Computational Complexity of Polynomial Subalgebras

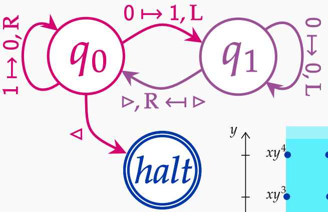
MAX PLANCK INSTITUTE
FOR MATHEMATICS
IN THE SCIENCES

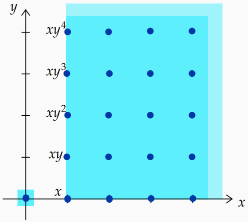
Leonie Kayser

leokayser.github.io

July 29, 2025

ISSAC'25





The dessert menu

Computational complexity

Subalgebra membership

Monomial and initial algebras

Mathematicians always have problems

Definition (Computational problem, Decision problem)

A **computational problem** consists of an input, e.g. a tuple of data, and a question or expected output. A **decision problem** has output `yes` or `no`.

- Input/output encoded over **finite alphabet $\boldsymbol{\Sigma}$**, $\Sigma^* := \{\text{strings over } \Sigma\}$
- Decision problems are just subsets $A \subseteq \Sigma^*$ (the "`yes`"-instances)

Definition (Ideal membership problem $\texttt{IdealMem}_K$)

Input: $f_1, \ldots, f_s, g \in \boldsymbol{R} := K[x_1, \ldots, x_n]$

Question: $g \in \langle f_1, \ldots, f_s \rangle_R$? (Decision problem)

Output: $h_1, \ldots, h_s \in R$ with $g = h_1 f_1 + \cdots + h_s f_s$ (Representation problem)

The Turing model of computation

Definition (Turing machine)

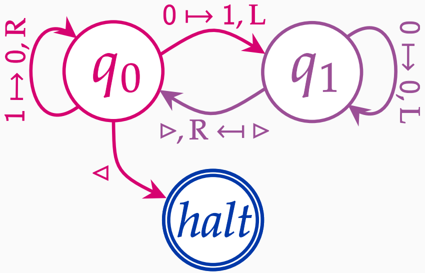
A **deterministic Turing machine** M (DTM) consists of

i) a finite set of **states** $\boldsymbol{Q}$, including an initial state q_0 and final states $F \subseteq Q$;

ii) a **tape alphabet** $\boldsymbol{\Gamma}$ containing the in/output alphabet;

iii) a **transition function** $\boldsymbol{\delta}\colon Q \times \Gamma \to Q \times \Gamma \times \{\mathrm{L}, \mathrm{R}\}$.

$$\begin{pmatrix} \text{current state,} \\ \text{read tape symbol} \end{pmatrix} \overset{\delta}{\mapsto} \begin{pmatrix} \text{next state,} \\ \text{overwrite symbol,} \\ \text{move left/right} \end{pmatrix}$$



▷ steps ≈ time, tape ≈ memory

Through time and space

Definition (TIME and SPACE)

Let $f : \mathbb{N} \to \mathbb{N}$ be a function $\geq \log n$.

i) $\mathrm{TIME}(f) = \{$decision prob. $A \mid \exists$DTM M deciding $w \in A$ in $O(f(|w|))$ steps$\}$

ii) $\mathrm{SPACE}(f) = \{A \mid \exists$DTM M deciding $w \in A$ using $O(f(|w|))$ cells$\}$

$$\mathrm{P} = \bigcup_k \mathrm{TIME}(n^k) \overset{?}{\subseteq} \mathrm{NP} = \bigcup_k \mathrm{NTIME}(n^k)$$
$$\subseteq \mathrm{PSPACE} = \bigcup_k \mathrm{SPACE}(n^k) \subsetneq \mathrm{EXPSPACE} = \bigcup_k \mathrm{SPACE}(2^{n^k})$$

Theorem (Hermann 1926, Mayr & Meyer 1982, Mayr 1989)

i) *If* $g = h_1 f_1 + \cdots + h_s f_s$, *then* $\exists (h_i)_i$ *with* $\deg h_i \leq \deg g + (s \cdot \max_i \deg f_i)^{2^n}$.

ii) $\texttt{IdealMem}_{\mathbb{Q}} \in \mathrm{EXPSPACE}$. *One can compute some* $(h_i)_i$ *in space* $2^{O(|w|)}$.

