Using Signature Gröbner Bases to Find Short Ideal Representations

Clemens Hofstadler[1], Thibaut Verron[2]

SIAM Conference on Applied Algebraic Geometry, 14 July 2023

Multivariate Polynomials, Ideals, and Modules: Algorithms and Applications

1. Institute of Mathematics, University of Kassel, Kassel, Germany
2. Institute for Algebra, Johannes Kepler University, Linz, Austria

JOHANNES KEPLER UNIVERSITÄT LINZ

Der Wissenschaftsfonds.

UNI KASSEL VERSITÄT

Example:

- Definition: an inner inverse of a matrix A is a matrix B such that $ABA = A$
- Theorem: if A is invertible with inverse C and if B is an inner inverse of A, then $B = C$
- Proof: easy exercise ■

Example:

- Definition: an inner inverse of a matrix A is a matrix B such that $ABA = A$
- Theorem: if A is invertible with inverse C and if B is an inner inverse of A, then $B = C$
- Proof: easy exercise ■

How to prove this with Gröbner bases?

- Objects → generators of a free algebra: $K\langle a, b, c\rangle$
- Axioms → ideal: $I = \langle ac - 1, ca - 1\rangle + \langle aba - a\rangle$
- Theorem → Ideal Membership Problem: $b - c \in I$?
- New proof: $b - c$ reduces to zero modulo a Gröbner basis of I
- Proof: trust me ■

Example:

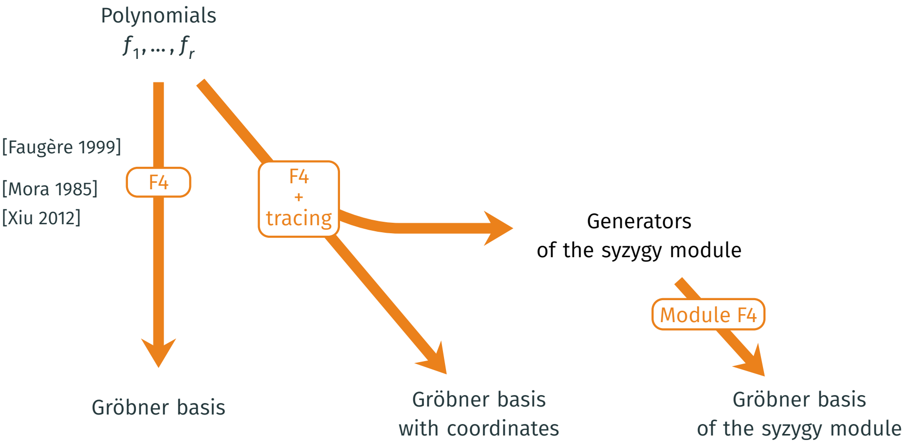
- Definition: an inner inverse of a matrix A is a matrix B such that $ABA = A$
- Theorem: if A is invertible with inverse C and if B is an inner inverse of A, then $B = C$
- Proof: easy exercise ■

How to prove this with Gröbner bases?

- Objects → generators of a free algebra: $K\langle a, b, c\rangle$
- Axioms → ideal: $I = \langle ac - 1, ca - 1\rangle + \langle aba - a\rangle$
- Theorem → Ideal Membership Problem: $b - c \in I$?
- New proof: $b - c$ reduces to zero modulo a Gröbner basis of I

- Proof: cofactor representation:

$$c - b = b\,(ac - 1) - c\,(ac - 1) - c\,(aba - a)\,c + (ca - 1)\,bac. \qquad \blacksquare$$



Ideal Membership Problem

"Does there exist (a_i, b_j) such that $p = a_1 f_{i_1} b_1 + \dots + a_N f_{i_N} b_N$?"

