What is Gröbner Bases and SAGBI Bases?

The 27th Clemson Mini-Conference

Mohammed Tesemma
Spelman College
Atlanta GA

Nov. 1, 2012
Polynomials in one variable
Consider a polynomial ring $\mathbb{k}[x]$, $\mathbb{k} = \text{a field}$, in one variable $x$. 
Consider a polynomial ring \( \mathbb{k}[x] \), \( \mathbb{k} = \text{a field} \), in one variable \( x \).

Given \( f(x), g(x) \in \mathbb{k}[x] \), \( \exists! \) \( q(x), r(x) \in \mathbb{k}[x] \)

\[ f(x) = q(x)g(x) + r(x) \text{ where } r = 0 \text{ or } \deg r < \deg g. \]
Consider a polynomial ring $\mathbb{k}[x]$, $\mathbb{k}$ = a field, in one variable $x$.

Given $f(x), g(x) \in \mathbb{k}[x]$  \exists! q(x), r(x) \in \mathbb{k}[x]$  

$$f(x) = q(x)g(x) + r(x) \text{ where } r = 0 \text{ or } \deg r < \deg g.$$  

At the level of ideals:

- Every ideal $I$ of $\mathbb{k}[x]$ is principal, say $I = \langle g \rangle$.
- Ideal membership: $f \in I \iff r = 0$
Multivariable polynomial rings
Let $\mathbb{k}[x] = \mathbb{k}[x_1, \ldots, x_n]$ be the polynomial ring in $n$-variables.
Let $\mathbb{k}[x] = \mathbb{k}[x_1, \ldots, x_n]$ be the polynomial ring in $n$-variables.

**Definition**

A **monomial order**, $\succeq$, is a total order on the monomials of $\mathbb{k}[x]$; 

1. $x^a \succeq x^b \Rightarrow x^a x^c \succeq x^b x^c$, $\forall a, b, c \in \mathbb{N}^n$. 
2. $x^0 = 1$ is the least element under $\succeq$. 

Mohammed Tesemma  Spelman College Atlanta GA

What is Gröbner Bases and SAGBI Bases? The 27th Clemson Interdisciplinary Conference
Let $\mathbb{k}[x] = \mathbb{k}[x_1, \ldots, x_n]$ be the polynomial ring in $n$-variables.

**Definition**

A **monomial order**, $\succeq$, is a total order on the monomials of $\mathbb{k}[x]$;

1. $x^a \succeq x^b \Rightarrow x^a x^c \succeq x^b x^c$, $\forall a, b, c \in \mathbb{N}^n$.

2. $x^0 = 1$ is the least element under $\succeq$.

**Example.** The Lexicographic (dictionary order), $\succeq_{\text{lex}}$
Let \( \mathbb{k}[x] = \mathbb{k}[x_1, \ldots, x_n] \) be the polynomial ring in \( n \)-variables.

**Definition**

A **monomial order**, \( \succeq \), is a total order on the monomials of \( \mathbb{k}[x] \);

1. \( x^a \succeq x^b \Rightarrow x^ax^c \succeq x^bx^c, \quad \forall a, b, c \in \mathbb{N}^n. \)
2. \( x^0 = 1 \) is the least element under \( \succeq \).

**Example.** The Lexicographic (dictionary order), \( \succeq_{lex} \)

\[ x^5y^3z \succeq x^5y^2z^9 \]
Let $\mathbb{k}[x] = \mathbb{k}[x_1, \ldots, x_n]$ be the polynomial ring in $n$-variables.

**Definition**

A **monomial order**, $\succeq$, is a total order on the monomials of $\mathbb{k}[x]$;

1. $x^a \succeq x^b \Rightarrow x^a x^c \succeq x^b x^c$, $\forall a, b, c \in \mathbb{N}^n$.
2. $x^0 = 1$ is the least element under $\succeq$.

**Example.** The Lexicographic (dictionary order), $\succeq_{lex}$

$$x^5y^3z \succeq x^5y^2z^9$$

For $n \geq 2$ there are uncountable monomial orders!
What is Gröbner Bases and SAGBI Bases? The 27th Clemson
Let $f \in \mathbb{k}[x] - \{0\}$, the initial (degree) of $f$ is the leading monomial w.r.t $\succ$. 

