I. Gröbner bases in free associative algebras

Viktor Levandovskyy

Lehrstuhl D für Mathematik, RWTH Aachen

EACA Summer School on Computer Algebra and its Applications

How general are Gröbner bases?

Let K be a field, $X = \{x_1, x_2, \dots\}$ be a finite or countable set.
Moreover, let $K\{X\}$ be the free non-associative algebra (magma) and $K\{\{X\}\}$ be the algebra of non-associative (or tree) power series.
Then there is a Gröbner bases theory over both $K\{X\}$ and $K\{\{X\}\}$!

References

Lothar Gerritzen, "Tree polynomials and non-associative Gröbner bases". Journal of Symbolic Computation, 41 (2006), no. 3-4, 297–316.

Serena Cicaló, Willem de Graaf "Non-associative Gröbner bases, finitely-presented Lie rings and the Engel condition", Proceedings of ISSAC 2007 (and follow-ups).

A historical sketch

A K-bilinear map $V \times V \to V$, $(a, b) \mapsto [a, b]$ is a **Lie bracket**, if

$[b, a] = -[a, b]$
$[[a, b], c] + [[c, a], b] + [[b, c], a] = 0$ (Jacobi identity).

$(V, [,])$ is called a Lie algebra. Any associative algebra can be viewed as a Lie algebra by defining $[a, b] := ab - ba$.

References

A.I. Shirshov "Some algorithmic problem for Lie algebras". Sibirsk. Mat. Zh. 3, (2) 292–296 (**1962**);
English translation in SIGSAM Bull. 33, 3–6 (**1999**)
the idea of *composition* (BB: *S-polynomial*) was present already in A.I. Shirshov "On free Lie rings". Mat. Sbornik 45 (87), 2 (**1958**), 178–218.

Adjusting terminology: **Gröbner-Shirshov bases** for non-associative and non-commutative algebras.

A historical sketch

A K-bilinear map $V \times V \to V$, $(a, b) \mapsto [a, b]$ is a **Lie bracket**, if

$[b, a] = -[a, b]$
$[[a, b], c] + [[c, a], b] + [[b, c], a] = 0$ (Jacobi identity).

$(V, [,])$ is called a Lie algebra. Any associative algebra can be viewed as a Lie algebra by defining $[a, b] := ab - ba$.

References

A.I. Shirshov "Some algorithmic problem for Lie algebras". Sibirsk. Mat. Zh. 3, (2) 292–296 (**1962**);
English translation in SIGSAM Bull. 33, 3–6 (**1999**)
the idea of *composition* (BB: *S-polynomial*) was present already in A.I. Shirshov "On free Lie rings". Mat. Sbornik 45 (87), 2 (**1958**), 178–218.

Adjusting terminology: **Gröbner-Shirshov bases** for non-associative and non-commutative algebras.

A historical sketch

A K-bilinear map $V \times V \to V$, $(a, b) \mapsto [a, b]$ is a **Lie bracket**, if

$[b, a] = -[a, b]$
$[[a, b], c] + [[c, a], b] + [[b, c], a] = 0$ (Jacobi identity).

$(V, [,])$ is called a Lie algebra. Any associative algebra can be viewed as a Lie algebra by defining $[a, b] := ab - ba$.

References

A.I. Shirshov "Some algorithmic problem for Lie algebras". Sibirsk. Mat. Zh. 3, (2) 292–296 (**1962**);
English translation in SIGSAM Bull. 33, 3–6 (**1999**)
the idea of *composition* (BB: *S-polynomial*) was present already in A.I. Shirshov "On free Lie rings". Mat. Sbornik 45 (87), 2 (**1958**), 178–218.

Adjusting terminology: **Gröbner-Shirshov bases** for non-associative and non-commutative algebras.

A historical sketch

A K-bilinear map $V \times V \to V$, $(a, b) \mapsto [a, b]$ is a **Lie bracket**, if

$[b, a] = -[a, b]$
$[[a, b], c] + [[c, a], b] + [[b, c], a] = 0$ (Jacobi identity).

$(V, [,])$ is called a Lie algebra. Any associative algebra can be viewed as a Lie algebra by defining $[a, b] := ab - ba$.

References

A.I. Shirshov "Some algorithmic problem for Lie algebras". Sibirsk. Mat. Zh. 3, (2) 292–296 (**1962**);
English translation in SIGSAM Bull. 33, 3–6 (**1999**)
the idea of *composition* (BB: *S-polynomial*) was present already in A.I. Shirshov "On free Lie rings". Mat. Sbornik 45 (87), 2 (**1958**), 178–218.

