Gröbner technology over free associative algebras over rings: semi-decidability, implementation and applications

Viktor Levandovskyy, University of Kassel, Germany

LIX Max Seminar, 29 March 2021

Appetizer

Let $X = \{x_1, \ldots, x_n\}$ be a finite set of indeterminates, and $\langle X \rangle$ the **free monoid** on X.

$\langle X \rangle$ as a set: all the words in the alphabet X, including the empty word ϵ (later identified with $1 \in \mathbb{Z}$ over rings).

Monoid operation (multiplication): concatenation (string gluing) $x_3x_1 \cdot x_2x_3 = x_3x_1x_2x_3$ which is associative but non-commutative $x_2 \cdot x_1 = x_2x_1 \neq x_1x_2 = x_1 \cdot x_2$.

For a commutative ring R, the **monoid ring** $R\langle X \rangle$ is the set of polynomials $\sum_i r_i w_i$, where $r_i \in R$ and $w_i \in \langle X \rangle$ subject to the usual addition and the multiplication, induced from $\langle X \rangle$.

Free associative algebra: $K\langle X \rangle$ for a field K; ring: $\mathbb{Z}\langle X \rangle$.

Q: why doing these terribly general free algebras?

A: well, every associative algebra is an epimorphic image of a certain free associative algebra in the following way:

Suppose A is gen. by $a_1, \ldots, a_m$ over K then

$$\varphi : K\langle x_1, \ldots, x_m\rangle \longrightarrow A, \quad x_i \mapsto a_i$$

is a homomorphism of K-algebras with the kernel $\mathcal{I} = \ker\varphi \subset K\langle X\rangle$, which is a **two-sided ideal**. Hence there is a canonical isomorphism of K-algebras

$$A \cong K\langle x_1, \ldots, x_m\rangle/\mathcal{I}.$$

Example: commutator ideal

$$K[x_1, \ldots, x_m] \cong K\langle x_1, \ldots, x_m\rangle/\langle\{x_j x_i - x_i x_j \mid 1 \leq i < j \leq n\}\rangle.$$

Effective computations: we need Gröbner bases over $K\langle X\rangle$!

Let X be a finite set of indeterminates,
$\langle X\rangle$ the free monoid on X and $\mathcal{P} = \mathbb{Z}\langle X\rangle$ or $K\langle X\rangle$.

Let X be a finite set of indeterminates,
$\langle X\rangle$ the free monoid on X and $\mathcal{P} = \mathbb{Z}\langle X\rangle$ or $K\langle X\rangle$.
We can write any element $f \in \mathcal{P} \setminus \{0\}$ as

$$f = c_1 t_1 + \ldots + c_n t_n$$

with

- **coefficients** $c_i \in \mathbb{Z} \setminus \{0\}$,
- **monomials** $t_i \in \langle X\rangle$ and
- **terms** $c_i t_i$.

Let X be a finite set of indeterminates,
$\langle X\rangle$ the free monoid on X and $\mathcal{P}=\mathbb{Z}\langle X\rangle$ or $K\langle X\rangle$.
We can write any element $f\in\mathcal{P}\setminus\{0\}$ as

$$f=c_1t_1+\ldots+c_nt_n$$

with

- **coefficients** $c_i\in\mathbb{Z}\setminus\{0\}$,
- **monomials** $t_i\in\langle X\rangle$ and
- **terms** c_it_i.

A **global monomial ordering** $\prec$ on $\langle X\rangle$ is a well–ordering satisfying

1. $x\prec y\Rightarrow uxw\prec uyw$ for all x, y, u, $w\in\langle X\rangle$ and
2. $1\preceq x$ for all $x\in\langle X\rangle$.

Remark: there is no **finite** classification of orderings over $\langle X\rangle$.

Let $t_n \prec \ldots \prec t_1$. Then, with respect to $\prec$ we define

- $\mathrm{LC}(f) := c_1$ is the **leading coefficient**,
- $\mathrm{LM}(f) := t_1$ is the **leading monomial** and
- $\mathrm{LT}(f) := c_1 t_1$ is the **leading term**.