Mohammed Tesemma Spelman College Atlanta GA

What is Gröbner Bases and SAGBI Bases? The 27th Clemson
Let $f \in \mathbb{k}[x] - \{0\}$, the initial (degree) of $f$ is the leading monomial w.r.t $\preceq$.

**Division algorithm:** Fix $\preceq_{\text{lex}}$

\[ f = xy^2 - x, \quad g_1 = xy + 1, \quad g_2 = y^2 - 1 \in \mathbb{k}[x, y] \]
Let $f \in \mathbb{k}[x] - \{0\}$, the initial (degree) of $f$ is the leading monomial w.r.t $\succeq$.

**Division algorithm:** Fix $\succeq_{\text{lex}}$

\[
f = xy^2 - x, \quad g_1 = xy + 1, \quad g_2 = y^2 - 1 \in \mathbb{k}[x, y]
\]

\[
f = x \cdot g_2 + 0 \cdot g_1 + 0; \quad \text{here } r = 0.
\]

Alternatively

\[
f = y \cdot g_1 + 0 \cdot g_2 + (-x - y); \quad \text{hence } r = -x - y \neq 0.
\]
Multivariable polynomial rings cont.
Division algorithm fail to check membership of ideal for

\[ I = \langle g_1, g_2 \rangle. \]
Division algorithm fail to check membership of ideal for

\[ I = \langle g_1, g_2 \rangle. \]

Let \( I \) be an ideal of \( k[x] \) given by

\[ I = \langle f_1, \ldots, f_s \rangle \]

Finite generation due to Hilbert’s basis theorem.
Division algorithm fail to check membership of ideal for

\[ I = \langle g_1, g_2 \rangle . \]

Let \( I \) be an ideal of \( \mathbb{k}[x] \) given by

\[ I = \langle f_1, \ldots, f_s \rangle \]

Finite generation due to Hilbert’s basis theorem.

Are there suitable generators where division algorithm works to check ideal membership?
Division algorithm fail to check membership of ideal for

\[ I = \langle g_1, g_2 \rangle. \]

Let \( I \) be an ideal of \( \mathbb{k}[x] \) given by

\[ I = \langle f_1, \ldots, f_s \rangle. \]

Finite generation due to Hilbert’s basis theorem.

Are there suitable generators where division algorithm works to check ideal membership?

Yes. Gröbner bases!
Monomial Ideals

What is Gröbner Bases and SAGBI Bases? The 27th Clemson
Monomial Ideals

Definition

A monomial ideal is an ideal generated by monomials.
Monomial Ideals

Definition

A monomial ideal is an ideal generated by monomials.

Let \( I \subset \mathbb{k}[x] \) and \( \succeq \) a monomial order. The monomial ideal

\[
\text{in}_{\succeq}(I) := \langle \text{in}_{\succeq}(f) : f \in I - \{0\} \rangle
\]

is called the initial ideal of \( I \).
What is Gröbner Bases and SAGBI Bases? The 27th Clemson
Gröbner Bases

**Definition (Gröbner bases)**

A finite set $G \subseteq I$ is called a Gröbner bases for $I$ w.r.t. $\succeq$ if

$$\{in_{\succeq}(g) : g \in G\}$$

generates the initial ideal $in_{\succeq}(I)$. 
Gröbner Bases

Definition (Gröbner bases)

A finite set $G \subseteq I$ is called a Gröbner bases for $I$ w.r.t. $\succeq$ if

$$\{\text{in}_{\succeq}(g) : g \in G\}$$
generates the initial ideal $\text{in}_{\succeq}(I)$.

It follows that:

i. $G$ generates $I$.

ii. Ideal membership can be verified from $G$ via division algorithm.
Buchberger’s Criterion
Let $f, g \in \mathbb{k}[x]$ and let $x^a := \text{Lcm}\{\text{in}_{\geq}(f), \text{in}_{\geq}(g)\}$. The S-Polynomial of $f$ and $g$ is

$$S(f, g) = \frac{x^a}{LT(f)} f - \frac{x^a}{LT(g)} g$$
Buchberger’s Criterion

Let $f, g \in \mathbb{k}[x]$ and let $x^a := \text{Lcm}\{\text{in}_{\geq}(f), \text{in}_{\geq}(g)\}$. The S-Polynomial of $f$ and $g$ is

$$S(f, g) = \frac{x^a}{\text{LT}(f)} f - \frac{x^a}{\text{LT}(g)} g$$

Let $F = \{f_1, \ldots, f_r\}$

$$\overline{f}^F := \text{the remainder on division of } f \text{ by the ordered } r\text{-tuple.}$$
Buchberger’s Criterion

Let \( f, g \in \mathbb{k}[x] \) and let \( x^a := Lcm\{in_{\geq}(f), in_{\geq}(g)\} \).

