Computational Complexity of Polynomial Subalgebras

Leonie Kayser

Abstract

The computational complexity of polynomial ideals and Gröbner bases has been studied since the 1980s. In recent years, the related notions of polynomial subalgebras and SAGBI bases have gained more and more attention in computational algebra, with a view towards effective algorithms. We investigate the computational complexity of the subalgebra membership problem and degree bounds. In particular, we show completeness for the complexity class EXPSPACE and prove PSPACE-completeness for homogeneous algebras. We highlight parallels and differences compared to the settings of ideals, and also look at important classes of polynomials such as monomial algebras.

1 Introduction

Let $\mathbb{K}$ be a field equipped with a suitable encoding over a finite alphabet, for example, the rational numbers $\mathbb{Q}$ or a finite field $\mathbb{F}_q$. At the heart of many algorithms in computer algebra lie efficient algorithms manipulating polynomial ideals and Gröbner bases, dating back at least to the 1960s [5]. Since the late 1980s, algorithms for computations with subalgebras have been studied [29, 27], which have applications in toric degenerations and polynomial system solving [3]. A fundamental computational problem for ideals and subalgebras of polynomial rings $\mathbb{K}[\underline{x}] = \mathbb{K}[x_1, \dots, x_n]$ is deciding *membership*. Of special interest are classes C of polynomials such as homogeneous polynomials (Homog), monomials (Mon), or polynomials with bounded degree or number of variables.

IdealMem$_{\mathbb{K}}(\mathsf{C})$, IdealMem$_{\mathbb{K}}$	
Input:	$f_1, \dots, f_s \in \mathsf{C}$ (or $\mathbb{K}[\underline{x}]$); $g \in \mathbb{K}[\underline{x}]$
Output:	Is $g \in \langle f_1, \dots, f_s \rangle$?

AlgMem$_{\mathbb{K}}(\mathsf{C})$, AlgMem$_{\mathbb{K}}$	
Input:	$f_1, \dots, f_s \in \mathsf{C}$ (or $\mathbb{K}[\underline{x}]$); $g \in \mathbb{K}[\underline{x}]$
Output:	Is $g \in \mathbb{K}[f_1, \dots, f_s]$?

Recall that $g \in \langle f_1, \dots, f_s \rangle$ if and only if there is a representation $g = h_1 f_1 + \cdots + h_s f_s$ with $h_1, \dots, h_s \in \mathbb{K}[\underline{x}]$; the *representation degree* (of the tuple $f_1, \dots, f_s, g$) is the smallest possible value of $D = \max\{\deg h_1, \dots, \deg h_s\}$. Similarly, $g \in \mathbb{K}[f_1, \dots, f_s]$ if and only if $g = p(f_1, \dots, f_s)$ for some *certificate* $p \in \mathbb{K}[t_1, \dots, t_s]$; we call the smallest possible degree of p the *certification degree*.

The computational complexity and representation degree bounds of IdealMem$_{\mathbb{K}}$ and its variants have been studied since the 1980s, we give a brief overview in Section 2.3. The

complexity of algebras in a more general sense has been studied before [18], though so far not for the concrete case of polynomial subalgebras. This paper is concerned with filling this gap and proving analogous results for $\textsc{AlgMem}_{\mathbb{K}}$ and bounds on the certification degree. In order to obtain reasonable upper bounds on the computational complexity, we assume that arithmetic in the base field $\mathbb{K}$ can be performed efficiently; this is formalized as being *well-endowed* [4]. A main theorem is the EXPSPACE- and PSPACE-completeness of the subalgebra membership problem and the homogeneous variant, combining the upper bounds Theorem 3.2 and 3.6 and the complementing lower bound Theorem 4.3.

Theorem 1.1. *Over a well-endowed field $\mathbb{K}$, the subalgebra membership problem* $\textsc{AlgMem}_{\mathbb{K}}$ *is* EXPSPACE*-complete and the homogeneous version* $\textsc{AlgMem}_{\mathbb{K}}(\mathsf{Homog})$ *is* PSPACE*-complete.*

One of the goals of this paper is to be accessible both to commutative algebraists and computer scientists. For this reason, we introduce the relevant results from algebra and complexity theory on ideals and Gröbner bases in Section 2. In Section 3 we prove various upper bound results on variations of $\textsc{AlgMem}_{\mathbb{K}}$, as well as an upper bound on the certification degree. In Section 4 we present a complexity-theoretic reduction from $\textsc{IdealMem}_{\mathbb{K}}$ to $\textsc{AlgMem}_{\mathbb{K}}$, proving matching lower bounds. In Section 5 we study the case of monomial subalgebras, which is still NP-complete, and discuss related questions with SAGBI bases.