Adjusting terminology: **Gröbner-Shirshov bases** for non-associative and non-commutative algebras.

Back to the cosy associativity: taxonomy of structures

Notations: $X := \{x_1, \ldots, x_n\}$ is the finite set of **variables** and K is a field.

Semigroup = associative magma

Monoid = semigroup with the neutral element (␣ or ϵ or 1)

Group = monoid, each element of which is invertible

Ring (with 1) $(R, +, 0, \star, 1)$:

- $(R, +, 0)$ is an abelian group with the neutral element 0
- $(R, \star, 1)$ is a monoid with the neutral element 1
- $\star$ is both left and right distributive over $+$, i.e. $a \star (b + c) = a \star b + a \star c$ and $(b + c) \star a = b \star a + c \star a$.

If R is a commutative ring, then an **associative** R-**algebra** is a ring and an R-module, such that $\forall r \in R \; \forall a, b \in A$ one has

$$r \star (a \star b) = (r \star a) \star b = a \star (r \star b) = (a \star b) \star r.$$

Free structures and some taxonomy

The free monoid on $X = \{x_1, \ldots, x_n\}$:

- denoted by $\langle X \rangle$
- carrier set: all finite words (including the empty word as the neutral element) in the alphabet X
- multiplication: $\star$ is the concatenation $x_2 \star x_1 = x_2 x_1 \neq x_1 x_2 = x_1 \star x_2$.
- divisibility: a partial relation on the set of words by string inclusion.

The free group on $X = \{x_1, \ldots, x_n\}$:

- denoted by $\langle X \rangle$ (arrgh, same as monoid!)
- carrier set: all finite reduced words (including the empty word as the neutral element) in the alphabet $X \cup X'$, where $X' = \{x_1^{-1}, \ldots, x_n^{-1}\}$
- multiplication: $\star$ is the concatenation taking inverses into account: $x_2 \star x_1 = x_2 x_1$ but $x_1 \star x_1^{-1} = x_1^{-1} \star x_1 = 1$.
- divisibility: a partial relation on the set of reduced words by string inclusion.

Free structures and some taxonomy

The free monoid on $X = \{x_1, \dots, x_n\}$:

denoted by $\langle X \rangle$

carrier set: all finite words (including the empty word as the neutral element) in the alphabet X

multiplication: $\star$ is the concatenation $x_2 \star x_1 = x_2 x_1 \neq x_1 x_2 = x_1 \star x_2$.

divisibility: a partial relation on the set of words by string inclusion.

The free group on $X = \{x_1, \dots, x_n\}$:

denoted by $\langle X \rangle$ (arrgh, same as monoid!)

carrier set: all finite reduced words (including the empty word as the neutral element) in the alphabet $X \cup X'$, where $X' = \{x_1^{-1}, \dots, x_n^{-1}\}$

multiplication: $\star$ is the concatenation taking inverses into account: $x_2 \star x_1 = x_2 x_1$ but $x_1 \star x_1^{-1} = x_1^{-1} \star x_1 = 1$.

divisibility: a partial relation on the set of reduced words by string inclusion.

Towards FPA

Over an arbitrary ring R and a monoid M we can create

The monoid algebra

denoted by RM

carrier set: finite sums $\sum r_i m_i$, where $r_i \in R \setminus \{0\}$ and $m_i \in M$

multiplication: $(\sum r_i m_i) \star (\sum r'_j m'_j) := \sum (r_i r'_j)(m_i m'_j)$

$\mathbf{K}\langle\mathbf{X}\rangle$, for X as above and a field K is called the **free associative algebra over** K = the tensor algebra TV of the vector space $V = K \oplus \bigoplus Kx_i$.

A K-algebra A is a finitely presented associative algebra (**FPA**), if $\exists n \in \mathbb{N}_0$ such that A is a homomorphic image of a free associative algebra over K on the set of n variables, i.e. $A = K\langle X\rangle / I$, where $I \subsetneq K\langle X\rangle$ is a **two-sided ideal**.

Free group is a finitely related (and thus not free!) monoid: generators $\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$ and relations $\{x_i y_i = 1, y_i x_i = 1 \mid 1 \leq i \leq n\}$

Graded structures

A ring R is called **($\mathbb{N}_0$-)graded** if there exist additive subgroups $R_i \subseteq R, i \in \mathbb{N}_0$, such that

- $R = \bigoplus_{i \in \mathbb{N}} R_i$
- $\forall k, j \in \mathbb{N}_0 \; R_k \cdot R_j \subseteq R_{k+j}$, that is $\forall r \in R_k, \forall s \in R_j$ one has $rs \in R_{k+j}$.

