tau}$.

Computation: OI-Buchberger's Criterion

Definition

Let $x^a e_{\pi,i}$ and $x^b e_{\rho,j}$ be monomials in $\mathbf{F}$. Define

$$\operatorname{lcm}(x^a e_{\pi,i}, x^b e_{\rho,j}) = \begin{cases} \operatorname{lcm}(x^a, x^b) e_{\pi,i} & \text{if } e_{\pi,i} = e_{\rho,j} \\ 0 & \text{otherwise.} \end{cases}$$

Computation: OI-Buchberger's Criterion

Definition

Let $x^a e_{\pi,i}$ and $x^b e_{\rho,j}$ be monomials in $\mathbf{F}$. Define

$$\operatorname{lcm}(x^a e_{\pi,i}, x^b e_{\rho,j}) = \begin{cases} \operatorname{lcm}(x^a, x^b) e_{\pi,i} & \text{if } e_{\pi,i} = e_{\rho,j} \\ 0 & \text{otherwise.} \end{cases}$$

Definition

Let $f, g \in \mathbf{F}_m$ be nonzero. The *S-polynomial* of f and g is the combination

$$S(f,g) = \frac{\operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))}{\operatorname{lt}(f)} f - \frac{\operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))}{\operatorname{lt}(g)} g \in \mathbf{F}_m.$$

Computation: OI-Buchberger's Criterion

Definition

Let $x^a e_{\pi,i}$ and $x^b e_{\rho,j}$ be monomials in $\mathbf{F}$. Define

$$\operatorname{lcm}(x^a e_{\pi,i}, x^b e_{\rho,j}) = \begin{cases} \operatorname{lcm}(x^a, x^b) e_{\pi,i} & \text{if } e_{\pi,i} = e_{\rho,j} \\ 0 & \text{otherwise.} \end{cases}$$

Definition

Let $f, g \in \mathbf{F}_m$ be nonzero. The *S-polynomial* of f and g is the combination

$$S(f,g) = \frac{\operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))}{\operatorname{lt}(f)} f - \frac{\operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))}{\operatorname{lt}(g)} g \in \mathbf{F}_m.$$

Remark

We have $\operatorname{lm}(S(f,g)) < \operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))$ for any monomial order $<$ on $\mathbf{F}$.

Computation: OI-Buchberger's Criterion

- We say a monomial $\mu \in \mathbf{F}$ *involves the basis element* $e_{\mathrm{id}_{[d_i]},i}$ provided $\mu = x^p e_{\pi,i}$ for some $\pi \in \mathrm{Hom}(d_i, w(\mu))$ and some $x^p \in \mathbf{P}_{w(\mu)}$. In this case we have $\mu = x^p \mathbf{F}(\pi)(e_{\mathrm{id}_{[d_i]},i})$.

Computation: OI-Buchberger's Criterion

- We say a monomial $\mu \in \mathbf{F}$ *involves the basis element* $e_{\mathrm{id}_{[d_i]},i}$ provided $\mu = x^p e_{\pi,i}$ for some $\pi \in \mathrm{Hom}(d_i, w(\mu))$ and some $x^p \in \mathbf{P}_{w(\mu)}$. In this case we have $\mu = x^p \mathbf{F}(\pi)(e_{\mathrm{id}_{[d_i]},i})$.
- Given $B \subseteq \mathbf{F}$, let $\mathscr{L}(B)$ denote the collection of all $(b_1, b_2) \in B \times B$ such that $\mathrm{lm}(b_1)$ and $\mathrm{lm}(b_2)$ involve the same basis element of $\mathbf{F}$.

Computation: OI-Buchberger's Criterion

- We say a monomial $\mu \in \mathbf{F}$ *involves the basis element* $e_{\mathrm{id}_{[d_i]},i}$ provided $\mu = x^p e_{\pi,i}$ for some $\pi \in \mathrm{Hom}(d_i, w(\mu))$ and some $x^p \in \mathbf{P}_{w(\mu)}$. In this case we have $\mu = x^p \mathbf{F}(\pi)(e_{\mathrm{id}_{[d_i]},i})$.
- Given $B \subseteq \mathbf{F}$, let $\mathscr{L}(B)$ denote the collection of all $(b_1, b_2) \in B \times B$ such that $\mathrm{lm}(b_1)$ and $\mathrm{lm}(b_2)$ involve the same basis element of $\mathbf{F}$.

Definition

Let $B \subseteq \mathbf{F}$, and define

$$\Omega(B) = \bigcup_{\substack{(b_1,b_2) \in \mathscr{L}(B) \\ m \in \omega(b_1,b_2)}} \mathrm{Orb}(b_1, m) \times \mathrm{Orb}(b_2, m)$$

where $\omega(b_1, b_2) = \{m \in \mathbb{N} \ : \ \max(w(b_1), w(b_2)) \leq m \leq w(b_1) + w(b_2)\}$.