2 Background in algebra and complexity theory

2.1 Ideals, subalgebras and their bases

Let $\mathbb{K}$ be a field, denote by $\mathbb{K}[\underline{x}] \coloneqq \mathbb{K}[x_1, \ldots, x_n]$ the polynomial ring in n variables, consisting of finite linear combinations

$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha, \qquad x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \quad c_\alpha \in \mathbb{K}.$$

Ideals and subalgebras arise naturally in algebra as the kernels and images of ($\mathbb{K}$-linear) ring homomorphisms. We briefly recall the basic definitions for both of them in parallel.

Definition 2.1. A subset $I \subseteq \mathbb{K}[\underline{x}]$ is an *ideal* if it is an additive subgroup (contains 0 and is closed under addition and subtraction) and also closed under multiplication with *arbitrary* polynomials $f \in \mathbb{K}[\underline{x}]$. A subset $A \subseteq \mathbb{K}[\underline{x}]$ is a *subalgebra* if it is an additive subgroup containing $\mathbb{K}$ and is closed under multiplication within A. Given a set $S \subseteq \mathbb{K}[\underline{x}]$, we denote by

$$\langle S \rangle = \left\{ \sum_{\text{finite}} h_i f_i \;\middle|\; \begin{matrix} f_i \in S, \\ h_i \in \mathbb{K}[\underline{x}] \end{matrix} \right\} = \{ \text{ lin. comb. of } S \text{ over } \mathbb{K}[\underline{x}] \}$$

$$\mathbb{K}[S] = \left\{ \sum_{\text{finite}} c_\alpha f^\alpha \;\middle|\; \begin{matrix} f_i \in S, \\ c_\alpha \in \mathbb{K} \end{matrix} \right\} = \{ \text{ polynomial expressions in } S \}$$

the ideal and subalgebra generated by S; it is the smallest ideal resp. subalgebra containing S.

Example 2.2. An important class of ideals and algebras are those generated by monomials x^α, or binomials $x^\alpha - x^\beta$. For example, monomial algebras show up as coordinate rings of affine toric varieties, and binomial ideals are related to commutative Thue systems, capturing the combinatorial worst-case complexity of ideal membership (see Theorem 2.12).

Definition 2.3. A *monomial order* $\prec$ is a total order on the set of monomials x^α stable under multiplication ($x^\alpha \preceq x^\beta$ implies $x^\alpha x^\gamma \preceq x^\beta x^\gamma$) and such that $1 = x^0$ is the minimal element. The *initial term* $\operatorname{in}_\prec(f)$ of a nonzero polynomial $f = \sum_\alpha c_\alpha x^\alpha$ is the nonzero term $c_\alpha x^\alpha$ with the largest monomial. For convenience define $\operatorname{in}_\prec(0) = 0$. Given an ideal I or a subalgebra A, its initial ideal or initial algebra, respectively, is

$$\operatorname{in}_\prec(I) = \langle \{ \operatorname{in}_\prec(f) \mid f \in I \} \rangle, \quad \operatorname{in}_\prec(A) = \mathbb{K}[\{ \operatorname{in}_\prec(f) \mid f \in A \}].$$

In the following fix such a monomial order, for example, the *lexicographic order* $\prec_{\text{lex}}$; we may assume $x_1 > \cdots > x_n$.

Definition 2.4. A *Gröbner basis* of an ideal I is a *finite* subset $G \subseteq I$ such that $\operatorname{in}_\prec(I) = \langle \{ \operatorname{in}_\prec(g) \mid g \in G \} \rangle$. A Gröbner basis is *reduced* if the leading coefficients are 1 and no term of $g \in G$ is in $\operatorname{in}_\prec(G \setminus \{g\})$.

On the other hand, a *SAGBI basis* of a subalgebra A is *any* subset $S \subseteq A$ such that $\operatorname{in}_\prec(A) = \mathbb{K}[\{ \operatorname{in}_\prec(f) \mid f \in S \}]$.

In both cases, such bases generate I and A respectively, hence the (historical) name "basis". The reduced Gröbner basis of an ideal I is unique and has the smallest number of elements and smallest degree among all Gröbner bases of I. For more background on Gröbner bases see for example [7, Chapter 2], [15, Chapter 21] or [19, Chapter 2].

By *Hilbert's basis theorem*, every ideal can be generated by a finite set of polynomials; in fact one can find such a finite set in any generating set. This implies the existence of (finite) Gröbner bases for any ideal. On the other hand, finite SAGBI bases may not exist; we will come back to this topic in Section 5.1.