IMP with certificate

"Compute (a_i, b_j) such that $p = a_1 f_{i_1} b_1 + \dots + a_N f_{i_N} b_N$"

Module of syzygies

"Find all (a_i, b_j) such that $a_1 f_{i_1} b_1 + \dots + a_N f_{i_N} b_N = 0$"

Gröbner bases and signature Gröbner bases

Polynomials
$f_1, \dots, f_r$

F5/GVW

[Faugère 2002] [Gao Volny Wang 2010]
[Eder Faugère 2017] [Lairez 2022]

[Hofstadler V. 2022, 2023]

Gröbner basis
with signatures

Gröbner basis

Gröbner basis
with coordinates

Gröbner basis
of the syzygy module

Ideal Membership Problem

*“Does there exist (a_i, b_j)
such that
$p = a_1 f_{i_1} b_1 + \dots + a_N f_{i_N} b_N$?”*

IMP with certificate

*“Compute (a_i, b_j)
such that
$p = a_1 f_{i_1} b_1 + \dots + a_N f_{i_N} b_N$”*

Module of syzygies

*“Find all (a_i, b_j)
such that
$a_1 f_{i_1} b_1 + \dots + a_N f_{i_N} b_N = 0$”*

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac - 1, ca - 1, aba - a\rangle$ in $K\langle a, b, c\rangle$?

	Gröbner basis element	Cofactors
$\boxed{1}$	$ac - 1$	$\boldsymbol{e}_1$
$\boxed{2}$	$ca - 1$	$\boldsymbol{e}_2$
$\boxed{3}$	$aba - a$	$\boldsymbol{e}_3$

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac - 1, ca - 1, aba - a\rangle$ in $K\langle a, b, c\rangle$?

	Gröbner basis element	Cofactors
$\boxed{1}$	$ac - 1$	$\boldsymbol{e}_1$
$\boxed{2}$	$ca - 1$	$\boldsymbol{e}_2$
$\boxed{3}$	$aba - a$	$\boldsymbol{e}_3$
$\boxed{4} = \boxed{3}c - ab\boxed{1}$	$-ac + ab$	$\boldsymbol{e}_3 c - ab\boldsymbol{e}_1$

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac - 1, ca - 1, aba - a \rangle$ in $K\langle a, b, c \rangle$?

	Gröbner basis element	Cofactors
$\boxed{1}$	$ac - 1$	$\boldsymbol{e}_1$
$\boxed{2}$	$ca - 1$	$\boldsymbol{e}_2$
$\boxed{3}$	$aba - a$	$\boldsymbol{e}_3$
$\boxed{4} = \boxed{3}\,c - ab\boxed{1} + \boxed{1}$	$ab - 1$	$\boldsymbol{e}_3 c - ab\boldsymbol{e}_1 + \boldsymbol{e}_1$

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac - 1, ca - 1, aba - a\rangle$ in $K\langle a, b, c\rangle$?

	Gröbner basis element	Cofactors
$\boxed{1}$	$ac - 1$	$\boldsymbol{e}_1$
$\boxed{2}$	$ca - 1$	$\boldsymbol{e}_2$
$\boxed{3}$	$aba - a$	$\boldsymbol{e}_3$
$\boxed{4} = \boxed{3}c - ab\boxed{1} + \boxed{1}$	$ab - 1$	$\boldsymbol{e}_3 c - ab\boldsymbol{e}_1 + \boldsymbol{e}_1$
$\boxed{5} = c\boxed{4} - \boxed{2}b$	$-c + b$	$c\boldsymbol{e}_3 c - \boldsymbol{e}_2 b - cab\boldsymbol{e}_1 - c\boldsymbol{e}_1$

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac - 1, ca - 1, aba - a\rangle$ in $K\langle a, b, c\rangle$?

	Gröbner basis element	Cofactors (signature)
$\boxed{1}$	$ac - 1$	$\boldsymbol{e}_1$
$\boxed{2}$	$ca - 1$	$\boldsymbol{e}_2$
$\boxed{3}$	$aba - a$	$\boldsymbol{e}_3$
$\boxed{4} = \boxed{3}c - ab\boxed{1} + \boxed{1}$	$ab - 1$	$\boldsymbol{e}_3 c - ab\boldsymbol{e}_1 + \boldsymbol{e}_1$
$\boxed{5} = c\boxed{4} - \boxed{2}b$	$-c + b$	$c\boldsymbol{e}_3 c - \boldsymbol{e}_2 b - cab\boldsymbol{e}_1 - c\boldsymbol{e}_1$

The signature is enough to reconstruct the cofactor representation:

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac - 1, ca - 1, aba - a\rangle$ in $K\langle a, b, c\rangle$?