Let $t_n \prec \ldots \prec t_1$. Then, with respect to $\prec$ we define

- $\mathsf{LC}(f) := c_1$ is the **leading coefficient**,
- $\mathsf{LM}(f) := t_1$ is the **leading monomial** and
- $\mathsf{LT}(f) := c_1 t_1$ is the **leading term**.

For $\emptyset \neq \mathcal{G} \subseteq \mathcal{P}$ we define

$$\mathsf{L}(\mathcal{G}) := \langle \mathsf{LT}(g) \mid g \in \mathcal{G} \setminus \{0\} \rangle$$

as the two–sided ideal generated by the leading terms of the elements in $\mathcal{G}$.

Let $t_n \prec \ldots \prec t_1$. Then, with respect to $\prec$ we define

- $\mathsf{LC}(f) := c_1$ is the **leading coefficient**,
- $\mathsf{LM}(f) := t_1$ is the **leading monomial** and
- $\mathsf{LT}(f) := c_1 t_1$ is the **leading term**.

For $\emptyset \neq \mathcal{G} \subseteq \mathcal{P}$ we define

$$\mathsf{L}(\mathcal{G}) := \langle \mathsf{LT}(g) \mid g \in \mathcal{G} \setminus \{0\} \rangle$$

as the two–sided ideal generated by the leading terms of the elements in $\mathcal{G}$.

We have a natural notion of **divisibility** on $\langle X \rangle$: u divides w if and only if there exist $p, q \in \langle X \rangle$ such that $w = p \cdot u \cdot q$, i.e. u is a subword of w.

Let $t_n \prec \ldots \prec t_1$. Then, with respect to $\prec$ we define

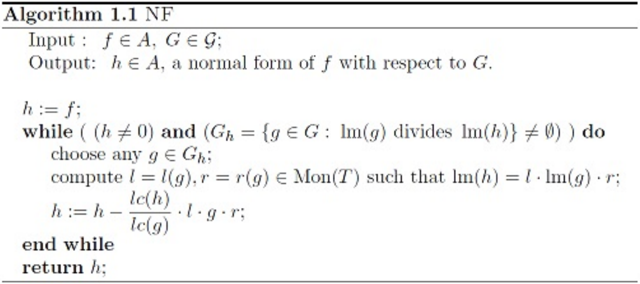
- $\mathsf{LC}(f) := c_1$ is the **leading coefficient**,
- $\mathsf{LM}(f) := t_1$ is the **leading monomial** and
- $\mathsf{LT}(f) := c_1 t_1$ is the **leading term**.

For $\emptyset \neq \mathcal{G} \subseteq \mathcal{P}$ we define

$$\mathsf{L}(\mathcal{G}) := \langle \mathsf{LT}(g) \mid g \in \mathcal{G} \setminus \{0\} \rangle$$

as the two–sided ideal generated by the leading terms of the elements in $\mathcal{G}$.

We have a natural notion of **divisibility** on $\langle X \rangle$: u divides w if and only if there exist $p, q \in \langle X \rangle$ such that $w = p \cdot u \cdot q$, i.e. u is a subword of w.
Hence a **division algorithm** of a polynomial p with respect to a set F follows.



Algorithm 1.1 NF

```
Input :  $f \in A,\ G \in \mathcal{G}$;
Output:  $h \in A$, a normal form of $f$ with respect to $G$.

$h := f$;
while ( ($h \neq 0$) and ($G_h = \{g \in G :\ \mathrm{lm}(g)$ divides $\mathrm{lm}(h)\} \neq \emptyset$) ) do
    choose any $g \in G_h$;
    compute $l = l(g), r = r(g) \in \mathrm{Mon}(T)$ such that $\mathrm{lm}(h) = l \cdot \mathrm{lm}(g) \cdot r$;
    $h := h - \frac{lc(h)}{lc(g)} \cdot l \cdot g \cdot r$;
end while
return $h$;
```

What does it mean for an ideal of $\mathcal{P}$ to be two–sided?