The S-Polynomial of \( f \) and \( g \) is

\[
S(f, g) = \frac{x^a}{LT(f)} f - \frac{x^a}{LT(g)} g
\]

Let \( F = \{f_1, \ldots, f_r\} \)

\( \overline{f}^F := \) the remainder on division of \( f \) by the ordered \( r \)-tuple.

Theorem (Buchberger’s Criterion)

A set of generators \( G = \{g_1, \ldots, g_r\} \) of ideal \( I \) is a Gröbner bases
for \( I \) iff \( S(g_i, g_j)^G = 0, \forall i < j \).
Buchberger’s Algorithm
Let $I = \langle f_1, \ldots, f_r \rangle$. Construct a Gröbner bases for $I$ w.r.t $\succeq$. 

Theorem (Buchberger Algorithm)
**Theorem (Buchberger Algorithm)**

Let \( I = \langle f_1, \ldots, f_r \rangle \). Construct a Gröbner bases for \( I \) w.r.t \( \succeq \).

**Input:** \( F = (f_1, \ldots, f_r) \)

**Output:** A Gröbner bases \( G = \{g_1, \ldots, g_t\} \) for \( I \) with \( F \subseteq G \)

\[
G := F
\]

**REPEAT**

\[
G' := G
\]

**FOR each pair** \( p, q, p \neq q \) in \( G' \) **DO**

\[
H := S(p, q)^{G'}
\]

**If** \( H \neq \emptyset \) **THEN** \( G = G' \cup H \)

**UNTIL** \( G = G' \)
What is Gröbner Bases and SAGBI Bases? The 27th Clemson
Subalgebra of polynomial rings

Definition

Let $S \subseteq k[x]$. A $k$-subalgebra of $k[x]$ is the set of all polynomials in $S$ with coefficients in $k$; denoted $k[S]$.
Subalgebra of polynomial rings

**Definition**

Let $S \subseteq k[x]$. A **$k$-subalgebra** of $k[x]$ is the set of all polynomials in $S$ with coefficients in $k$; denoted $k[S]$.

1. Unlike ideals not every subalgebra is finitely generated.

\[ k[x, xy, xy^2, xy^3, \ldots] \subseteq k[x, y] \] is not finitely generated.
Subalgebra of polynomial rings

Definition

Let $S \subseteq \mathbb{k}[x]$. A $\mathbb{k}$-subalgebra of $\mathbb{k}[x]$ is the set of all polynomials in $S$ with coefficients in $\mathbb{k}$; denoted $\mathbb{k}[S]$

1. Unlike ideals not every subalgebra is finitely generated.

$$\mathbb{k}[x, xy, xy^2, xy^3, \ldots] \subseteq \mathbb{k}[x, y]$$ is not finitely generated.

2. Membership: How we check if $f \in \mathbb{k}[S]$?
Subduction Algorithm
Subduction Algorithm

Fix a monomial order and consider a subalgebra $R$ of $\mathbb{k}[x]$. The initial algebra of $R$ is:

$$in_{\succeq}(R) = \mathbb{k}[in_{\succeq}(f) : f \in R - \{0\}]$$
Subduction Algorithm

Fix a monomial order and consider a subalgebra $R$ of $\mathbb{k}[x]$. The initial algebra of $R$ is:

$$in_\prec(R) = \mathbb{k}[in_\prec(f) : f \in R - \{0\}]$$

Assume $in_\prec(R)$ is finitely generated say

$$in_\prec(R) = \mathbb{k}[in_\prec(f_1), \ldots, in_\prec(f_s)], \text{ for some } f_i \in R.$$
Subduction Algorithm

Fix a monomial order and consider a subalgebra $R$ of $\mathbb{k}[x]$. The initial algebra of $R$ is:

$$in_{\succeq}(R) = \mathbb{k}[in_{\succeq}(f) : f \in R - \{0\}]$$

Assume $in_{\succeq}(R)$ is finitely generated say

$$in_{\succeq}(R) = \mathbb{k}[in_{\succeq}(f_1), \ldots, in_{\succeq}(f_s)], \quad \text{for some } f_i \in R$$

Theorem

$R$ is generated by $\{f_1, \ldots, f_s\}$.