	Gröbner basis element	Cofactors (signature)
$\boxed{1}$	$ac - 1$	$\boldsymbol{e}_1$
$\boxed{2}$	$ca - 1$	$\boldsymbol{e}_2$
$\boxed{3}$	$aba - a$	$\boldsymbol{e}_3$
$\boxed{4} = \boxed{3}c - ab\boxed{1} + \boxed{1}$	$ab - 1$	$\boldsymbol{e}_3 c - ab\boldsymbol{e}_1 + \boldsymbol{e}_1$
$\boxed{5} = c\boxed{4} - \boxed{2}b$	$-c + b$	$c\boldsymbol{e}_3 c - \boldsymbol{e}_2 b - cab\boldsymbol{e}_1 - c\boldsymbol{e}_1$

The signature is enough to reconstruct the cofactor representation:

1. $ac - 1$ with signature $\boldsymbol{e}_1 \longrightarrow f_1 - (ac - 1) = 0$

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac - 1, ca - 1, aba - a\rangle$ in $K\langle a, b, c\rangle$?

	Gröbner basis element	Cofactors (signature)
$\boxed{1}$	$ac - 1$	$\boldsymbol{e}_1$
$\boxed{2}$	$ca - 1$	$\boldsymbol{e}_2$
$\boxed{3}$	$aba - a$	$\boldsymbol{e}_3$
$\boxed{4} = \boxed{3}c - ab\boxed{1} + \boxed{1}$	$ab - 1$	$\boldsymbol{e}_3 c - ab\boldsymbol{e}_1 + \boldsymbol{e}_1$
$\boxed{5} = c\boxed{4} - \boxed{2}b$	$-c + b$	$c\boldsymbol{e}_3 c - \boldsymbol{e}_2 b - cab\boldsymbol{e}_1 - c\boldsymbol{e}_1$

The signature is enough to reconstruct the cofactor representation:

1. $ac - 1$ with signature $\boldsymbol{e}_1 \longrightarrow f_1 - (ac - 1) = 0$
2. $ca - 1$ with signature $\boldsymbol{e}_2 \longrightarrow f_2 - (ca - 1) = 0$
3. $aba - a$ with signature $\boldsymbol{e}_3 \longrightarrow f_3 - (aba - a) = 0$

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac - 1, ca - 1, aba - a\rangle$ in $K\langle a, b, c\rangle$?

	Gröbner basis element	Cofactors (signature)
$\boxed{1}$	$ac - 1$	$\mathbf{e}_1$
$\boxed{2}$	$ca - 1$	$\mathbf{e}_2$
$\boxed{3}$	$aba - a$	$\mathbf{e}_3$
$\boxed{4} = \boxed{3}c - ab\boxed{1} + \boxed{1}$	$ab - 1$	$\mathbf{e}_3 c - ab\mathbf{e}_1 + \mathbf{e}_1$
$\boxed{5} = c\boxed{4} - \boxed{2}b$	$-c + b$	$c\mathbf{e}_3 c - \mathbf{e}_2 b - cab\mathbf{e}_1 - c\mathbf{e}_1$

The signature is enough to reconstruct the cofactor representation:

1. $ac - 1$ with signature $\mathbf{e}_1 \longrightarrow f_1 - (ac - 1) = 0$
2. $ca - 1$ with signature $\mathbf{e}_2 \longrightarrow f_2 - (ca - 1) = 0$
3. $aba - a$ with signature $\mathbf{e}_3 \longrightarrow f_3 - (aba - a) = 0$
4. $ab - 1$ with signature $\mathbf{e}_3 c \longrightarrow f_3 c \qquad - (ab - 1) = abac - ac - ab + 1 \quad \neq 0$

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac - 1, ca - 1, aba - a \rangle$ in $K\langle a, b, c \rangle$?

