Gröbner bases over free associative algebras: Algorithmics, Implementation, and Applications I

Viktor Levandovskyy and Team

Universität Kassel, Germany and American University Kyiv, Ukraine

Dec 6, 2023, TU Berlin

UNIKASSEL VERSITÄT

American University Kyiv

Taxonomy of associative 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 ($\sqcup$ 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.

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 nor weak 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?
- $\star$ is $K\langle X\rangle/I$ left or right or weak Noetherian? Is it prime or semi-prime?
- $\star$ what are the values of various ring-theoretic dimensions of $K\langle X\rangle/I$?
- and many other... ($\star$ means that the answer is not always complete)

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

The giants' shoulders

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

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 $x_n \succ \ldots x_1 \succ 1$ *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 $\nu = x_{\ell_1} x_{\ell_2} \cdots x_{\ell_{\tilde{k}}}$ from $\langle X \rangle$

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

  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 $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{R}^n_+$ and again let $\mu, \nu \in \langle X \rangle$ as before.

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

  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 left (right, two-sided) monoid ideals,
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

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

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

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 $\langle G \rangle$.

$H := G \setminus \{0\}$;
$P := \{(f, g) \mid f, g \in H\}$; (note: (f, g) and (g, f) are different pairs!)
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
    $h := \mathrm{NF}(o, H)$;
    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 $\prec$ be a monomial ordering on $K\langle X\rangle$ and G a Gröbner basis of I wrt $\prec$. 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 $\prec$ 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 "below 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 of overlap polynomials of degree $\geq d+1$ might add new elements of degree $\leq d$.

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

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

Moreover, $o_{1,2} - x o_{1,1} = xy^3 x - y^3 x^2 = o_{1,1} x$, 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

$o_2 = f_2 yx - xyf_2 = xyyxy - yxyyx$. 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

$(\mathbf{f_1}, \mathbf{f_2})$: $\mathrm{lm}(f_1)$ and $\mathrm{lm}(f_2)$ 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.

Gröbner bases over free associative algebras: Algorithmics, Implementation, and Applications II

Viktor Levandovskyy and Team

Universität Kassel, Germany and American University Kyiv, Ukraine

Dec 6, 2023, TU Berlin

UNIKASSEL VERSITÄT

Letterplace Gröbner Bases Q&A

What? Letterplace Gröbner basis is a special generating set for an ideal in infinitely generated **commutative** ring $K[X|P]$. It is tightly connected to the Gröbner basis of an ideal $I \subset K\langle X\rangle$.

Why? Among other, the Letterplace technique works over a commutative polynomial ring, hence know-how's of last 50 years in commutative computer algebra can be reused. For this reason, we have an implementation in SINGULAR calles LETTERPLACE.

What is behind LPGB? The contents of next minutes before the reception.

Who is behind? V. L., Tobias Metzlaff, Leonard Schmitz, Hannes Schönemann, Karim Abou Zeid.

- We present the theory and algorithmics which led to the implementation in the subsystem LETTERPLACE of SINGULAR 4-1-3, for computations with modules over finitely presented associative non-commutative algebras (including free algebras) over effective fields and some rings including $\mathbb{Z}$.
- We offer very rich functionality at decent speed.
- In particular, we cover not only Gröbner trinity (including syzygies) but also many of Gröbner basics, covering procedures, relevant to old and new applications.
- One can download the newest SINGULAR release 4-1-3 containing LETTERPLACE at

  `https://www.singular.uni-kl.de`

What is and what does LETTERPLACE

The name *Letterplace* comes from the **Letterplace correspondence** between the ideals of the free associative algebra $K\langle X\rangle$ and the so-called *Letterplace ideals* of the infinitely gen. commutative algebra $K[X \mid \mathbb{N}] = K[\{x_i(j) : x_i \in X, j \in \mathbb{N}]$.

- By means of the correspondence, *Letterplace Gröbner bases* from $K[X \mid \mathbb{N}]$ are transferred back to Gröbner bases in $K\langle X\rangle$.
- This theory together with algorithms was introduced by R. La Scala and V. Levandovskyy (JSC papers 2009, 2013 etc).

In the modern implementation in SINGULAR:LETTERPLACE the user operates with objects in free algebras.

But: internally all computations happen in the Letterplace ring.

The very theory allows to use commutative data structures and reuse via reinterpretation some of the functionality.

Fundamental Functionality

Below, F is a set of generators and G is a two-sided Gröbner basis for an ideal or a submodule over $K\langle X\rangle$ or even $\mathbb{Z}\langle X\rangle$.