Definition 2.5. Given an ideal $I \subseteq \mathbb{K}[\underline{x}]$, the *normal form* $\operatorname{nf}_\prec(f, I)$ of an element $f \in \mathbb{K}[\underline{x}]$ against I is the unique polynomial $r \in f + I$ such that no monomial of r is in $\operatorname{in}_\prec(I)$ [19, Definition 2.4.8].

One can compute $\operatorname{nf}_\prec(f, I)$ by dividing f by a Gröbner basis G, the remainder is the normal form [7, Proposition 2.6.1]. This gives a membership test for polynomial ideals: $f \in I$ if and only if $\operatorname{nf}_\prec(f, I) = 0$.

2.2 Complexity theory

We use the Turing model of computation, though the details of this formalism are not required to follow this paper. Here we introduce the concepts and computational problems used in the

sequel. A classical reference for computational complexity theory is the book by Hopcroft and Ullman [14], a more modern treatment is the book by Arora and Barak [1], for a brief introduction with a view towards computer algebra, see also [15, Section 25.8].

Informally, the complexity of an algorithm is the amount of resources (time or memory) used in the computation as a function of the *input length*.

Definition 2.6. A *decision problem* A is the problem of deciding whether a given input $x \in \Sigma^* := \{\text{words over the alphabet } \Sigma\}$ has a certain property, i. e. deciding membership in the set $A \subseteq \Sigma^*$. Problems in P, PSPACE, and $\mathsf{EXPSPACE}$ can be solved algorithmically in polynomial time, polynomial space, and exponential space, respectively, while the answer to problems in NP can be *verified* in polynomial time provided a certificate.

One has the inclusions of complexity classes

$$\mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{PSPACE} \subsetneq \mathsf{EXPSPACE}.$$

A standard problem in NP is SAT, deciding whether a given boolean formula $\varphi(x_1, \dots, x_n)$ can be satisfied by some assignment $\{x_1, \dots, x_n\} \to \{\texttt{true}, \texttt{false}\}$. We will later need the useful variant 1IN3SAT (compare [28], also known as *positive/monotone* 1IN3SAT) and the UNBOUNDEDSUBSETSUM problem:

1IN3SAT	
Input:	$S_1, \dots, S_n \subseteq \mathbb{N}$, $\lvert S_i\rvert \leq 3$
Output:	Is there a set $T \subseteq \mathbb{N}$ such that $\lvert T \cap S_i\rvert = 1$ for all i?

UNBOUNDEDSUBSETSUM	
Input:	$a_1, \dots, a_s; b \in \mathbb{N}$
Output:	Is $\sum_{i=1}^{s} c_i a_i = b$ for some $c_1, \dots, c_s \in \mathbb{N}$?

A typical example of a problem in PSPACE is the halting problem for (deterministic) linearly bounded automata (LBA). Here a LBA M consists of a finite set of states Q including a starting state q_0 and a halting state q_{halt}, a tape alphabet $\Gamma = \{\texttt{0}, \texttt{1}, \triangleright, \triangleleft\}$ containing the input alphabet $\Sigma = \{\texttt{0}, \texttt{1}\}$, and a transition function

$$\delta \colon (Q \setminus \{q_{\text{halt}}\}) \times \Gamma \to Q \times \Gamma \times \{\mathrm{L}, \mathrm{R}\}.$$

A configuration is a triple $(q, i, b_0 b_1 \dots) \in Q \times \mathbb{Z} \times \Gamma^*$, and if $\delta(q, b_i) = (q', c, X)$, then M transitions as

$$(q, i, \dots b_{i-1} b_i b_{i+1} \dots) \Rightarrow \begin{cases} (q', i-1, \dots b_{i-1} c b_{i+1} \dots) & \text{if } X = \mathrm{L}, \\ (q', i+1, \dots b_{i-1} c b_{i+1} \dots) & \text{if } X = \mathrm{R}. \end{cases}$$

On the input string $w \in \Sigma^*$, the machine M starts on the starting configuration $(q_0, 1, \triangleright w_1 \dots w_n \triangleleft)$ (here $\triangleright$ is at position 0) and repeatedly transitions according to δ. The end markers $\triangleright, \triangleleft$ may never be overwritten and the head may not pass over them (e.g. $\delta(q, \triangleleft) = (q', \triangleleft, \mathrm{R})$ is not allowed). M halts if it eventually reaches a configuration of the form (q_{halt}, i, b).