For sake of completeness

Definition (Karp-reduction, hardness & completeness)

Let $A \subseteq \Sigma^*$, $B \subseteq \Delta^*$ be decision problems.

i) $A \leq_{\mathbf{m}}^{\mathbf{P}} B$ if there is a "simple" function $f\colon \Sigma^* \to \Delta^*$ with $w \in A \Leftrightarrow f(w) \in B$.

ii) B is **hard** for a complexity class $\mathcal{C}$ if $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ for all $A \in \mathcal{C}$.

iii) B is **complete** for a complexity class $\mathcal{C}$ if $B \in \mathcal{C}$ and hard for $\mathcal{C}$.

- Reduction embeds problem A into problem B, "A is at most as difficult as B"
- Cook-Levin theorem: `3SAT` is NP-complete; stepping stone for hardness results

Theorem (Mayr & Meyer 1982, Mayr 1989)

i) *Hermann's degree bound* $O((sd)^{2^n})$ *for certificates* $(h_i)_i$ *is sharp.*

ii) $\mathtt{IdealMem}_{\mathbb{Q}}$ *is* $\mathrm{EXPSPACE}$*-complete, even for binomial ideals.*

The scary doubly-exponential examples

Theorem (Dubé 1990, Kühnle & Mayr ISSAC'96)

Let $I = \langle f_1, \ldots, f_s \rangle_{K[x_1,\ldots,x_n]}$ be an ideal and $d = \max_i \deg f_i$. The reduced Gröbner basis $G = \{g_i\}_i$ of I (w.r.t. any monomial order) has degree

$$\deg g_i \leq 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}.$$

One can enumerate the reduced Gröbner basis in exponential working space.

Theorem (Huynh 1986, my MA thesis 2022)

i) *There are ideals in $K[x_1, \ldots, x_n]$ generated by $O(n)$ polynomials of degree $O(1)$, whose reduced Gröbner basis has at least 2^{2^n} elements and degree $\geq 2^{2^n}$.*

ii) *Membership in the reduced Gröbner basis is $\mathrm{EXPSPACE}$-complete.*

The (not so) ideal world

Theorem (Mayr 1989, 1997)

$\texttt{IdealMem}_{\mathbb{Q}}$ *restricted to homogeneous polynomials is* PSPACE*-complete.*

- Gröbner bases can still be doubly-exponential even for homogeneous ideals
- Deciding whether $1 \in \langle f_1, \ldots, f_s \rangle_R$ (the "Nullstellensatz") is also in PSPACE, in fact low in the Polynomial Hierarchy (though at least NP-hard)
- Bounding the number of variables also drops the complexity to PSPACE
- There are dimension-dependent degree bounds available [Mayr & Ritscher 2013]
- The complexity of computing Gröbner bases seems to be linked to its Castelnuovo-Mumford regularity [Bayer & Mumford 1993]

The dessert menu

Computational complexity

Subalgebra membership

Monomial and initial algebras

Subgalgebra Analogue to Membership Problem for Ideals (SAMPI)

Definition (Subalgebra membership problem $\texttt{AlgMem}_K$)

Input: $f_1, \ldots, f_s, g \in K[x_1, \ldots, x_n]$

Question: $g \in K[f_1, \ldots, f_s]$? (Decision problem)

Output: $p \in K[t_1, \ldots, t_s]$ with $g = p(f_1, \ldots, f_s)$ (Certification problem)

Some questions:

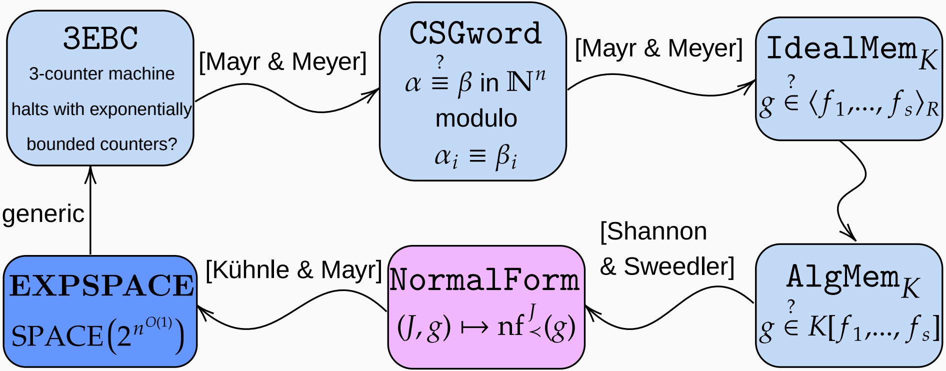
i) Degree bounds on p depending on $n, s, \deg f_i$?

ii) Upper and lower bounds on complexity of $\texttt{AlgMem}_{\mathbb{Q}}$? Related to $\texttt{IdealMem}_{\mathbb{Q}}$?

iii) Easier when the polynomials are homogeneous? Or monomials? Or n bounded?

iv) The analogue to Gröbner bases for ideals are SAGBI bases for subalgebras. What is the complexity of SAGBI bases?

A chain of reductions



Subalgebra membership using normal forms

- Given $f_1, \ldots, f_s, g \in K[x_1, \ldots, x_n]$, want to check if $g \in K[f_1, \ldots, f_n]$
- Consider the ideal $J = \langle f_1 - t_1, \ldots, f_s - t_s \rangle \subseteq K[\boldsymbol{x}, t_1, \ldots, t_s]$
- Let $\prec$ be a mon. order on $K[\boldsymbol{x}, \boldsymbol{t}]$ such that $x_i \succ \boldsymbol{t}^\alpha$ for all $x_i, \boldsymbol{t}^\alpha$, e.g. $\prec_{\text{lex}}$
- The normal form $\mathrm{nf}_\prec^J(g)$ is the unique $g' \in g + J$ such that no term in g' is divisible by the leading term of any element of J

Theorem (Shannon & Sweedler 1986, attributed to Spear)

$g \in K[f_1, \ldots, f_s]$ *if and only if* $p := \mathrm{nf}_\prec^J(g) \in K[\boldsymbol{x}, \boldsymbol{t}]$ *is in* $K[\boldsymbol{t}]$.
In this case, considering p *as a polynomial in* $t_1, \ldots, t_s$*, one has* $g = p(f_1, \ldots, f_s)$.

$\rightsquigarrow$ Reduces subalgebra membership to normal form calculation

The upper bound

Theorem (K. 2025)

$\texttt{AlgMem}_{\mathbb{Q}}$ *is in* $\mathrm{EXPSPACE}$ *and* $\texttt{AlgMem}_{\mathbb{Q}}(\text{homog})$ *is in* PSPACE.
A certificate $p \in \mathbb{Q}[t_1, \ldots, t_s]$ *can be computed using* $2^{O(|w|)}$ *working space.*

Proof idea. Combine the previous elimination method with the exponential working space algorithm for normal forms by [Kühnle & Mayr 1996]. □

- Careful analysis reveals that the bounded variable case is also in PSPACE
- We also get a degree bound for the certificate using the Dubé bound:

Theorem (K. 2025)

If $g \in K[f_1, \ldots, f_s]$, $e := \deg g$, *then there is a* p *with* $p(f_1, \ldots, f_s) = g$ *of degree*

$$\deg p \le e + \left(\left(\tfrac{1}{2} d^{2s^2} + d \right)^{2^n} + 1 \right)^{(n+s)^2+1} e^{n+s} \approx d^{O((n+s)^4 2^n)} e^{n+s}.$$