An element f is in the two–sided ideal of $\mathcal{P}$, generated by $\{g_1, \ldots, g_m\}$, iff there exist $\ell_{ij}, \wp_{ij} \in \mathcal{P}$ and $d_i \in \mathbb{N}$, such that

$$f = \sum_{i=1}^{m} \sum_{j=1}^{d_i} \ell_{ij} \cdot g_i \cdot \wp_{ij}.$$

This is a **two–sided presentation** of f.

What does it mean for an ideal of $\mathcal{P}$ to be two–sided?

An element f is in the two–sided ideal of $\mathcal{P}$, generated by $\{g_1, \ldots, g_m\}$, iff there exist $\ell_{ij}, \wp_{ij} \in \mathcal{P}$ and $d_i \in \mathbb{N}$, such that

$$f = \sum_{i=1}^{m} \sum_{j=1}^{d_i} \ell_{ij} \cdot g_i \cdot \wp_{ij}.$$

This is a **two–sided presentation** of f.

Note, that $\mathcal{P}^e = \mathcal{P} \otimes_{\mathbb{Z}} \mathcal{P}^{\text{opp}}$ naturally acts on $\mathcal{P}$ via

$$\left(\sum_{j=1}^{d} \ell_j \otimes \wp_j \right) \bullet g = \sum_{j=1}^{d} \ell_j \cdot g \cdot \wp_j \in \mathcal{P}.$$

(opp: "opposite")

Thus, we can use $\mathcal{P}^e$ for an easier encoding

$$f = \sum_{i=1}^{m} \sum_{j=1}^{d_i} \ell_{ij} \cdot g_i \cdot \wp_{ij} = \sum_{i=1}^{m} \underbrace{\left(\sum_{j=1}^{d_i} \ell_{ij} \otimes \wp_{ij} \right)}_{=p_i} \bullet g_i =: \sum_{i=1}^{m} p_i g_i .$$

with $p_i \in \mathcal{P}^e$, where we leave out the "$\bullet$" denoting the action.

Thus, we can use $\mathcal{P}^e$ for an easier encoding

$$f = \sum_{i=1}^{m} \sum_{j=1}^{d_i} \ell_{ij} \cdot g_i \cdot \wp_{ij} = \sum_{i=1}^{m} \underbrace{\left(\sum_{j=1}^{d_i} \ell_{ij} \otimes \wp_{ij} \right)}_{=p_i} \bullet g_i =: \sum_{i=1}^{m} p_i g_i.$$

with $p_i \in \mathcal{P}^e$, where we leave out the "$\bullet$" denoting the action.

Let $\mathcal{I} = \langle \mathcal{G} \rangle$ for a non–empty subset $\mathcal{G} \subseteq \mathcal{P}$. Clearly $\mathsf{L}(\mathcal{G}) \subseteq \mathsf{L}(\mathcal{I})$. $\mathcal{G}$ is called a **Gröbner basis** for $\mathcal{I}$, if $\mathsf{L}(\mathcal{G}) = \mathsf{L}(\mathcal{I})$.

Thus, we can use $\mathcal{P}^e$ for an easier encoding

$$f = \sum_{i=1}^{m} \sum_{j=1}^{d_i} \ell_{ij} \cdot g_i \cdot \wp_{ij} = \sum_{i=1}^{m} \underbrace{\left(\sum_{j=1}^{d_i} \ell_{ij} \otimes \wp_{ij} \right)}_{=p_i} \bullet g_i =: \sum_{i=1}^{m} p_i g_i .$$

with $p_i \in \mathcal{P}^e$, where we leave out the “$\bullet$” denoting the action.

Let $\mathcal{I} = \langle \mathcal{G} \rangle$ for a non–empty subset $\mathcal{G} \subseteq \mathcal{P}$. Clearly $\mathrm{L}(\mathcal{G}) \subseteq \mathrm{L}(\mathcal{I})$. $\mathcal{G}$ is called a **Gröbner basis** for $\mathcal{I}$, if $\mathrm{L}(\mathcal{G}) = \mathrm{L}(\mathcal{I})$.