	Gröbner basis element	Cofactors (signature)
$\boxed{1}$	$ac - 1$	$\boldsymbol{e}_1$
$\boxed{2}$	$ca - 1$	$\boldsymbol{e}_2$
$\boxed{3}$	$aba - a$	$\boldsymbol{e}_3$
$\boxed{4} = \boxed{3}c - ab\boxed{1} + \boxed{1}$	$ab - 1$	$\boldsymbol{e}_3 c - ab\boldsymbol{e}_1 + \boldsymbol{e}_1$
$\boxed{5} = c\boxed{4} - \boxed{2}b$	$-c + b$	$c\boldsymbol{e}_3 c - \boldsymbol{e}_2 b - cab\boldsymbol{e}_1 - c\boldsymbol{e}_1$

The signature is enough to reconstruct the cofactor representation:

1. $ac - 1$ with signature $\boldsymbol{e}_1 \longrightarrow f_1 - (ac - 1) = 0$
2. $ca - 1$ with signature $\boldsymbol{e}_2 \longrightarrow f_2 - (ca - 1) = 0$
3. $aba - a$ with signature $\boldsymbol{e}_3 \longrightarrow f_3 - (aba - a) = 0$
4. $ab - 1$ with signature $\boldsymbol{e}_3 c \longrightarrow f_3 c - (ab - 1) = abac - ac - ab + 1 \neq 0$

   $f_3 c - abf_1 - (ab - 1) = -ac + 1 \neq 0$

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac - 1, ca - 1, aba - a\rangle$ in $K\langle a, b, c\rangle$?

	Gröbner basis element	Cofactors (signature)
$\boxed{1}$	$ac - 1$	$\boldsymbol{e}_1$
$\boxed{2}$	$ca - 1$	$\boldsymbol{e}_2$
$\boxed{3}$	$aba - a$	$\boldsymbol{e}_3$
$\boxed{4} = \boxed{3}c - ab\boxed{1} + \boxed{1}$	$ab - 1$	$\boldsymbol{e}_3 c - ab\boldsymbol{e}_1 + \boldsymbol{e}_1$
$\boxed{5} = c\boxed{4} - \boxed{2}b$	$-c + b$	$c\boldsymbol{e}_3 c - \boldsymbol{e}_2 b - cab\boldsymbol{e}_1 - c\boldsymbol{e}_1$

The signature is enough to reconstruct the cofactor representation:

1. $ac - 1$ with signature $\boldsymbol{e}_1 \longrightarrow f_1 - (ac - 1) = 0$
2. $ca - 1$ with signature $\boldsymbol{e}_2 \longrightarrow f_2 - (ca - 1) = 0$
3. $aba - a$ with signature $\boldsymbol{e}_3 \longrightarrow f_3 - (aba - a) = 0$
4. $ab - 1$ with signature $\boldsymbol{e}_3 c \longrightarrow$

$$
\begin{aligned}
&f_3 c &&- (ab - 1) = abac - ac - ab + 1 && \neq 0\\
&f_3 c - abf_1 &&- (ab - 1) = -ac + 1 && \neq 0\\
&f_3 c - abf_1 + f_1 &&- (ab - 1) = 0 &&
\end{aligned}
$$

Back to the example

Question: does $b - c$ lie in the ideal $\langle ac-1, ca-1, aba-a\rangle$ in $K\langle a,b,c\rangle$?

	Gröbner basis element	Cofactors (signature)
$\boxed{1}$	$ac-1$	$\boldsymbol{e}_1$
$\boxed{2}$	$ca-1$	$\boldsymbol{e}_2$
$\boxed{3}$	$aba-a$	$\boldsymbol{e}_3$
$\boxed{4} = \boxed{3}c - ab\boxed{1} + \boxed{1}$	$ab-1$	$\boldsymbol{e}_3 c - ab\boldsymbol{e}_1 + \boldsymbol{e}_1$
$\boxed{5} = c\boxed{4} - \boxed{2}b$	$-c+b$	$c\boldsymbol{e}_3 c - \boldsymbol{e}_2 b - cab\boldsymbol{e}_1 - c\boldsymbol{e}_1$