$p \in R_i$ is called a **homogeneous** (or a **graded**) element of **degree** i.

Properties

$R_0 \subseteq R$ is a subring, R_i are R_0-bimodules.

We are interested in nontrivial gradings, i. e. those for which $R \neq R_0$. In general, a grading can be provided by an additive semigroup, most often $\mathbb{N}_0^n, \mathbb{Z}, \mathbb{Z}^n$.

Graded structures

An ideal $I \subset R$ in a graded ring R is called **graded** if $I = \bigoplus_i I_i$, where $I_i = I \cap R_i$.

Properties

∘ If I is graded, then $\forall p \in I \;\; p = p_1 + \ldots p_k, p_i \in R_i \Rightarrow p_i \in I$.
∘ A graded ideal possesses a generating set, consisting of graded elements.
∘ Any monomial ideal is graded.
∘ For a graded ideal $I \subset R$ in a graded ring R, the factor ring R/I has an induced grading.

Graded modules form a very pleasant subcategory of the category of modules (with morphisms being graded morphisms, i.e. those, which respect the grading)!

Some properties of $K\langle X\rangle$

$K\langle x_1\rangle = K[x_1]$ is commutative, so let $n \geq 2$.

∘ $A := K\langle X\rangle$ is naturally $\mathbb{N}_0$-graded: set $\deg(x_i) = 1$, then $A_0 = K$ and for $i \geq 1$ $A_i = \oplus\{Kw : w \in X, \deg(w) = i\}$.

∘ The number of variables of $K\langle X\rangle$ **does not** lead to the nice notion of rank : for $n \geq 3$ there exist embeddings of $K\langle x_1, \ldots, x_n\rangle$ into $K\langle x_1, x_2\rangle$.

∘ $K\langle X\rangle$ is a domain (there are no zero-divisors).

∘ $K\langle X\rangle$ is neither left nor right Noetherian: there exist infinite strictly ascending chains of ideals; we have to admit infinite generating sets.

Gröbner Bases Q&A

What? Gröbner basis of an ideal $I \subset K\langle X \rangle$ is a generating set for I, possessing many nice properties.

Why? Knowing a Gröbner basis of I, we can answer the following questions about $K\langle X \rangle / I$:

- is $K\langle X \rangle / I = 0$? This happens iff $1 \in I$ iff $1 \in GB(I)$
- is $K\langle X \rangle / I$ finite dimensional algebra? Compute a K-basis of such.
- for $p \in K\langle X \rangle$, is $p \in I$? Ideal membership problem.
- is $K\langle X \rangle / I$ commutative algebra?
- is $K\langle X \rangle / I$ left or right Noetherian? Is it prime or semi-prime?
- what are the values of various ring-theoretic dimensions of $K\langle X \rangle / I$?
- and many other...

How to compute GB? The contents of next lectures and exercises.

Back to the cosy associativity

From now on, all algebras will be considered associative.

A Gröbner bases theory for (free) assoc. algebras builds on top of G. M. Bergman, "The diamond lemma for ring theory", Adv. in Math., 29 (**1978**), 178–218.

However, L. A. Bokut in "Imbeddings into simple associative algebras", Algebra Logika, 15 (**1976**), 117–142 has already specialized Gröbner-Shirshov bases for the associative case.

More systematic approach to Gröbner bases (also for free algebras) was performed by Teo Mora in

"Seven variations on standard bases", **1988**, preprint
"Groebner bases in non-commutative algebras", Proc. ISSAC'88 (**1989**), 150–161

Back to the cosy associativity

From now on, all algebras will be considered associative.

A Gröbner bases theory for (free) assoc. algebras builds on top of
G. M. Bergman, "The diamond lemma for ring theory", Adv. in Math., 29 (**1978**), 178–218.

However, L. A. Bokut in "Imbeddings into simple associative algebras", Algebra Logika, 15 (**1976**), 117–142 has already specialized Gröbner-Shirshov bases for the associative case.