Computationally: a single S-polynomial of a critical pair of polynomials (f, g) from the commutative case is replaced by the **set of overlaps** $\mathcal{O}(f, g)$: for $f = xy, g = yz$ we have

x	y	
	y	z
x	y	z

Q: why coefficients in $\mathbb{Z}$ are important?

A: Results of computations over $\mathbb{Z}$ contain information of computations over prime fields $GF(p)$ and rings $\mathbb{Z}/m\mathbb{Z}$ of **all** characteristics.

Later in the talk we will illustrate this in an example.

Q: why coefficients in $\mathbb{Z}$ are important?

A: Results of computations over $\mathbb{Z}$ contain information of computations over prime fields $GF(p)$ and rings $\mathbb{Z}/m\mathbb{Z}$ of **all** characteristics.

Later in the talk we will illustrate this in an example.

We concentrate on free algebras $\mathbb{Z}\langle X\rangle$, provide theoretical algorithmic advances and detect intrinsic phenomena.
These occuring neither in $K\langle X\rangle$ nor over $\mathbb{Z}[X]$!

Notably, Gröbner bases over $\mathbb{Z}\langle X\rangle$ are – in a sense – more often infinite than over $K\langle X\rangle$.

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.

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 (as suggested by Mora, Pritchard).

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 (as suggested by 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.

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 (as suggested by 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 undecidable.

Genetics (A. Cohen et al.): check the latest Nobel Prize!

In 2005, the Dutch journal *"Natuur en Techniek"* asked: is there a DNA change of cows so that they could produce **cola** instead of **milk**. There are tools to perform the following five allowed DNA string operations on the A, C, G, T

$$TCAT \to T, GAG \to AG, CTC \to TC, AGTA \to A, TAT \to CT.$$

Question:

Can one (and how) transform the gene of milk $TAGCTAGCTAGCT$ to the gene of cola $CTGACTGACT$? Is there a way to avoid hitting a retrovirus (close to corona, originally related to *mad cow disease*) $CTGCTACTGACT$?

In order to answer these questions, we need Gröbner bases over free algebras.

Create $K\langle A, C, G, T\rangle$, collect the rules into the two-sided ideal $\mathcal{I} = \langle TCAT - T, \ldots, \rangle$, and check, whether the difference of gene sequences `milk-cola` belongs to the ideal $\mathcal{I}$ (ideal membership problem).

Create $K\langle A, C, G, T\rangle$, collect the rules into the two-sided ideal $\mathcal{I} = \langle TCAT - T, \ldots, \rangle$, and check, whether the difference of gene sequences `milk-cola` belongs to the ideal $\mathcal{I}$ (ideal membership problem).

The Gröbner basis $\mathcal{F}$ of $\mathcal{I}$ is finite and nice indeed:

$$f_1 = GA - A,\ f_2 = CT - T,\ f_3 = TCA - TA,$$

$$f_4 = TAT - T,\ f_5 = ATA - A,\ f_6 = AGT - AT.$$

Now we perform division with remainder wrt the Gröbner basis $\mathcal{F}$:

$$\text{(milk) } TAGCTAGCTAGCT \to_{f_2} TAGTAGTAGT$$

$$\to_{f_6} TATATAT \to_{f_5} TAT \to_{f_4} T$$

$$\text{(cola) } CTGACTGACT \to_{f_1} CTACTACT \to_{f_2} TATAT \to_{f_1} T$$

$$\text{(retro) } CTGCTACTGACT \to_{\mathcal{F}} TGT$$

With a Gröbner bases theory for objects in a certain category, one usually strives to answer the questions like

- ideal/submodule membership problem:
  - in a boolean form (yes/no) or
  - in a certified form (an instance of the *division with remainder* algorithm)
- what are the linear relations with coefficient in a given ring between the given elements? (known as *syzygies*)
- what is a subideal/submodule, expressed with a subset of the set of variables? (*elimination of variables*)
- and many more...