The signature is enough to reconstruct the cofactor representation:

1. $ac-1$ with signature $\boldsymbol{e}_1 \longrightarrow f_1 - (ac-1) = 0$
2. $ca-1$ with signature $\boldsymbol{e}_2 \longrightarrow f_2 - (ca-1) = 0$
3. $aba-a$ with signature $\boldsymbol{e}_3 \longrightarrow f_3 - (aba-a) = 0$
4. $ab-1$ with signature $\boldsymbol{e}_3 c \longrightarrow$
$$f_3 c - (ab-1) = abac - ac - ab + 1 \neq 0$$
$$f_3 c - abf_1 - (ab-1) = -ac + 1 \neq 0$$
$$f_3 c - abf_1 + f_1 - (ab-1) = 0$$
5. $-c+b$ with signature $c\boldsymbol{e}_3 c \longrightarrow$
$$c(f_3 c - abf_1 + f_1) - (-c+b) = cab - b \neq 0$$
$$cf_3 c - cabf_1 + cf_1 - f_2 b - (-c+b) = 0$$

Short cofactor representations

Cofactor representations are not unique!

Example: $b - c = c(aba - a)c + (ca - 1)bac + b(ac - 1) - c(ac - 1)$

$$= c(aba - a)c - (ca - 1)b - cab(ac - 1) + c(ac - 1)$$

Short proofs are important for proof analysis.

Example: $b - c \in I = \langle ac - 1, ca - 1, aba - a, bab - b, ab - ed, ba - de \rangle \subseteq K\langle a, b, c, d, e \rangle$

($b : A^\dagger$ (Moore-Penrose inverse), $c : A^{-1}, d : A^*, e : (A^\dagger)^*$)

$$\begin{aligned} b - c = {} & b(ac - 1) - c(ac - 1) + (ca - 1)bac + c(aba - a)c \\ & - be(bab - b) + (bab - b)eb - b(ab - ed)eb + be(ba - de)a \end{aligned}$$

This work

- Algorithm for finding short (and often shortest) representations
- Also works in the commutative case
- Reduces to and generalizes a classical linear algebra problem
- Main tools: signatures and linear optimization

On the edge of decidability

Fact: the IMP over non-commutative polynomials is not decidable

Theorem (Hofstadler, V. 2023)
The problem of, given $f_1, \dots, f_r, f \in K\langle X\rangle$ and $N \in \mathbb{N}$, deciding whether f has a cofactor representation of length at most N in the f_i,
i.e., whether there exists $a_k, b_k \in \langle X\rangle$, $i_k \in \{1, \dots, r\}$ such that

$$f = a_1 f_{i_1} b_1 + \cdots + a_N f_{i_N} b_N,$$

is decidable.

Difficulty: no bound on the degrees of a_k and b_k

On the edge of decidability

Fact: the IMP over non-commutative polynomials is not decidable

Theorem (Hofstadler, V. 2023)
The problem of, given $f_1, \dots, f_r, f \in K\langle X \rangle$ and $N \in \mathbb{N}$, deciding whether f has a cofactor representation of length at most N in the f_i,
i.e., whether there exists $a_k, b_k \in \langle X \rangle$, $i_k \in \{1, \dots, r\}$ such that

$$f = a_1 f_{i_1} b_1 + \dots + a_N f_{i_N} b_N,$$

is decidable.

Difficulty: no bound on the degrees of a_k and b_k

For minimal representations, we can say more!

Rewriting
Example: given $f = x + xy$, $g = y + z$:

- $f - xg = x + xy - xy - xz$ is a rewriting of f by g
- $f + xg = x + 2xy + xz$ is also a rewriting of f by g
- $f + yg = x + xy + y^2 + yz$ is not a rewriting

- Any minimal representation of f by $f_1, \dots, f_r$ of length N can be expressed as N successive rewritings starting with f and ending with 0
- There is a bound on the degree of terms appearing in a rewriting!