More systematic approach to Gröbner bases (also for free algebras) was performed by Teo Mora in

"Seven variations on standard bases", **1988**, preprint
"Groebner bases in non-commutative algebras", Proc. ISSAC'88 (**1989**), 150–161

Higmans' lemma

Definitions

- A **quasi-ordering** is a binary relation $\preceq$, which is reflexive ($a \preceq a$) and transitive ($a \preceq b,\ b \preceq c \Rightarrow a \preceq c$).
- An ordering is **well-founded**, if every nonempty set has a minimal element.
- A **well-quasi-ordering** is a well-founded quasi-ordering, such that there is no infinite sequence $\{x_i\}$ with $x_i \not\preceq x_j$ for all $i < j$

Higmans' lemma (1952)

The set of finite sequences over a well-quasi-ordered set of labels is itself well-quasi-ordered.

Now, we enter the realm of Gröbner bases.

- $A = K\langle X\rangle$, the free associative algebra over K.
- $M = \langle X\rangle$ is the free monoid (with 1 as the empty word)

A **monomial ordering** $\prec$ on A is a total ordering on M which is compatible with multiplication. Precisely one has:

(i) either $u \prec v$ or $v \prec u$, for any $u, v \in M, u \neq v$;

(ii) if $u \prec v$ then $wu \prec wv$ and $uw \prec vw$, for all $u, v, w \in M$;

Moreover, if every non-empty subset of M has a minimal element wrt $\prec$ (that is, $\prec$ is well-founded), one says that $\prec$ **is a monomial well-ordering**.

Remark

By Higman's lemma, any total ordering on M (even if the number of variables of the polynomial algebra A is infinite), which is compatible with multiplication and such that $1 \prec x_0 \prec x_1 \prec \ldots$ holds, is a monomial well-ordering.

Now, we enter the realm of Gröbner bases.

- $A = K\langle X\rangle$, the free associative algebra over K.
- $M = \langle X\rangle$ is the free monoid (with 1 as the empty word)

A **monomial ordering** $\prec$ on A is a total ordering on M which is compatible with multiplication. Precisely one has:

(i) either $u \prec v$ or $v \prec u$, for any $u, v \in M, u \neq v$;

(ii) if $u \prec v$ then $wu \prec wv$ and $uw \prec vw$, for all $u, v, w \in M$;

Moreover, if every non-empty subset of M has a minimal element wrt $\prec$ (that is, $\prec$ is well-founded), one says that $\prec$ **is a monomial well-ordering**.

Remark

By Higman's lemma, any total ordering on M (even if the number of variables of the polynomial algebra A is infinite), which is compatible with multiplication and such that $1 \prec x_0 \prec x_1 \prec \ldots$ holds, is a monomial well-ordering.

(Monomial) orderings

Let $\langle X \rangle = \langle x_1, \ldots, x_n \rangle$. We always impose a *linear preordering* $x_1 > x_2 > \ldots > x_n > 1$ first.

- For $\mu = x_{j_1} x_{j_2} \cdots x_{j_k}$ and $\nu = x_{l_1} x_{l_2} \cdots x_{l_{\tilde{k}}}$ from $\langle X \rangle$

$$\mu <_{\text{llex}} \nu \quad \Longleftrightarrow \quad \exists 1 \leq i \leq \min\{k, \tilde{k}\} : \ x_{j_w} = x_{l_w} \ \forall w < i \ \wedge \ x_{j_i} < x_{l_i}$$
$$\text{or } \nu = \mu \tilde{\nu} \quad \text{for some } \tilde{\nu} \in \langle X \rangle.$$

This is called the **left lexicographical ordering**.

Analogously one can define the **right lexicographical ordering** rlex.

Houston, we've got a problem!

Neither llex nor rlex are monomial orderings.

Hint: $x_2 x_1 <_{llex} x_1$, but this is a contradiction (why?) to $1 < x_2$.

Monomial degree orderings

- Take μ, ν as before. We define:

$$\mu <_{\text{degllex}} \nu \iff \begin{cases} k < \tilde{k} & \text{, or} \\ k = \tilde{k} \text{ and } \mu <_{\text{llex}} \nu. \end{cases}$$

  This is called the **degree (left) lexicographical ordering**.

- Take $\omega = (\omega_1, \dots, \omega_n) \in \mathbb{R}^n \setminus \{0\}$ and again let $\mu, \nu \in \langle X \rangle$ as before.

$$\mu <_{\omega} \nu \iff \begin{cases} \sum_{i=1}^{k} \omega_{j_i} < \sum_{i=1}^{\tilde{k}} \omega_{l_i} & \text{or} \\ k = \tilde{k} \text{ and } \mu <_{\text{llex}} \nu. \end{cases}$$

  This is called the **weighted degree left lexicographical ordering** with weight vector ω.
  Both `degllex` and ω-`degllex` are monomial orderings.