The answers to these questions in form of theory, algorithms and implementations . . .

are rudimentary known for commutative polynomial rings with coefficients in effective fields $K[X] = K[x_1, \dots, x_n]$;

The answers to these questions in form of theory, algorithms and implementations . . .

for commutative polynomial rings with coefficients in principal ideal rings $R[X]$ have been **only recently** formulated in an **implementable** way.

Thanks to the work of many people, among other *D. Lichtblau, J. Apel, F. Pauer, O. Wienand, G. Pfister, A. Frühbis-Krüger, A. Popescu, C. Eder, T. Hofmann, Teo Mora and F. Pritchard.*

The answers to these questions in form of theory, algorithms and implementations . . .

for commutative polynomial rings with coefficients in principal ideal rings $R[X]$ have been **only recently** formulated in an **implementable** way.

Thanks to the work of many people, among other *D. Lichtblau, J. Apel, F. Pauer, O. Wienand, G. Pfister, A. Frühbis-Krüger, A. Popescu, C. Eder, T. Hofmann, Teo Mora and F. Pritchard.*

“A Manual for creating own Gröbner basis theory” by Teo Mora

Solving Polynomial Equation Systems IV:
Buchberger Theory and Beyond

This recent book (becoming the standard reference) summarizes modern Gröbner bases (Buchberger) theory for e.g. associative algebras over effective rings.

The answers to the questions above in form of theory, algorithms and implementations ...

for associative free non-commutative algebras with coefficients in effective fields $K\langle X\rangle = K\langle x_1, \dots, x_n\rangle$

are known; there are implementations in MAGMA (actual), GBNP (GAP) and NCALGEBRA (MATHEMATICA) (modern), BERGMAN, FELIX, OPAL (older).

SINGULAR:LETTERPLACE 4-1-3

We utilize the *Letterplace* correspondence by La Scala and Levandovskyy, which allows e.g. to use commutative data structures and special *Letterplace Gröbner bases*. It has been formulated in an **implementable** way.

With SINGULAR 4-1-3, we offer the broadest functionality among all these systems at a decent speed.

The answers to the questions above in form of theory, algorithms and implementations ...

for non-commutative free associative algebras with coefficients in rings $R\langle X\rangle = R\langle x_1, \ldots, x_n\rangle$

It suffices to implement $R = \mathbb{Z}$ and $R = \mathbb{Z}/m\mathbb{Z}$ for $m \in \mathbb{N}$ as coefficients for our rings!

Block elimination orderings allow the treatment of $(\mathbb{Z}\langle Y\rangle/J)\langle X\rangle$ via computing in $\mathbb{Z}\langle Y, X\rangle$ subject to an appropriate ordering. We offer at least two types of such block elimination orderings.

To the best of our knowledge, there are no computer algebra systems, with which we could compare our implementation in $\mathbb{Z}\langle X\rangle$.

Decidabililty I

Everyone knows that *the word problem in $K\langle X\rangle$ is undecidable*, i.e. given p and $I \subset K\langle X\rangle$, there is no **algorithm** to check $p \in I$.

Decidabililty I

Everyone knows that *the word problem in $K\langle X\rangle$ is undecidable*, i.e. given p and $I \subset K\langle X\rangle$, there is no **algorithm** to check $p \in I$.

$p \in I$ via Gröbner bases

$p \in I \Leftrightarrow$ the remainder of division of p wrt a Gröbner basis G is 0.

Decidabililty I

Everyone knows that *the word problem in $K\langle X\rangle$ is undecidable*, i.e. given p and $I \subset K\langle X\rangle$, there is no **algorithm** to check $p \in I$.

$p \in I$ via Gröbner bases

$p \in I \Leftrightarrow$ the remainder of division of p wrt a Gröbner basis G is 0.

Assuming a well-ordering $<$, the bottleneck is the computation of a Gröbner basis: since $R\langle X\rangle$ is not Noetherian (even for a ring R being a field), a Gröbner basis need not be finite.