Remark

If B is finite, then $\Omega(B)$ is also finite.

Computation: OI-Buchberger's Criterion

OI-Buchberger's Criterion (M-Nagel)

Let $\mathbf{M}$ *be a submodule of* $\mathbf{F}$ *generated by* $B \subseteq \mathbf{M}$. *Then* B *forms a Gröbner basis for* $\mathbf{M}$ *if and only if any S-polynomial* $S(f,g)$ *with* $(f,g) \in \Omega(B)$ *has a remainder of zero modulo* B.

Computation: OI-Buchberger's Criterion

OI-Buchberger's Criterion (M-Nagel)

Let $\mathbf{M}$ *be a submodule of* $\mathbf{F}$ *generated by* $B \subseteq \mathbf{M}$*. Then* B *forms a Gröbner basis for* $\mathbf{M}$ *if and only if any S-polynomial* $S(f,g)$ *with* $(f,g) \in \Omega(B)$ *has a remainder of zero modulo* B*.*

Key Idea

- Let $(b_1, b_2) \in \mathscr{L}(B)$ and consider maps $\sigma \in \mathrm{Hom}(w(b_1), m)$ and $\tau \in \mathrm{Hom}(w(b_2), m)$ for some $m \geq \max(w(b_1), w(b_2))$. By the OI-Factorization Lemma, we can write

$$S(\mathbf{F}(\sigma)(b_1),\ \mathbf{F}(\tau)(b_2)) = \mathbf{F}(\rho)(S(\mathbf{F}(\widetilde{\sigma})(b_1),\ \mathbf{F}(\widetilde{\tau})(b_2)))$$

  for some maps $\widetilde{\sigma} \in \mathrm{Hom}(w(b_1), \ell)$, $\widetilde{\tau} \in \mathrm{Hom}(w(b_2), \ell)$ and $\rho \in \mathrm{Hom}(\ell, m)$ where $\ell \leq w(b_1) + w(b_2)$.

Computation: OI-Buchberger's Criterion

OI-Buchberger's Criterion (M-Nagel)

Let $\mathbf{M}$ *be a submodule of* $\mathbf{F}$ *generated by* $B \subseteq \mathbf{M}$*. Then* B *forms a Gröbner basis for* $\mathbf{M}$ *if and only if any S-polynomial* $S(f,g)$ *with* $(f,g) \in \Omega(B)$ *has a remainder of zero modulo* B*.*

Key Idea

- Let $(b_1, b_2) \in \mathscr{L}(B)$ and consider maps $\sigma \in \mathrm{Hom}(w(b_1), m)$ and $\tau \in \mathrm{Hom}(w(b_2), m)$ for some $m \geq \max(w(b_1), w(b_2))$. By the OI-Factorization Lemma, we can write

$$S(\mathbf{F}(\sigma)(b_1),\ \mathbf{F}(\tau)(b_2)) = \mathbf{F}(\rho)(S(\mathbf{F}(\widetilde{\sigma})(b_1),\ \mathbf{F}(\widetilde{\tau})(b_2)))$$

  for some maps $\widetilde{\sigma} \in \mathrm{Hom}(w(b_1), \ell)$, $\widetilde{\tau} \in \mathrm{Hom}(w(b_2), \ell)$ and $\rho \in \mathrm{Hom}(\ell, m)$ where $\ell \leq w(b_1) + w(b_2)$.
- Thus, if B is finite, we can describe all S-polynomials by using only finitely many of them, since $(\mathbf{F}(\widetilde{\sigma})(b_1),\ \mathbf{F}(\widetilde{\tau})(b_2)) \in \Omega(B)$.

Computation: OI-Buchberger's Algorithm

- The OI-Buchberger's Criterion naturally leads to an algorithm for computing Gröbner bases if B is a finite set.

OI-Buchberger's Algorithm (M-Nagel)

Let $\mathbf{M}$ *be a submodule of* $\mathbf{F}$ *finitely generated by a set* $B \subseteq \mathbf{M}$. *Then a finite Gröbner basis (containing* B*) for* $\mathbf{M}$ *can be computed in finite time.*

Computation: OI-Buchberger's Algorithm

- The OI-Buchberger's Criterion naturally leads to an algorithm for computing Gröbner bases if B is a finite set.

OI-Buchberger's Algorithm (M-Nagel)

Let $\mathbf{M}$ *be a submodule of* $\mathbf{F}$ *finitely generated by a set* $B \subseteq \mathbf{M}$. *Then a finite Gröbner basis (containing* B*) for* $\mathbf{M}$ *can be computed in finite time.*

Remark

The algorithm terminates in finite time due to the noetherianity of $\mathbf{F}$ which says that every strictly increasing sequence of submodules of $\mathbf{F}$ must eventually stabilize (see [NR19, 6.17]).