Notations

- $\mathrm{lm}(f) \in \langle X \rangle$ the leading (greatest) monomial of $f \in K\langle X \rangle \setminus \{0\}$
- $\mathrm{lc}(f) \in K \setminus \{0\}$ the leading coefficient of $f \in K\langle X \rangle \setminus \{0\}$
- $\mathrm{lm}(G) = \{\mathrm{lm}(g) \,|\, g \in G \setminus \{0\}\}$ with $\emptyset \neq G \subset K\langle X \rangle$
- $\mathrm{LM}(G)$ the two-sided ideal generated by $\mathrm{lm}(G)$

Definition

Let I be a left (right, two-sided) ideal of $K\langle X \rangle$ and $G \subset I$.

If $\mathrm{LM}(G) = \mathrm{LM}(I)$ as a left (right, two-sided) monoid ideal, then G is called a **left (right, two-sided) Gröbner basis** of I.

In other words, for all $f \in I \setminus \{0\}$ $\exists g \in G \setminus \{0\}$ and

Left GB: $\exists w_L \in \langle X \rangle \ : \ \mathrm{lm}(f) = w_L \cdot \mathrm{lm}(g)$.

Two-sided GB: $\exists w_L, w_R \in \langle X \rangle \ : \ \mathrm{lm}(f) = w_L \cdot \mathrm{lm}(g) \cdot w_R$.

Notations

- $\mathrm{lm}(f) \in \langle X \rangle$ the leading (greatest) monomial of $f \in K\langle X \rangle \setminus \{0\}$
- $\mathrm{lc}(f) \in K \setminus \{0\}$ the leading coefficient of $f \in K\langle X \rangle \setminus \{0\}$
- $\mathrm{lm}(G) = \{\mathrm{lm}(g) \,|\, g \in G \setminus \{0\}\}$ with $\emptyset \neq G \subset K\langle X \rangle$
- $\mathrm{LM}(G)$ the two-sided ideal generated by $\mathrm{lm}(G)$

Definition

Let I be a left (right, two-sided) ideal of $K\langle X \rangle$ and $G \subset I$.

If $\mathrm{LM}(G) = \mathrm{LM}(I)$ as a left (right, two-sided) monoid ideal, then G is called a **left (right, two-sided) Gröbner basis** of I.

In other words, for all $f \in I \setminus \{0\}$ $\exists g \in G \setminus \{0\}$ and

Left GB: $\exists w_L \in \langle X \rangle \; : \; \mathrm{lm}(f) = w_L \cdot \mathrm{lm}(g)$.

Two-sided GB: $\exists w_L, w_R \in \langle X \rangle \; : \; \mathrm{lm}(f) = w_L \cdot \mathrm{lm}(g) \cdot w_R$.

Gröbner representation

Definition

Let $G \subset K\langle X\rangle, f \in K\langle X\rangle$. We say that f has a **two-sided Gröbner representation** with respect to G if $f = 0$ or there is a finite index set I, $\lambda_i, \rho_i \in K\langle X\rangle, g_i \in G$ such that

$$f = \sum_{i \in I} \lambda_i g_i \rho_i$$

with either $\lambda_i g_i \rho_i = 0$ or $\mathrm{lm}(f) \succeq \mathrm{lm}(\lambda_i)\mathrm{lm}(g_i)\mathrm{lm}(\rho_i)$ holds.

Lemma

Let $\prec$ be a well ordering. Then G is a Gröbner basis (of $\langle G\rangle$) if and only if every $f \in \langle G\rangle \setminus \{0\}$ has a Gröbner representation.

Intuition: given an ordering and a generating set G of an ideal, we want to produce new polynomials, which do not possess a Gröbner representation with respect to G, and enlarge G by those.

Divisibility and overlaps

Let $u, w \in \langle X \rangle$ be two monomials.

- We say that u **divides** w (or w **is divisible by** u), if there exist $p, q \in \langle X \rangle$ such that $\mathbf{w} = p \cdot \mathbf{u} \cdot q$.
- If $w = pu$, then w **is divisible by** u **from the left**.
- The set G is called **minimal**, if $\forall g_1, g_2 \in G$, $\mathrm{lm}(g_1)$ does not divide $\mathrm{lm}(g_2)$ and vice versa.

Two monomials $u, w \in \langle X \rangle$ have an **overlap** at a monomial o, if $w = ow'$ and $u = u'o$. We denote the overlapping by $u' \cdot o \cdot w'$. If $o = 1$, the overlap is trivial.