Algorithm

I: $f, f_1, \dots, f_r \in K\langle X\rangle$, $N \in \mathbb{N}$

O: a (minimal) cofactor representation of f of length $\leq N$ if one exists

1. Compute the degree bound $D = \deg(f) + N \max \deg(f_i)$
2. Compute the set L of all polynomials af_ib with $i \in \{1, \dots, n\}$, $a, b \in \langle X\rangle$, $\deg(af_ib) \leq D$
3. Look for a K-linear combination of elements of L equal to f with $\leq N$ nonzero summands

Observations:

- The bulk of the computation is in the last step
- That step is difficult but decidable (if only by bruteforce)
- The input for that step is huge but finite
- The algorithm is not practical for anything but trivial examples

So we need:

- A better algorithm for solving the last step: linear programming
- A better bound on the search space: signatures

Min-RVLS (Minimum Relevant Variables in Linear Systems):

I: $A \in \mathbb{Q}^{m \times n}, b \in \mathbb{Q}^m, N \in \mathbb{N}$

O: $y \in \mathbb{Q}^n$ with $Ay = b$ and at most N nonzero coordinates if one exists

This is a difficult problem: NP-complete, hard to approximate.

Basis pursuit: ℓ_1 relaxation + Linear Programming [Chen, Donoho, Saunders 2001]

I. $A \in \mathbb{Q}^{m \times n}, b \in \mathbb{Q}^m, N \in \mathbb{N}$

O. $y \in \mathbb{Q}^n$ minimizing $\sum_{i=1}^n |y_i|$ under the constraint $Ay = b$.

Algorithm

I: $f, f_1, \dots, f_r \in K\langle X\rangle$, σ a signature

O: a cofactor representation of f with signature $\leq \sigma$ and minimal 1-norm (if it exists)

1. Compute the set L of all polynomials $a_k f_{i_k} b_k$ with $a_k \boldsymbol{e}_{i_k} b_k \leq \sigma$
2. Put them in a matrix A
3. Solve the linear problem:
   find $\begin{pmatrix} p \\ m \end{pmatrix}$ minimizing $\sum_i p_i + \sum_i m_i$ under the constraints $\begin{pmatrix} A & -A \end{pmatrix} \begin{pmatrix} p \\ m \end{pmatrix} = f$ and $p, m \geq 0$
4. Return $\sum_k (p_k - m_k) a_k \boldsymbol{e}_{i_k} b_k$

Observations:

- Deciding whether the search space is empty requires finding *any* solution of the linear system
- Doing so is essentially equivalent to computing a signature Gröbner basis up to signature σ (Matrix-F5 algorithm)

Symbolic preprocessing

Observation: if α and β have disjoint support, then

$$\|\alpha + \beta\| = \|\alpha\| + \|\beta\| \qquad \text{(both for 0-“norm” and 1-norm)}$$

Theorem (Hofstadler, V. 2023)

Let:

- H be a Gröbner basis of the module of syzygies up to some signature σ
- α be a cofactor representation of f in terms of $f_1, \ldots, f_r$ with $\mathrm{sig}(\alpha) \leq \sigma$
- β be a representation of f, shortest or 1-norm minimal among those with sig $\leq \sigma$

Then α can be rewritten to β by H, and the signature of every rewriter is $\leq \sigma$.

Symbolic preprocessing

Observation: if α and β have disjoint support, then

$$\|\alpha + \beta\| = \|\alpha\| + \|\beta\| \qquad \text{(both for 0-“norm” and 1-norm)}$$

Theorem (Hofstadler, V. 2023)
Let:

- H be a Gröbner basis of the module of syzygies up to some signature σ
- α be a cofactor representation of f in terms of $f_1, \dots, f_r$ with $\mathrm{sig}(\alpha) \leq \sigma$
- β be a representation of f, shortest or 1-norm minimal among those with sig $\leq \sigma$

Then α can be rewritten to β by H, and the signature of every rewriter is $\leq \sigma$.

Algorithm: Symbolic preprocessing

I: σ, H, α as above

O: a generating set B of $V \subset \mathrm{Syz}(f_1, \dots, f_r)$ such that for any optimal β, $\beta \in \alpha + V$.

