The Computational Complexity of Subalgebra Membership

MAX PLANCK INSTITUTE
FOR MATHEMATICS
IN THE SCIENCES

Leonie Kayser

leo.kayser@mis.mpg.de

December 14, 2023

Nonlinear Algebra Seminar

Table of Contents

Computational problems

Definition (Computational 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 $\mathtt{yes}$ or $\mathtt{no}$.

- If there is a unique output (e.g. for decision problems), then this is just a function
- For theoretical and practical purposes the input/output needs to be suitably encoded over some **finite alphabet** Σ; the set of strings of characters is Σ^*
- Decision problems are just subsets $A \subseteq \Sigma^*$ (the "yes"-instances)
- Assume that the input is syntactically correct (actually encodes a number/graph/...)
- **Output complexity:** How long is the (shortest) output compared to $|w|$?

The Turing model of computation

Definition (Turing machine)

A **deterministic Turing machine** M (TM/DTM for short) 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 alphabets and a blank $\square \in \Gamma$;
iii) a **transition function** $\boldsymbol{\delta}\colon (Q \setminus F) \times \Gamma \to Q \times \Gamma \times \{\mathrm{L}, \mathrm{R}\}$.

A **non-deterministic TM** instead has $\delta\colon (Q \setminus F) \times \Gamma \to \mathcal{P}(Q \times \Gamma \times \{\mathrm{L}, \mathrm{R}\})$.

- Configuration = (current tape $(\gamma_i)_{i \in \mathbb{Z}}$, head position $i \in \mathbb{Z}$, state $q \in Q$)
- Initial configuration = (input surrounded by $\square$'s, head in position 0, $q = q_0$)
- δ defines transitions between configurations $c \vdash_M c'$
- DTMs are "roughly" equivalent to computers (steps $\approx$ time, tape $\approx$ 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) $\mathrm{NTIME}(f) = \{A \mid \exists$non-determ. TM M deciding $w \in A$ in $O(f(|w|))$ steps$\}$

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

- $\mathrm{TIME}(f) \subseteq \mathrm{NTIME}(f) \subseteq \mathrm{SPACE}(f) \subseteq \mathrm{TIME}(2^{f(n)})$
- Hierarchy theorems: If $f_1 \in o(f_2)$ (+ technicalities), then

$$\mathrm{TIME}(f_1) \subsetneq \mathrm{TIME}(f_2 \log f_2), \qquad \mathrm{SPACE}(f_1) \subsetneq \mathrm{SPACE}(f_2)$$

- Important complexity classes

$$\mathrm{P} = \bigcup_k \mathrm{TIME}(n^k), \quad \mathrm{NP} = \bigcup_k \mathrm{NTIME}(n^k), \quad \mathrm{PSPACE} = \bigcup_k \mathrm{SPACE}(n^k), \ \ldots$$

For sake of completeness

Definition (Polynomial-time many-one reduction, hardness & completeness)

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

i) $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ if there is a function $f\colon \Sigma^* \to \Delta^*$ in FP 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 $\mathcal{C}$.

- Informally: Karp-reductions embed/translate problem A into problem B
- $\leq_{\mathrm{m}}^{\mathrm{P}}$ is reflexive & transitive, formalizes "A is at most as difficult to decide as B"
- Many classes are closed under reduction, i.e. $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ and $B \in \mathcal{C} \Rightarrow A \in \mathcal{C}$
- Cook-Levin theorem: `3SAT` is NP-complete; stepping stone for hardness results

Table of Contents

Representing polynomials on a computer

Need to encode polynomials $f = \sum_{|\alpha| \le d} c_\alpha \boldsymbol{x}^\alpha \in K[x_1, \ldots, x_n]$.

- Fix encoding enc of K, e.g. $\operatorname{bin}(a) / \operatorname{bin}(b)$ for $\frac{a}{b} \in \mathbb{Q}$ or $\{\mathsf{a}_1, \ldots, \mathsf{a}_q\}$ for $\mathbb{F}_q$
- There are two ways of representing a monomial $\boldsymbol{x}^\alpha$: **exponential** or **unary**

$$\mathtt{X}_1\, \hat{}\, \operatorname{bin}(\alpha_1) \ldots \mathtt{X}_n\, \hat{}\, \operatorname{bin}(\alpha_n) \qquad \text{vs} \qquad \underbrace{\mathtt{X}_1 \ldots \mathtt{X}_1}_{\alpha_1 \text{ times}} \ldots \underbrace{\mathtt{X}_n \ldots \mathtt{X}_n}_{\alpha_n \text{ times}}$$

- Unary encoding ensures that $|\operatorname{enc}(\boldsymbol{x}^\alpha)| \ge \deg \boldsymbol{x}^\alpha$
- To encode the terms of f, list...
  - *all* terms of degree $\le \deg f$ with their coeffients (**dense**)
  - or only those with nonzero coeffients (**sparse**)
- Dense encoding ensures $|\operatorname{enc}(f)| \ge \binom{n+d}{n}$, in particular

$$|\text{exponential+sparse}| \le |\text{unary+sparse}| \le |\text{unary+dense}| = O(|\text{exponential+dense}|)$$

Ideal membership

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

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

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

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

Theorem (Hermann 1926, Mayr & Meyer 1982)

If $g \in \langle f_1, \ldots, f_s \rangle_R$, *then there exist* $(h_i)_i$ *with* $\deg h_i \leq \deg g + (s \cdot \max_i \deg f_i)^{2^n}$.

Theorem (Mayr 1989)

One can compute a certificate using working space $2^{O(|w|)}$.

Caveat: The certificates are written to an output tape not counted as working space.