Exercise: for a fixed $u, w \in \langle X \rangle$ there are finitely many overlaps (u, w, o_i).
Observation: Working with left ideals, the only divisibility from the left can be achieved by proper submonomials.

Normal form

Let $\mathcal{G}$ be the set of all finite and ordered subsets of $K\langle X\rangle$.
A map $\mathrm{NF} : K\langle X\rangle \times \mathcal{G} \to K\langle X\rangle$, $(f, G) \mapsto \mathrm{NF}(f|G)$ is called a **(two-sided) normal form** on $K\langle X\rangle$ if

(i) $\mathrm{NF}(0 \mid G) = 0$,

(ii) $\mathrm{NF}(f|G) \neq 0 \;\Rightarrow\; \mathrm{lm}(\mathrm{NF}(f|G)) \notin LM(G)$, and

(iii) $f - \mathrm{NF}(f|G) \in \langle G\rangle$, for all $f \in K\langle X\rangle$ and $G \in \mathcal{G}$.

Let $f, g \in K\langle X\rangle$. Suppose that there are $p, q \in \langle X\rangle$ such that

- $\mathrm{lm}(f)\, q = p\, \mathrm{lm}(g)$,
- $\mathrm{lm}(f)$ does not divide p and $\mathrm{lm}(g)$ does not divide q.

Then the **overlap polynomial (relation)** of f, g by p, q is defined as

$$o(f, g, p, q) = \frac{1}{\mathrm{lc}(f)} fq - \frac{1}{\mathrm{lc}(g)} pg.$$

Division algorithm and Normal form

Algorithm NF

Input: $f \in K\langle x_1, \ldots, x_n \rangle$, $G \in \mathcal{G}$;
Output: h, a normal form of f with respect to G.

$h := f$;
while ($(h \neq 0)$ **and** $(G_h = \{g \in G : \mathrm{lm}(g) \text{ divides } \mathrm{lm}(h)\} \neq \emptyset)$) do
choose **any** $g \in G_h$;
compute $w_L, w_R \in \langle X \rangle$ such that $\mathrm{lm}(h) = w_L \cdot \mathrm{lm}(g) \cdot w_R$;
$h := h - \frac{lc(h)}{lc(g)} \cdot w_L \cdot g \cdot w_R$;
return h.

Lemma

NF(h, G) *always terminates. (Key: monomial ordering!)*

A useful isomorphism and K-basis

Lemma

Let $\prec$ be a well-ordering on $K\langle X\rangle$ and $G \subset K\langle X\rangle$ a Gröbner basis of $I = \langle G\rangle$. Then there is the following isomorphism of K-vector spaces

$$K\langle X\rangle \cong K\langle X\rangle/\mathrm{LM}(I) \oplus I, \quad f \mapsto (\mathrm{NF}(f,G),\ f - \mathrm{NF}(f,G)).$$

Since G is a GB of I, $\mathrm{LM}(I) = \mathrm{LM}(G)$. Note, that $K\langle X\rangle/\mathrm{LM}(I)$ is a monomial algebra.

Corollary

- $K\langle X\rangle/\mathrm{LM}(I) \cong K\langle X\rangle/I$ as K-vector spaces
- $\{w \in \langle X\rangle : w \notin \mathrm{LM}(I)\}$ is the canonical (with respect to $\prec$) monomial K-basis of $K\langle X\rangle/I$.

Generalized Buchberger's Criterion

Theorem

Let $\prec$ be a well-ordering on $K\langle X\rangle$ and $G \subset K\langle X\rangle$.
Then the following conditions are equivalent:

1. *G is a (two-sided) Gröbner basis of $\langle G\rangle$*
2. *$\forall g_1, g_2 \in G$, for every overlap polynomial holds*
$$\mathrm{NF}(\ o(g_1, g_2, p, q)\ \mid\ G) = 0.$$
3. *$\forall g_1, g_2 \in G$, every overlap polynomial $o(g_1, g_2, p, q)$ has a Gröbner representation with respect to G.*

Note: infinite Gröbner bases exist (even monomial ones).

Procedure GroebnerBasis

Input: $G \in \mathcal{G}$.
Output: H, a (two-sided) Gröbner basis of $\langle G \rangle$.

$H := G \setminus \{0\}$;
$P := \{(f, g) \mid f, g \in H\}$;
while $P \neq \emptyset$ do
  choose $(f, g) \in P$;
  $P := P \setminus \{(f, g)\}$;
  $O := \{o(f, g, p, q)\}$; (the set of all overlap polynomials between f, g)
  for $o \in O$ do
    $h :=$ NF(o, H);
    if $h \neq 0$ then
      $H := H \cup \{h\}$;
      $P := P \cup \{(f, h) \mid f \in H\}$; (note: (h, h) are added as well)
  end if; end for; end while;
return H.