Proof: Uses what is known as subduction algorithm.
What is Gröbner Bases and SAGBI Bases?

Mohammed Tesemma Spelman College Atlanta GA
**Definition**

The generators \( \{f_1, \ldots, f_s\} \) are called **SAGBI** bases.

SAGBI is acronym for **Subalgebra Analogue to Gröbner Bases for Ideals**.

Characterizing subalgebras of \( \mathbb{k}[x] \) that have finite SAGBI bases: “This is still an important open problem!” Sturmfels - - Gröbner bases and Convex Polytopes
Examples
Example

1. \( \mathbb{k}[x + y, xy, xy^2] \leq \mathbb{k}[x, y] \) have no finite SAGBI bases w.r.t. any monomial order. One can construct \( xy, xy^2, xy^3, \ldots \) from its initial algebra.
Examples

1. \( \mathbb{k}[x + y, xy, xy^2] \leq \mathbb{k}[x, y] \) have no finite SAGBI bases w.r.t. any monomial order. One can construct \( xy, xy^2, xy^3, \ldots \) from its initial algebra.

2. The algebra of symmetric polynomials
\[ \mathbb{k}[x_1 + \ldots + x_n, x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n, \ldots, x_1x_2 \cdots x_n] \leq \mathbb{k}[x_1, \ldots, x_n] \] have a finite SAGBI bases w.r.t any monomial order.
Examples

Example

1. \( \mathbb{k}[x + y, xy, xy^2] \leq \mathbb{k}[x, y] \) have no finite SAGBI bases w.r.t. any monomial order. One can construct \( xy, xy^2, xy^3, \ldots \) from its initial algebra.

2. The algebra of symmetric polynomials
\( \mathbb{k}[x_1 + \ldots + x_n, \ x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n, \ldots, x_1x_2 \cdots x_n] \leq \mathbb{k}[x_1, \ldots, x_n] \) have a finite SAGBI bases w.r.t any monomial order.

3. \( \mathbb{k}[x, xy - y^2, xy^2] \leq \mathbb{k}[x, y] \) have finite SAGBI bases if \( y > x \) but not if \( x > y \).
Univariate Polynomial Ring
Consider

\[ f = x^3 + a_2x^2 + a_1x + a_0, \quad g = x^2 + b_1x + b_0 \in \mathbb{k}[x] \]
Consider
\[ f = x^3 + a_2 x^2 + a_1 x + a_0, \quad g = x^2 + b_1 x + b_0 \in \mathbb{k}[x] \]

Is there \( h \) of degree 1 in \( \mathbb{k}[f, g] \)?
Consider

\[ f = x^3 + a_2 x^2 + a_1 x + a_0, \quad g = x^2 + b_1 x + b_0 \in \mathbb{k}[x] \]

Is there \( h \) of degree 1 in \( \mathbb{k}[f, g] \)?

\[ h_1 = f^2 - g^3 = c_5 x^5 + \ldots \] is a polynomial of degree 5.
Consider

\[ f = x^3 + a_2 x^2 + a_1 x + a_0, \quad g = x^2 + b_1 x + b_0 \in k[x] \]

Is there \( h \) of degree 1 in \( k[f, g] \)?

\[ h_1 = f^2 - g^3 = c_5 x^5 + \ldots \text{ is a pol. of degree 5.} \]

\[ h_2 = h_1 - c_5 fg = d_4 x^4 + \ldots \text{ is a pol. of degree 4.} \]
Consider

\[ f = x^3 + a_2x^2 + a_1x + a_0, \quad g = x^2 + b_1x + b_0 \in \mathbb{k}[x] \]

Is there \( h \) of degree 1 in \( \mathbb{k}[f, g] \)?

\[ h_1 = f^2 - g^3 = c_5x^5 + \ldots \text{ is a pol. of degree 5.} \]

\[ h_2 = h_1 - c_5fg = d_4x^4 + \ldots \text{ is a pol. of degree 4.} \]