1. $B \leftarrow \emptyset$, TODO $\leftarrow$ Support of α
2. While TODO is not empty
   - 2.1 Pick a monomial $\mu \in$ TODO
   - 2.2 Take all the multiples $a\gamma b$ of elements in H with signature $\leq \sigma$ and with μ in their support
   - 2.3 Add them to V and their support to TODO

Algorithm

I: $f, f_1, \dots, f_r \in K\langle X\rangle$, σ a signature, α a representation with signature $\leq \sigma$

O: a cofactor representation of f with signature $\leq \sigma$ and minimal 1-norm (it exists!)

1. Compute a Gröbner basis of $\mathrm{Syz}(f_1, \dots, f_r)$ up to signature σ
2. Compute the search space $B = \left\{a_1 \boldsymbol{e}_{i_1} b_1,\ a_2 \boldsymbol{e}_{i_2} b_2, \dots\right\}$ (symbolic preprocessing)
3. Prune B using further criteria and heuristics
4. Put B and α in a matrix A
5. Solve the linear problem:
   find $\begin{pmatrix} p \\ m \end{pmatrix}$ minimizing $\sum_i p_i + \sum_i m_i$ under the constraints $\begin{pmatrix} A & -A \end{pmatrix}\begin{pmatrix} p \\ m \end{pmatrix} = f$ and $p, m \geq 0$
6. Return $\sum_k (p_k - m_k) a_k \boldsymbol{e}_{i_k} b_k$

About the ℓ_1-relaxation

- With the 1-norm, $x\boldsymbol{e}_1 + y\boldsymbol{e}_2 + z\boldsymbol{e}_3$ is smaller than $35z\boldsymbol{e}_4 - \boldsymbol{e}_5$.
- Experimentally, the algorithm can still find shorter proofs than the best computer proofs
- In practice, in many examples the coefficients are small, bringing the two sparsity measures closer together
- In particular, a lot of examples are totally unimodular (e.g. pure difference binomials)
- Then the coefficients of minimal representations are 0 or ±1
- In that case the algorithm is guaranteed to return a sparsest solution

- In the other direction, the linear programming approach opens the way to thinner metrics
- For example, it is possible to weigh the 1-norm with the degree of the terms

Experimental data

Example	#gens	deg	GB	SigGB	LP	Mtx size	Pruning ratio
SVD	32	3	51	39	25	118 k × 328 k	0.83
ROL	28	5	80	39	30	22 k × 56 k	0.55
ROL-2	28	5	20	21	15	23 k × 60 k	0.56
ROL-3	28	5	49	44	31	18 k × 46 k	0.53
ROL-4	28	5	59	46	33	64 k × 137 k	0.58
ROL-5	28	5	28	30	22	31 k × 80 k	0.60
ROL-6	28	5	39	39	30	21 k × 55 k	0.56
ROL-7	40	9	85	23	17	17 k × 46 k	0.54
ROL-8	44	7	241	19	17	249 k × 560 k	0.58
Hartwig-4	23	15	316	54	46	349 k × 1 460 k	0.84
Hartwig-5	26	15	99	43	35	398 k × 1 374 k	0.84
Hartwig-6	24	15	86	33	29	217 k × 808 k	0.84
Ker	12	3	49	34	23	51 k × 129 k	0.90
SMW	36	7	63	42	39	44 k × 94 k	0.83
Sum	20	3	313	178	85	11 k × 17 k	0.93

Conclusion

What we presented

- New approach for computing short proofs of ideal membership
- Generalization of Min-RVLS to algebraic systems
- Combination of signature techniques and linear programming
- Flexible for other metrics
- Also works in the commutative case

Future work

- Choice of a signature ordering
- More efficient representations using additional generators ("lemmas")

More details and references

- Hofstadler and Verron, *Signature Gröbner bases, bases of syzygies and cofactor reconstruction in the free algebra* (JSC 2022) `ArXiV:2107.14675`
- Hofstadler and Verron, *Signature Gröbner bases in free algebras over rings* (ISSAC 2023) `ArXiV:2302.06483`
- Hofstadler and Verron, *Short proofs of ideal membership*, `ArXiv:2302.02832`

Thank you for your attention!