Word problem and ideal membership

Lemma

Let $<$ be a monomial ordering on $K\langle X\rangle$ and G a Gröbner basis of I wrt $<$. Then $f \in I \Leftrightarrow \mathrm{NF}(f, G) = 0$.

Applications

triviality: $K\langle X\rangle/I = 0 \Leftrightarrow 1 \in I \Leftrightarrow 1 \in GB(I)$

commutativity: $K\langle X\rangle/I$ is commutative $\Leftrightarrow \{[x_j, x_i]\} \subseteq I$

algebraicity: $p \in K\langle X\rangle/I$ is algebraic $\Leftrightarrow \exists k \geq 1, c_i \in K : \sum_i^k c_i p^i \in I$

Houston, we've got a problem!

We can check the above properties and many more, if a Gröbner basis of I wrt $<$ is finite.

Trying various orderings heuristically might sometimes help.

But there are plenty of ideals, which do not have any finite Gröbner basis!

Word problem and ideal membership

Lemma

Let $<$ be a monomial ordering on $K\langle X\rangle$ and G a Gröbner basis of I wrt $<$. Then $f \in I \Leftrightarrow \mathrm{NF}(f, G) = 0$.

Applications

triviality: $K\langle X\rangle/I = 0 \Leftrightarrow 1 \in I \Leftrightarrow 1 \in GB(I)$

commutativity: $K\langle X\rangle/I$ is commutative $\Leftrightarrow \{[x_j, x_i]\} \subseteq I$

algebraicity: $p \in K\langle X\rangle/I$ is algebraic $\Leftrightarrow \exists k \geq 1, c_i \in K : \sum_i^k c_i p^i \in I$

Houston, we've got a problem!

We can check the above properties and many more, if a Gröbner basis of I wrt $<$ is finite.

Trying various orderings heuristically might sometimes help.

But there are plenty of ideals, which do not have any finite Gröbner basis!

Finiteness of Gröbner bases

Lemma (T. Mora)

If $\dim_K(K\langle X\rangle/I) < \infty$, *then every minimal Gröbner basis of* I *is finite.*

Proof.

Having a finite K-basis B (wlog monomial) of $K\langle X\rangle/I$ implies, that the set of monomials "above the staircase"

$$\{w \in \mathrm{LM}(I) \mid \exists i \in [1,n]\ \exists b \in B : w = bx_i \text{ or } w = x_i b\}$$

is finite. The same set clearly generates $\mathrm{LM}(I)$, and hence for any Gröbner basis G of I the monoid ideal $\mathrm{LM}(G) = \mathrm{LM}(I)$ is finitely generated, so a minimal G is finite. □

Fine, but what can we do with infinite dimensional algebras?

Finiteness of Gröbner bases II

Proposition

Let $I \subset K\langle X \rangle$ be a **graded** *two-sided ideal and $d > 0$ an integer. If I has a finite number of graded generators F of degree $\leq d$ then the algorithm* NCGBasis *computes in a finite number of steps all elements of degree $\leq d$ of a graded Gröbner basis of I.*

Proof.

Exercise: (a) any overlap polynomial between the elements from F is homogeneous of higher degree,
(b) the normal form of a homogeneous g wrt F is either zero or homogeneous of same degree as g.
This means, that as soon as we process all pairs of polynomials of degree $\leq d$, reduction on overlap polynomials of degree $\geq d+1$ does not have impact on the degrees $\leq d$.
Yet another explanation: since F is a set of graded polynomials, $I = \langle F \rangle$ is a graded ideal $I = \bigoplus I_i$. □

Finiteness of Gröbner bases III and the word problem

The word problem for finitely presented **graded** associative algebras is solvable! If $f \in K\langle X \rangle$ is homogeneous of degree d, compute a Gröbner basis of $I_{\leq d}$ (which is finite) and $NF(f, I_{\leq d})$.

If an ideal is not graded, then the word problem is **unsolvable in general**. The truncation of a non-graded ideal up to a given degree is not well-defined, since reduction on overlap polynomials of degree $\geq d+1$ might have impact on the degrees $\leq d$.