Can we say more? **Yes!**

Decidabililty I

Everyone knows that *the word problem in* $K\langle X\rangle$ *is undecidable*, i.e. given p and $I \subset K\langle X\rangle$, there is no **algorithm** to check $p \in I$.

$p \in I$ via Gröbner bases

$p \in I \Leftrightarrow$ the remainder of division of p wrt a Gröbner basis G is 0.

Assuming a well-ordering $<$, the bottleneck is the computation of a Gröbner basis: since $R\langle X\rangle$ is not Noetherian (even for a ring R being a field), a Gröbner basis need not be finite.

Can we say more? **Yes!**

Finite GB = Decidable

If a Gröbner basis of an ideal I wrt $<$ is finite, it will be computed in finitely many steps. GB Algorithm need to have this property.

Decidabililty II

Graded by Well-ordered Monoid = Decidable

If a generating set of an ideal I can be **graded** via a monoid Γ, which is (think about $\mathbb{N}, \mathbb{N}^n$)

- well-ordered (say, via $\prec$),
- has only finitely many elements smaller wrt $\prec$ than the identity,

then computing wrt any ordering, *compatible with* Γ yields a **truncated** Gröbner basis.

Decidabililty II

Graded by Well-ordered Monoid = Decidable

If a generating set of an ideal I can be **graded** via a monoid Γ, which is (think about $\mathbb{N}, \mathbb{N}^n$)

- well-ordered (say, via $\prec$),
- has only finitely many elements smaller wrt $\prec$ than the identity,

then computing wrt any ordering, *compatible with* Γ yields a **truncated** Gröbner basis.

In other words: *operations with elements, whose LMs are bigger than some $\gamma \in \Gamma$, do not change the elements whose LMs are smaller than γ.*
Since p has a finite graded degree, say γ, we have

$$p \in I \Leftrightarrow p \in \oplus_{\alpha \leq \gamma} I_\alpha.$$

Decidabililty III

Bad news

if a module (or an ideal) cannot be graded by Γ, and no finite Gröbner basis exists, **we know very little on the module**.

Decidabililty III

Bad news

if a module (or an ideal) cannot be graded by Γ, and no finite Gröbner basis exists, **we know very little on the module**.

Computing up to a degree bound does not result in a **trustable truncation** since
manipulating elements, whose LMs are bigger than some $\gamma \in \Gamma$,
will *change the elements whose LMs are smaller than* γ.

Thus, if $p \notin I$, even by increasing the truncation bound we will be involved in the **infinite computation**, what is the real meaning of undecidability.

Good news

knowing the affirmative answer $p \in I$ in advance makes the computation of the certificate (or a proof) for this decidable!

Decidabililty IV: algebras of iterated two-sided inverses

An important exception: algebras of iterated two-sided inverses

Let A be a fin. pres. assoc. algebra and $a \in A$ be regular.

Adjoining to A a new variable t with relations $ta - 1, at - 1$, we obtain an algebra, containing A as a subalgebra.

Repeating this finitely many times, we obtain an *algebra of iterated two-sided inverses* over A.

Decidabililty IV: algebras of iterated two-sided inverses

An important exception: algebras of iterated two-sided inverses

Let A be a fin. pres. assoc. algebra and $a \in A$ be regular.

Adjoining to A a new variable t with relations $ta - 1, at - 1$, we obtain an algebra, containing A as a subalgebra.

Repeating this finitely many times, we obtain an *algebra of iterated two-sided inverses* over A.

(Amitsur, P. M. Cohn): doing this for **all** elements of $K\langle X\rangle \setminus \{0\}$, we obtain **the free field on $\boldsymbol{X}$**, the universal field of fractions of $K\langle X\rangle$.

Decidabililty: algebras of iterated two-sided inverses

Almost a miracle: Cohn and Reutenauer (1999)

The word problem in the free field is decidable.