The exponential space lower bound

Lemma (K. 2025)

Let $f_1, \dots, f_s, g \in R = K[x_1, \dots, x_n]$*, then the following are equivalent:*

i) $g \in \langle f_1, \dots, f_s \rangle_R$;
ii) $ug \in A \coloneqq K[x_1, \dots, x_n, uf_1, \dots, uf_s] \subseteq R[u]$.

The minimal degree of $p \in K[t_1, \dots, t_{n+s}]$ *with* $p(x_1, \dots, uf_s) = ug$ *is one less than the minimal degree of a representation* $\max_i \deg h_i$*.The minimal number of terms of* p *coincides with the minimal total number of terms of* $h_1, \dots, h_s$*.*

Theorem (K. 2025)

i) $\texttt{IdealMem}_{\mathbb{Q}} \leq_m^{\mathrm{P}} \texttt{AlgMem}_{\mathbb{Q}}$*, thus* $\texttt{AlgMem}_{\mathbb{Q}}$ *is* $\mathrm{EXPSPACE}$*-complete.*
ii) *Similar for homogen. polynomials,* $\texttt{AlgMem}_{\mathbb{Q}}(\text{homog})$ *is* PSPACE*-complete.*

Worst-case examples for subalgebra membership

Corollary (The Mayr–Meyer algebras)

For every n, there exists polynomials $f_1, \ldots, f_s, g \in K[x_1, \ldots, x_{O(n)}]$, $s \in O(n)$, such that

- $\deg f_i, \deg g \leq 6$,
- *each f_i, g has at most two terms (single variable or binomial),*
- *$g \in K[f_1, \ldots, f_s]$, but every $p \in K[t_1, \ldots, t_s]$ with $p(f_1, \ldots, f_s) = g$ has degree and number of terms at least 2^{2^n}.*

If the f_i, g are homogeneous (degree $O(n)$), then one can still archieve 2^n terms.

Idea. Build counter machine as a commutative semigroup, embed into subalgebra

The binary counting subalgebra

- Tape content $b_1 \cdots b_n \in \{0,1\}^n$, state q_i, head position j, $\hat{=}\ q_i h_j x_{1,b_1} \cdots x_{n,b_n}$

$$
\begin{aligned}
\mathcal{T} = \{q_0, q_1\} \,\dot\cup\, \{h_0, \ldots, h_n\}, \quad \boldsymbol{x} = \{x_{1,0}, x_{1,1}, \ldots, x_{n,0}, x_{n,1}\}, \\
\mathcal{R} &:= \{\, q_0 h_i x_{i,0} - q_1 h_{i-1} x_{i,1} \mid 1 \le i \le n \,\} \\
&\quad \cup \{\, q_0 h_i x_{i,1} - q_0 h_{i+1} x_{i,0} \mid 1 \le i \le n-1 \,\} \\
&\quad \cup \{\, q_1 h_i x_{i,0} - q_1 h_{i-1} x_{i,0} \mid 1 \le i \le n \,\} \\
&\quad \cup \{\, q_1 h_0 - q_0 h_1 \,\}, \\
A &:= \mathbb{K}[f_1, \ldots, f_{5n}] := \mathbb{K}[\mathcal{R} \cup \boldsymbol{x}], \\
g &:= q_0 h_1 x_{1,0} \cdots x_{n,0} - q_0 h_n x_{1,0} \cdots x_{n-1,0} x_{n,1}.
\end{aligned}
$$

The dessert menu

Computational complexity

Subalgebra membership

Monomial and initial algebras

The McNugget problem

Theorem (K. 2025)

$\texttt{IdealMem}_{\mathbb{Q}}$ restricted to monomial algebras is NP-complete.
This is still true if $d \leq n$ or the univariate case[1].