The CSG word problem hides in $\mathtt{IdealMem}_K$

Theorem (Mayr & Meyer 1982)

The word problem for finitely presented commutative semigroups $\mathtt{CSGword}$ *is* $\mathrm{EXPSPACE}$*-complete.*

Lemma ($\mathtt{CSGword} \leq_{\mathbf{m}}^{\mathrm{P}} \mathtt{IdealMem}_K$)

Let $\equiv$ be a congruence rel. on $\mathbb{N}^n$ generated by $\{\alpha_i \equiv \beta_i\}_i$, and $\alpha, \beta \in \mathbb{N}^n$. Then

i) $\alpha \equiv \beta$ *in the commutative semigroup* $\mathbb{N}^n / \equiv$ *if and only if*

ii) $\boldsymbol{x}^\alpha - \boldsymbol{x}^\beta \in \langle \{\boldsymbol{x}^{\alpha_i} - \boldsymbol{x}^{\beta_i}\}_i \rangle_{K[x_1,\ldots,x_n]}$.

Theorem (Mayr & Meyer 1982, Mayr 1989)

$\mathtt{IdealMem}_{\mathbb{Q}}$ *is* $\mathrm{EXPSPACE}$*-complete, even for dense encodings.*

Hermann's degree bound for certificates $(h_i)_i$ is (essentially) sharp.

The scary doubly-exponential examples

Theorem (Dubé 1990, Kühnle & Mayr 1996)

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. an arbitrary 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)

Ther 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 $\geq 2^{2^n}$. Membership in the reduced Gröbner basis is $\mathrm{EXPSPACE}$-complete.

Not all is lost

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 also dimension-dependent degree bounds available
- The complexity of computing Gröbner bases seems to be linked to its Castelnuovo-Mumford regularity [Bayer & Mumford 1993]

Table of Contents

Big questions

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

Input: $f_1, \dots, f_s, g \in R = K[x_1, \dots, x_n]$

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

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

Some questions (followed by partial answers):

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

ii) Upper and lower bounds on complexity of $\mathtt{AlgMem}_{\mathbb{Q}}$?

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?

Subalgebra membership using normal forms

- Given $f_1, \dots, f_s, g \in K[x_1, \dots, x_n]$, want to check if $g \in K[f_1, \dots, f_n]$
- Consider the ideal $J = \langle f_1 - t_1, \dots, f_s - t_s \rangle \subseteq K[\boldsymbol{x}, t_1, \dots, t_s]$
- 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. $\prec_{\mathsf{lex}}$
- 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)

$g \in K[f_1, \dots, f_s]$ *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* $t_1, \dots, t_s$*, one has* $g = p(f_1, \dots, f_s)$.

A first upper bound

Theorem

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

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

- More careful analysis should reveal that the homogeneous problem is in PSPACE
- We also get a degree bound for the certificate using the Dubé bound:

Theorem

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

$$\deg p \leq ((2n(d^2/2 + d)^{2^{n-1}})^n \deg g)^{n+1}.$$

The McNugget problem

Theorem

The subalgebra membership restricted to monomial algebras is NP*-complete.*
This is still true if one bounds the degrees, or one restricts to a single variable.

- Note in the last case a sparse+exp. encoding must be used (otherwise in L)
- Here p can be chosen to be a monomial, this reduces to a problem in $(\mathbb{N}^n, +)$
- The problem is in NP, as one can non-deterministically guess p
- The univariate case is "exactly" the NP-complete change-making problem

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

- For bounded degree one can reduce from a problem similar to `ILP`

A first lower bound

Theorem

$\texttt{AlgMem}_K$ *is* PSPACE*-hard, even when restricted to homogeneous generators.*

Proof idea. Inspired by the homogeneous ideal case [Mayr 1997].

- A LBA M is a Turing machine only using its input as working tape
- Assume M has tape alphabet $\Gamma = \{0, 1\}$ and states Q, input length n
- Consider $R = K[\{x_{i,0}, x_{i,1}, y_i\}_{1 \leq i \leq n} \cup Q]$
- Configuration $(w_1 \dots w_n \in \{0, 1\}^n, i, q) \mathrel{\hat{=}}$ monomial $x_{1,w_1} \cdots x_{n,w_n} y_i q$
- Generators are all $x_{i,j}$ and binomials reflecting the transition function
- The resulting subalgebra is $\mathbb{N}^2$-graded over $K[x_{i,j}]$ (by the y_i and Q variables)

$\rightsquigarrow$ This grading is used to prove the reduction $\texttt{LBAword} \leq_{\mathrm{m}}^{\mathrm{P}} \texttt{AlgMem}_K$ $\square$

What if I don't care about computational complexity?

Corollary

There exists polynomials $f_1, \ldots, f_s, g \in K[x_1, \ldots, x_{3n+O(1)}]$, $s \in O(n)$, *such that*

- *they are homogeneous with* $\deg f_i \leq 2$, $\deg g = n + 2$,
- $g \in K[f_1, \ldots, f_s]$,
- *each* f_i, g *has at most two terms, but*
- *every* $p \in K[t_1, \ldots, t_s]$ *with* $p(f_1, \ldots, f_s) = g$ *has at least* 2^n *terms!*

Proof. Build binary counter as an LBA and encode as subalgebra as previously!

Open questions about SAGBI bases

- The initial algebra $\mathrm{in}_\prec(A)$ is the subalgebra with basis consisting of initial monomials of polynomials in A
- A SAGBI basis of A is a subset of 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, e.g. the invariants $K[x_1, x_2, x_3]^{A_3} = K[e_1, e_2, e_3, \Delta]$
- No known general criterion on finiteness of SAGBI bases
- Conjecture: The finiteness problem is compuationally hard, maybe undecidable
- Initial algebra membership should be at least as difficult as subalgebra membership; in homogeneous case it is also PSPACE-complete

Thank you! Questions?