Models of computation

- we always work up to a fixed degree bound d
- homogeneous input allows to use **truncated** Gröbner basis up to degree d, where $\forall k \in \mathbb{N}\ G_d \subseteq G_{d+k}$ holds (adaptive)
- inhomogeneous input: either compute a Gröbner basis up to degree d (approximation) or homogenize the input and proceed as before
- problems: Gröbner basis of a homogenized set is rather infinite, ...

Finiteness of Gröbner bases III and the word problem

The word problem for finitely presented **graded** associative algebras is solvable! If $f \in K\langle X \rangle$ is homogeneous of degree d, compute a Gröbner basis of $I_{\leq d}$ (which is finite) and $NF(f, I_{\leq d})$.

If an ideal is not graded, then the word problem is **unsolvable in general**. The truncation of a non-graded ideal up to a given degree is not well-defined, since reduction on overlap polynomials of degree $\geq d+1$ might have impact on the degrees $\leq d$.

Models of computation

- we always work up to a fixed degree bound d
- homogeneous input allows to use **truncated** Gröbner basis up to degree d, where $\forall k \in \mathbb{N}\ G_d \subseteq G_{d+k}$ holds (adaptive)
- inhomogeneous input: either compute a Gröbner basis up to degree d (approximation) or homogenize the input and proceed as before
- problems: Gröbner basis of a homogenized set is rather infinite, ...

Gröbner basis computation in $K\langle X\rangle$: Example

Let $X=\{x,y\}$. Consider $f_1=x^3-y^3=xxx-yyy, f_2=xyx-yxy$ and $I=\langle f_1,f_2\rangle\subset K\langle X\rangle$ with respect to the degree left lexicographical ordering. We compute truncated Gröbner basis up to degree $d=5$.
Let $G=\{f_1,f_2\}$. $(\mathbf{f_1},\mathbf{f_1}):\ \ \mathrm{lm}(f_1)=xxx$, so there are two self-overlaps

$$o_1:=o_{1,1}=f_1x-xf_1=xy^3-y^3x,\ o_{1,2}=f_1x^2-x^2f_1=x^2y^3-y^3x^2.$$

Moreover, $o_{1,2}-xo_{1,1}=xy^3x-y^3x^2=o_{1,1}x$, so $o_{1,2}$ reduces to 0. Hence $G:=G\cup\{o_1\}=\{\mathbf{f_1},\mathbf{f_2},\mathbf{o_1}\}$.
$(\mathbf{f_2},\mathbf{f_2}):\ \ \mathrm{lm}(f_2)=xyx$, there are two self-overlaps. Symmetry implies that both of them originate from the overlap $xy\cdot x\cdot yx$ of $\mathrm{lm}(f_2)$. Then

$$o_2=f_2yx-xyf_2=xyyxy-yxyyx. \text{ So } G:=G\cup\{o_2\}=\{\mathbf{f_1},\mathbf{f_2},\mathbf{o_1},\mathbf{o_2}\}.$$

Gröbner basis in $K\langle X\rangle$: Example continued

$(\mathbf{f_1}, \mathbf{f_2})$: $\operatorname{lm}(f_1)$ and $\operatorname{lm}(f_2)$ have two overlaps $xx \cdot x \cdot yx$ and $xy \cdot x \cdot xx$, hence

$$o_{3,1} = f_1 yx - xxf_2 = xxyxy - y^4 x \text{ and } o_{3,2} = f_2 xx - xyf_1 = xy^4 - yxyxx.$$

Performing reductions, we see that $o_{3,1} - xf_2 y - f_2 yy - yo_1 = 0$ and $o_{32} - o_1 y + yf_2 x + yyf_2 = yyyxy - yyyxy = 0$.
$(\mathbf{f_1}, \mathbf{o_1})$ has overlap $xx \cdot x \cdot yyy$, $(\mathbf{f_2}, \mathbf{o_1})$ has overlap $xy \cdot x \cdot yyy$,
$(\mathbf{f_1}, \mathbf{o_2})$ has overlap $xx \cdot x \cdot yyxy$, $(\mathbf{o_1}, \mathbf{o_2})$ has overlap $xyy \cdot xy \cdot yy$,
$\mathbf{o_2}$ has a self-overlap $xyy \cdot xy \cdot yxy$ and $(\mathbf{f_2}, \mathbf{o_2})$ has two overlaps $xy \cdot x \cdot yyxy$ and $xyy \cdot xy \cdot x$. Since all these elements are of degree ≥ 6 and we are in the graded case, we conclude that

$G = \{f_1, f_2, o_1, o_2\}$ is truncated Gröbner basis up to degree 5.