`twostd(`F`)`	a two-sided Gröbner basis of F
`reduce(`p, G`)`	a normal form of a poly/vector p wrt G
`syz(`F`)`	a generating set of the syzygy bimodule of F
`modulo(`M, F`)`	kernel of a bimodule homomorphism, defined by M into a bimodule, presented by F
`lift(`M, N`)`	computation of a bi-transformation matrix between a module M and its submodule N
`liftstd(`F, T`[,`S`])`	two-sided Gröbner basis, bi-transformation matrix T and (optionally) a generating set S for the syzygy bimodule of F
`rightstd(`F`)`	a right Gröbner basis of F *especially useful over quotient rings (*`qring`*)*

Advanced Functionality: libraries in SINGULAR language

`freegb.lib`	main initialization library (also contains legacy, conversion and technical routines)
`fpaprops.lib`	various properties such as GK dimension and Noetherianity of fin. pres. algebras
`fpadim.lib`	vector space dimensions and bases of fin.-dim. algebras, and finite Hilbert series
`fpalgebras.lib`	predefined relations of many algebras including group algebras of fin. gen. groups
`ncHilb.lib` (Tiwari, LaScala)	computations of multi-graded Hilbert series of not necessary fin. pres. algebras (automata)

Bimodules and One-sided Modules

For treating not only ideals, but also bimodules, we have to work with a *free bimodule of finite rank*.

For a finitely presented algebra R, let ε_i denote the i-th canonical generator of a free bimodule, commuting *only* with the constants from the ground field/ring.

Then the free bimodule of rank $r \in \mathbb{N}$ is $\mathcal{F}_r(A) = \bigoplus_{i=1}^{r} A\varepsilon_i A$.

Realization of objects

In SINGULAR, the canonical (commuting with everything) i-th generator of a free module e_i is denoted by `gen(i)`.
We introduce `ncgen(i)` to be used as `ncgen(i)*gen(i)`.

Operations with one-sided ideals/modules over $K\langle X\rangle$: easy;
over fin. pres. algebra $A = K\langle X\rangle/I$ and $\mathcal{F}_r(A)$: **involved** !
We already provide **right Gröbner bases** for the above.

Gröbner Technology = Gröbner Trinity + Gröbner Basics

Gröbner Trinity consists of three components

1. STD/GB Gröbner basis $\mathcal{G}$ of a module M
2. SYZ Gröbner basis of the syzygy module of M
3. LIFT the transformation matrix between two bases $\mathcal{G}$ and M

The function LIFTSTD computes all the trinity data at once.

Gröbner Trinity should be formulated separately for one-sided (left and right) and for two-sided modules (bimodules).

Therefore we have `twostd` and `rightstd` functions.

Gröbner basics (as coined by Buchberger, Sturmfels et al.)

... are the most important and fundamental applications of Gröbner Bases.

Universal Gröbner Basics

- Ideal (resp. module) membership problem (`reduce, NF`)
- Intersection of ideals resp. submodules
- Quotient and saturation of ideals
- Kernel of a module homomorphism (`modulo`)
- Intersection with subrings (aka elimination of variables)
- Kernel of a ring homomorphism and algebraic dependence between polynomials
- Hilbert series of modules (`ncHilb.lib, fpadim.lib`)

We offer these and other functionality incl. various dimensions with our latest release, both over effective fields and over $\mathbb{Z}$ as coeffs.

Models of Computation

Problem: $R\langle X\rangle$ is not Noetherian, even if a ring R is a field, thus a generating set and a Gröbner basis need not be finite.

Solution: 1) Formulate procedures in such a way, that in case when a Gröbner basis of a module with respect to a given monomial ordering is finite, the procedure computes it and terminates (Mora, Pritchard).

2) Compute up to a specified **length bound** (generalizes a **degree bound**). In the situation, when a module is $\mathbb{N}$-graded, computing wrt an ordering, compatible with the grading yields a **truncated** Gröbner basis, which is a part of the complete one.
In particular, the word problem in this case is decidable.

3) Bad news: if a module cannot be graded by $\mathbb{N}$ or $\mathbb{N}^n$, and no finite Gröbner basis exists, we know very little on the module. In particular, in this situation the word problem is indecidable.

Monomial Orderings

One advantage of the *Letterplace Correspondence* is the formulation of the theory for $K\langle X\rangle$ and $\mathbb{Z}\langle X\rangle$ in terms of commutative polynomial data structures.

In the free case there's no analogon to Robbiano's Lemma and there's no classification of monomial orderings.

We provide the following monomial orderings

`dp`	degree right lexicographical ordering
`Dp`	degree left lexicographical ordering
`Wp(w)`	`w`–weighted degree left lexicographical ordering
`lp/rp`	left/right total elimination ordering
`(a(v),<)`	extra `v`–weight ordering extension of `<`

where $w = (w_1, \ldots, w_n), w_i \in \mathbb{N}_+$ and $v = (v_1, \ldots, v_n), v_i \in \mathbb{N}_0$ are weight vectors for the ordered list of variables $x_1, \ldots, x_n$.

Note: `lp` and `rp` and iterated `(a(V1), a(V2),..,a(VN),<)` for certain vectors V_i are **block elimination** orderings.

Modules, Grading and Length-incompatible orderings

For submodules of free bimodules we offer constructions of

both increasing and decreasing
POT (position-over-term) and *TOP* (term-over-position)
module monomial orderings, using the monomial orderings as above for ordering the elements of the algebra.

Grading is effective with Gröbner computations, when

the current monomial ordering is compatible with the $\mathbb{N}^n$-grading.