- Here p can be chosen to be a monomial, this reduces to a problem in $(\mathbb{N}^n, +)$
- The univariate case is "exactly" the NP-complete change-making problem

$$x^{43} \overset{?}{\in} \mathbb{Q}[x^6, x^9, x^{20}] \quad \Leftrightarrow \quad 43 = 6a + 9b + 20c,\ a, b, c \in \mathbb{N}$$

- Problem is in NP, one can easily verify p; hardness from combinatorics/ILPs

[1] But only with binary exponent encoding: $|\texttt{enc}(x^e)| \approx \log_2 e$. With unary encoding in TC^0.

SAGBI bases are complicated . . .

Definition (Initial algebra, SAGBI basis)

Given monomial order $\prec$ and subalgebra $A \subseteq K[x_1, \ldots, x_n]$, the **initial algebra** is

$$\mathrm{in}_\prec(A) := K[\{\, \mathrm{in}_\prec(g) \mid g \in A \setminus 0 \,\}]$$

A **SAGBI basis** of A is a set $S \subseteq A$ whose initial monomials generate $\mathrm{in}_\prec(A)$.

- Not every subalgebra $K[f_1, \ldots, f_s] \subseteq K[\boldsymbol{x}]$ has a finitely gen'd initial algebra

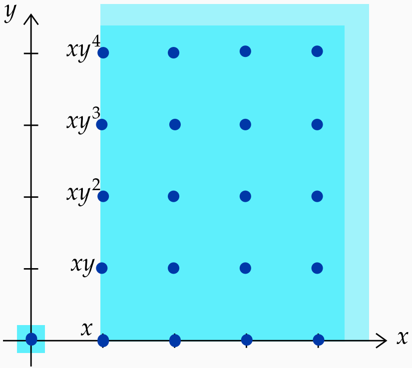
$$A = K[x, xy - y^2, xy^2], \qquad \rightsquigarrow \qquad \mathrm{in}_\prec(A) = K[x, xy, xy^2, xy^3, xy^4, \ldots]$$

- No known general criterion on finiteness of SAGBI bases
- Conjecture: The finiteness problem is computationally hard

Theorem (Robbiano & Sweedler 1990)

$\mathtt{SAGBIfinite}_K$ *is semi-decidable using the subduction algorithm.*

. . . but may have interesting structure?



$$\mathrm{in}_<(A) = 1K + xK[x,y]$$
$$= \{0\} \cup \left(e_1 + \mathbb{N}^2\right)$$

Definition (Affine-linear set, semilinear set)

i) An **affine-linear set** $X \subseteq \mathbb{Z}^n$ has the form $X = v_0 + \langle v_1, \ldots, v_m \rangle_{\mathbb{N}}$, $v_i \in \mathbb{Z}^n$.

ii) A **semilinear set** $X \subseteq \mathbb{Z}^n$ is a finite union of affine-linear sets.

The semilinearity conjecture

Semilinearity conjecture (K. & Reinke 2025+)

The initial monomials of a finitely generated subalgebra form a semilinear set.

- Clearly true if $\mathrm{in}_\prec(A)$ is finitely generated (even linear set)
- All known examples seem to have this structure
- Not true for “wild” monomimal orders, need “reasonable” orders

Theorem (K. & Reinke 2025+)

Let $G \leq \mathrm{GL}(\mathbb{Z}^n)$ be a finite group, $M \subseteq \mathbb{Z}^n$ an affine semigroup invariant under G and $\prec$ a rational weight order. Then the semilin. conjecture holds for $A = K[M]^G$.

- Idea: Semilinear sets are exactly sets in $\mathbb{N}^n$ described by Presburger formulas
- Can define initial algebra membership here as Presburger formula

Hope: Decide `SAGBIfinite` using effective semilinear presentation of $\mathrm{in}_\prec(A)$!

Thank you! Questions?