By using

- Higman's linearization trick from the ring theory,
- *linear realizations*, stemming initially from control theory
- test for maximality of the inner rank of a matrix over $K\langle X\rangle$

one can not only prove the decidability, but also give algorithms to compute the boolean form of the word problem!

J. Hoffmann, R. Schnur (Saarbrücken): implementations `ncrat.lib` in SINGULAR and `FreeFractions.jl` in OSCAR.

Algebraic Analysis with Letterplace

The newly released subsystem Singular:Letterplace can perform computations (Gröbner bases and numerous advanced applications of them) within free associative algebras over fields and over $\mathbb{Z}$.

Example (L.-S.-Z. paper, ISSAC 2020)

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

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

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

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

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:

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

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 $K\langle X\rangle$.

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.

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.

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 $\mathcal{F}_r(A) = \bigoplus_{i=1}^{r} A\,\varepsilon_i\,A$.

Operations with one-sided ideals/modules over $K\langle X\rangle$: easy;
over fin. pres. algebra $A = K\langle X\rangle/\mathcal{I}$ 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 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.

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.

Fundamental Functionality

Below, F is a set of generators and G is a two-sided Gröbner basis for an ideal or a submodule.

`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`*)*

Genetics Example

```
LIB "freegb.lib";
ring r = 0,(A,C,G,T),Dp;
ring R = freeAlgebra(r,15);
ideal I=T*C*A*T-T,G*A*G-A*G,C*T*C-T*C,A*G*T*A-A,T*A*T-C*T;
option(prot); ideal J = twostd(I);
poly milk = T*A*G*C*T*A*G*C*T*A*G*C*T;
reduce(milk, J); // T
poly cola = C*T*G*A*C*T*G*A*C*T;
reduce(cola, J); // T, same as milk, so "yes" to cola
poly retro = C*T*G*C*T*A*C*T*G*A*C*T;
reduce(retro, J); // TGT, not the same, so "no" to retro
```

with the help of the function `lift` we are able to extract the exact way of the transformation of milk into the cola.

Some live examples over $\mathbb{Z}\langle x, y, z\rangle$

```
LIB "freegb.lib";
ring r = integer,(x,y,z),dp;
ring R = freeAlgebra(r, 7);
ideal I = 3x, 2y;
option(prot);     // explain here what the protocol means
I = twostd(I); I;

ideal J = z*y - y*z + z^2, z*x + y^2, y*x - 3*x*y;
J = twostd(J); J; // we see the impact of 7 on leadcoeffs

ring r7 = 7,(x,y,z),dp; // this time we compute over Z/7Z =
ring R7 = freeAlgebra(r7, 7);
ideal J = z*y - y*z + z^2, z*x + y^2, y*x - 3*x*y;
J = twostd(J); J;
```

Thanks for your attention

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)
`ncfactor.lib` (Heinle-L)	factorization of polynomials over free and fin. pres. algebras

Advanced Functionality

`fpaprops.lib`, one of our flagships, offers computations of

- Gel'fand–Kirillov dimension (aka *growth*) of $K\langle X\rangle/\mathcal{I}$
- an upper bound of the global dimension of $K\langle X\rangle/\mathcal{I}$
- whether the factor algebra is left/right/weak Noetherian
- whether the factor algebra is prime or semiprime

Integro-differential algebra

```
LIB "freegb.lib";
ring r = 0,(D,I,x),dp;
ring R = freeAlgebra(r, 5);
ideal J = D*x-x*D-1, I*x-x*I+I*I, D*I-1;
J = twostd(J); J;  // infinite GB!
ring r = 0,(D,I,x),rp; // other ordering
ring R = freeAlgebra(r, 5);
ideal J = D*x-x*D-1, I*x-x*I+I*I, D*I-1;
J = twostd(J); J; // a finite GB
LIB "fpaprops.lib";
lpGkDim(J); // 3
lpGlDimBound(J); // 3 hence gldim=GKdim=3
lpIsPrime(J); // 0
lpIsSemiPrime(J); // 0
lpNoetherian(J); //0
```