A price to pay for supporting length-incompatible orderings:

stop of a Gröbner-based computation with the message like

```
? degree bound of Letterplace ring is 10char‘
but at least 11 is needed for this multiplication
```

It is not a bug; we do not (yet) see the possibility to automate this.

Example

In $D_1(\mathbb{Q}) = \mathbb{Q}\langle x, \partial \mid \partial x = x\partial + 1\rangle$, consider the subalgebra S, generated by $\{x\partial^2, x^2\partial\}$. S is even $\mathbb{Z}$-graded as D_1 itself.

Questions: (1) does the Euler derivation $x\partial$ belong to S?

(2) What is the kernel of the homo of $\mathbb{Q}$-algebras

$$\mathbb{Q}\langle a, b\rangle \to \mathbb{Q}\langle x, \partial\rangle / \langle \partial x - x\partial - 1\rangle,\ a \mapsto x\partial^2,\ b \mapsto x^2\partial,$$

i.e. find a *presentation* of S.

Questions like these require **computations in the free algebra**.

Answers

Use a for $x\partial^2$, b for $x^2\partial$ and c for $x\partial$. Then $c \in S$ since

(1) $c = -\frac{1}{40}\left(6(ab)^2 - 21ba^2b + 24(ba)^2 - 9b^2a^2 - 32ab - 76ba\right)$.

(2) $S \cong \mathbb{Q}\langle a, b\rangle / J$, where J is generated by long and complicated

$$ab^3 - 3bab^2 + 3b^2ab - b^3a - 6b^2, \ldots,$$

$$9a^2bab - 108ba^2ba + 171baba^2 - 72b^2a^3 + 34a^2b - 800aba - \ldots$$

Since $\{a, b, c\}$ generate the same algebra as $\{a, b\}$ by (1), we have

$$S \cong \mathbb{Q}\langle a, b, c\rangle / \langle cb - bc - b,\ ca - ac + a,\ ba - ab + 3c^2 - c,\ c^3 - ab + c^2\rangle.$$

The Gröbner basis property of the latter ideal of relations imply, that we are dealing with a GR-algebra incarnation of S:

$$\mathbb{Q}\langle a, b, c \mid ba = ab - 3c^2 + c,\ cb = bc + b,\ ca = ac - a\rangle / \langle c^3 - ab + c^2\rangle.$$

Thank you for your attention!

letterplace

OSCAR

SYMBOLIC TOOLS

New Developments regarding the GK Dimension

One way to compute the GK dimension of $K\langle X\rangle/I$

Given the Ufnarovski graph of I, one has to count the maximum number of distinct cycles occurring in a single route.

But if there are two distinct cycles with a common vertex in the graph, one is done immediately (i.e. the GKdim is ∞).

Because of this exception we were able to develop the MAXIMUM CYCLE COUNT algorithm which computes this property of the graph in $O(|V| + |E|)$.

Without this exception, the problem is closely related to an NP-hard problem known as #CYCLE.

We have also **generalized** this algorithm to f. p. bimodules.

Application to Finitely Presented Algebras

The book "Gröbner Bases in Ring Theory" (2012) by Huishi Li was a motivating companion to us.

We have detected and repaired a serious mistake in an example, running through this book. Namely, for $n \in \mathbb{N}_0$ consider the family of ideals $I_n = \langle X^n Y \rangle \subset A = K\langle X, Y \rangle$. Then the following holds

- if $n = 1$, $\operatorname{GKdim} A/I_1 = 2 = \text{gl. dim}\, A/I_1$,
- for $n \geq 2$, $\operatorname{GKdim} A/I_n = 2$ and $\text{gl. dim}\, A/I_n = 2$ (**false**)
- for $n \geq 2$, $\operatorname{GKdim} A/I_n = \infty$ and $\text{gl. dim}\, A/I_n = 2$ (**true**).

Proof: a) We show, that for $n \geq 2$ A/I_n contains a free algebra in two variables by giving explicit generators (this implies $\operatorname{GKdim} A/I_n = \infty$) and that only $\text{gl. dim}\, A/I_n \leq 2$ holds.
b) By providing an explicit free bimodule resolution of an ideal over A/I_n, we show that $\text{gl. dim}\, A/I_n \geq 2$ holds.
Both cases were **heavily supported** by computations.

Timings for Gröbner bases over $\mathbb{Q}$ wrt degree right lex (dp)

Intel Core i7-9700K, 64GB RAM, Debian GNU/Linux 10.
Singular 4.1.2 and Magma V2.24-10.

Example	**Singular**	**Magma (BB)**	**Magma (F4)**
lascala_neuh_d10	30.35	26.23	13.62
serre-f4-d15	5.45	62.58	8.96
serre-ha11-d15	11.27	49.63	5.80
serre-eha112-d13	2.05	3.41	1.72
4nilp5s-d8	36.68	55.43	9.54
braidXY	114.19	163.72	4.20
ug2-x1x2x3x4	1.10	21.60	0.83
serre-e6-d15	22.76	154.03	40.99
braid3-11	1.79	2.29	0.64
ufn3	70.22	3.36	2.26
ls3nilp-d10	0.72	3.57	1.98