Finally

\[ h = h_2 - d_4g^2 - \alpha f - \beta g \quad \text{must be of degree at most 1.} \]
Consider

\[ f = x^3 + a_2x^2 + a_1x + a_0, \quad g = x^2 + b_1x + b_0 \in \mathbb{k}[x] \]

Is there \( h \) of degree 1 in \( \mathbb{k}[f, g] \)?

\[ h_1 = f^2 - g^3 = c_5x^5 + \ldots \text{ is a pol. of degree 5.} \]

\[ h_2 = h_1 - c_5 fg = d_4x^4 + \ldots \text{ is a pol. of degree 4.} \]

Finally

\[ h = h_2 - d_4g^2 - \alpha f - \beta g \quad \text{must be of degree atmost 1.} \]

A famous epimorphism of Abhyanker and Moh. (1973) shows this is not the case!
What is Gröbner Bases and SAGBI Bases? The 27th Clemson Mini-Conference
The reason behind: \( \{ f, g \} \) is a SAGBI bases of \( \mathbb{k}[x] \). i.e.
The reason behind: \( \{f, g\} \) is a SAGBI bases of \( \mathbb{k}[x] \). i.e.

\[
in(\mathbb{k}[f, g]) = \mathbb{k}[\text{in}(f), \text{in}(g)] = \mathbb{k}[x^3, x^2]
\]
The reason behind: \( \{f, g\} \) is a SAGBI bases of \( \mathbb{k}[x] \). i.e.

\[
\text{in}(\mathbb{k}[f, g]) = \mathbb{k}[\text{in}(f), \text{in}(g)] = \mathbb{k}[x^3, x^2]
\]

**Theorem ([Torstensson et al.] J. Symb. Comp. 2005.)**

Let \( f, g \in \mathbb{k}[x] \) be polynomials of degree \( m \) and \( n \) resp., let \( d = \gcd(m, n) \). The following are equivalent

i. \( \{f, g\} \) is a SAGBI bases

ii. \( \exists h \in \mathbb{k}[x] \) of degree \( d \) and polynomials \( F \) and \( G \) such that \( f = F \circ h \) and \( G = g \circ h \).

iii. \( [\mathbb{k}(x) : \mathbb{k}(f, g)] = d \)
What is Gröbner Bases and SAGBI Bases? The 27th Clemson Mini-Conference
Consider two polynomials $f, g \in \mathbb{k}[x] = \mathbb{k}[x_1, \ldots, x_n]$. 
Consider two polynomials $f, g \in \mathbb{k}[x] = \mathbb{k}[x_1, \ldots, x_n]$.

**Problem:** When does $\mathbb{k}[f, g]$ have a finite SAGBI bases?
Consider two polynomials $f, g \in \mathbb{k}[x] = \mathbb{k}[x_1, \ldots, x_n]$.

**Problem:** When does $\mathbb{k}[f, g]$ have a finite SAGBI bases?

**Theorem**

Let $\succeq$ be a monomial order and $\text{in}_\succeq(f) = x^u$, $\text{in}_\succeq(g) = x^v$. Then $\mathbb{k}[f, g]$ have a finite SAGBI bases in the following cases.

1. $u$ and $v$ are linearly independent over $\mathbb{Q}$.
2. $u = \frac{m}{n}v$ for some $m, n \in \mathbb{N}$ and let $h = f^n - g^m$ where $\text{in}_\succeq(h) = x^w$ satisfies $w$ and $u$ are linearly independent.
Consider two polynomials $f, g \in \mathbb{k}[x] = \mathbb{k}[x_1, \ldots, x_n]$. 

**Problem:** When does $\mathbb{k}[f, g]$ have a finite SAGBI bases?

**Theorem**

Let $\succeq$ be a monomial order and $\text{in}_\succeq(f) = x^u$, $\text{in}_\succeq(g) = x^v$. Then $\mathbb{k}[f, g]$ have a finite SAGBI bases in the following cases.

1. $u$ and $v$ are linearly independent over $\mathbb{Q}$.
2. $u = \frac{m}{n}v$ for some $m, n \in \mathbb{N}$ and let $h = f^n - g^m$ where $\text{in}_\succeq(h) = x^w$ satisfies $w$ and $u$ are linearly independent.

The case in 2 above where $w$ and $u$ are linearly dependent is open.
THANK YOU!!