Computation: OI-Buchberger's Algorithm

- We conclude with an example.

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$ and let $\mathbf{M} = \langle x_1^2 e_{\mathrm{id}_{[1]}},\ x_2^2 e_\rho + x_1 x_2 e_\rho \rangle_{\mathbf{F}}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

Computation: OI-Buchberger's Algorithm

- We conclude with an example.

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$ and let $\mathbf{M} = \langle x_1^2 e_{\mathrm{id}_{[1]}},\ x_2^2 e_\rho + x_1 x_2 e_\rho \rangle_{\mathbf{F}}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

- As before, let $b_1 = x_1^2 e_{\mathrm{id}_{[1]}}$ and let $b_2 = x_2^2 e_\rho + x_1 x_2 e_\rho$.

Computation: OI-Buchberger's Algorithm

- We conclude with an example.

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$ and let $\mathbf{M} = \langle x_1^2 e_{\mathrm{id}_{[1]}},\ x_2^2 e_\rho + x_1 x_2 e_\rho \rangle_{\mathbf{F}}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

- As before, let $b_1 = x_1^2 e_{\mathrm{id}_{[1]}}$ and let $b_2 = x_2^2 e_\rho + x_1 x_2 e_\rho$.
- Consider the lex order $<$ on $\mathbf{F}$. Then $\mathrm{lm}(b_1) = x_1^2 e_{\mathrm{id}_{[1]}}$ and $\mathrm{lm}(b_2) = x_2^2 e_\rho$.

Computation: OI-Buchberger's Algorithm

- We conclude with an example.

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$ and let $\mathbf{M} = \langle x_1^2 e_{\mathrm{id}_{[1]}},\ x_2^2 e_\rho + x_1 x_2 e_\rho \rangle_{\mathbf{F}}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

- As before, let $b_1 = x_1^2 e_{\mathrm{id}_{[1]}}$ and let $b_2 = x_2^2 e_\rho + x_1 x_2 e_\rho$.
- Consider the lex order $<$ on $\mathbf{F}$. Then $\mathrm{lm}(b_1) = x_1^2 e_{\mathrm{id}_{[1]}}$ and $\mathrm{lm}(b_2) = x_2^2 e_\rho$.
- We have the S-polynomial $S(\mathbf{F}(\mathrm{id}_{[2]})(b_2), \mathbf{F}(\rho)(b_1)) = x_1 x_2 e_\rho$ which is not OI-divisible by either $\mathrm{lm}(b_1)$ or $\mathrm{lm}(b_2)$. Thus we append $b_3 := x_1 x_2 e_\rho$ to our generating set.

Computation: OI-Buchberger's Algorithm

- We conclude with an example.

Example

Let $c = 1$, let $\mathbf{F} = \mathbf{F}^{\mathrm{OI},1}$ and let $\mathbf{M} = \langle x_1^2 e_{\mathrm{id}_{[1]}},\ x_2^2 e_\rho + x_1 x_2 e_\rho \rangle_{\mathbf{F}}$ where $\rho : [1] \longrightarrow [2]$ is given by $\rho(1) = 2$.

- As before, let $b_1 = x_1^2 e_{\mathrm{id}_{[1]}}$ and let $b_2 = x_2^2 e_\rho + x_1 x_2 e_\rho$.
- Consider the lex order $<$ on $\mathbf{F}$. Then $\mathrm{lm}(b_1) = x_1^2 e_{\mathrm{id}_{[1]}}$ and $\mathrm{lm}(b_2) = x_2^2 e_\rho$.
- We have the S-polynomial $S(\mathbf{F}(\mathrm{id}_{[2]})(b_2), \mathbf{F}(\rho)(b_1)) = x_1 x_2 e_\rho$ which is not OI-divisible by either $\mathrm{lm}(b_1)$ or $\mathrm{lm}(b_2)$. Thus we append $b_3 := x_1 x_2 e_\rho$ to our generating set.
- One checks that $S(f, g)$ has a remainder of zero modulo $\{b_1, b_2, b_3\}$ for all $(f, g) \in \Omega(\{b_1, b_2, b_3\})$. Hence the OI-Buchberger's Criterion says $\{b_1, b_2, b_3\}$ forms a Gröbner basis for $\mathbf{M}$.

References

[NR19] U. Nagel, T. Römer, *FI- and OI-modules with varying coefficients*, J. Algebra **535** (2019), 286-322.

[Nag21] U. Nagel, *Rationality of equivariant Hilbert series and asymptotic properties*, Trans. Amer. Math. Soc. **374** (2021), no. 10, 7313-7357.

[Eis95] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer (1995).