LBAHALT	
Input:	A LBA $M = (Q, \delta, q_0, q_{\text{halt}})$ and an input $w \in \{\texttt{0}, \texttt{1}\}^*$
Output:	Does M halt on input w?

Example 2.7. The following table shows the transition function of a LBA consists of two states q_0, q_1 (plus a halting state), and on input $w \coloneqq \mathtt{0}\ldots\mathtt{0}$ (n zeros) will count in binary to $\mathtt{1}\ldots\mathtt{1}$ and then halt:

b	$\triangleright$	$\mathtt{0}$	$\mathtt{1}$	$\triangleleft$
q_0		$(q_1, \mathtt{1}, \mathrm{L})$	$(q_0, \mathtt{0}, \mathrm{R})$	halt
q_1	$(q_0, \triangleright, \mathrm{R})$	$(q_1, \mathtt{0}, \mathrm{L})$		

Transitions that do not occur (on input w) have been left unspecified for simplicity. An example of the transition sequence can be found at

mathrepo.mis.mpg.de/ComplexityOfSubalgebras/configurations.html

Definition 2.8. A *complexity upper bound* for a decision problem A and a complexity class C is an algorithm solving A and satisfying the resource constraints of C.

A *lower bound* or C-*hardness* result for A is a proof that the computation of any problem $A' \in \mathsf{C}$ can be reduced to the problem A. We use the notion of log-space many-one reductions:

Definition 2.9. For two sets $A \subseteq \Sigma^*$, $A' \subseteq (\Sigma')^*$, the problem A' is *log-space many-one reducible* to A, in symbols $A' \leq^{\mathsf{L}}_{\mathrm{m}} A$, if there is a map $f\colon (\Sigma')^* \to \Sigma^*$ computable in logarithmic working space, such that $x \in A'$ if and only if $f(x) \in A$.

A problem A is C-*hard*, if $A' \leq^{\mathsf{L}}_{\mathrm{m}} A$ for all A' in C. It is C-*complete* if it is also in C.

For example, Sat, 1in3Sat, and UnboundedSubsetSum are NP-complete, and LBA-halt is PSPACE-complete.

In the problems $\textsc{IdealMem}_{\mathbb{K}}$ and $\textsc{AlgMem}_{\mathbb{K}}$, the input consists of encoded polynomials over $\mathbb{K}$, for example as a string of characters. Choosing a reasonable representation, the input length is bounded below by the number of terms, the number of variables occurring, and, depending on the encoding, the coefficients and the (logarithm of the) degree.

Definition 2.10. The encoding of a polynomial $f = \sum_{|\alpha|\leq d} c_\alpha x^\alpha$ is *dense* if it lists all monomials with their coefficients (α, c_α) up to its degree, and *sparse* if it only lists those terms with non-zero coeffient. The representation of a monomial $x^\alpha \mathrel{\hat{=}} (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ is in *binary* if each α_i is encoded in binary, and *unary* if it is encoded in unary.

Example 2.11. The term $f = 42x_1^3x_3^6 \in \mathbb{Q}[x_1, x_2, x_3]$ could be encoded with binary exponents as $((11, 0, 110), \mathtt{enc}(42))$, and with unary as $((111, 0, 111111), \mathtt{enc}(42))$. In dense encoding, a representation of f would have to list all $\binom{9+3}{3} = 220$ monomials up to degree 9 (which most have coefficient 0), while a sparse encoding only has to list that one term.

All our complexity results will hold with respect to both dense and sparse encodings and binary or unary monomial representation (with the exception of Theorem 5.2), as long as we make the reasonable assumption that the field $\mathbb{K}$ is *well-endowed* [4]. Commonly used fields in computer algebra such as number fields and finite fields are well-endowed. For this reason, we will not elaborate further on the encoding.

2.3 The ideal world: brief summary of results

In this section, we give an overview of the complexity results regarding ideal membership, representation degree, and Gröbner basis degrees. Our upper bounds on $\textsc{AlgMem}_{\mathbb{K}}$ will rely on refined representation and Gröbner basis degree upper bounds presented below. A more comprehensive discussion of the complexity of ideals can be found in [26].

Theorem 2.12. *Let $\mathbb{K}$ be a well-endowed field (the lower bounds do not require this).*

(i) (Mayr & Mayer [24], Mayr [22]) *The problem* $\textsc{IdealMem}_{\mathbb{K}}$ *is complete for* EXPSPACE. *A representation can be enumerated in exponential working space.*

(ii) (Mayr [23]) *The problem* $\textsc{IdealMem}_{\mathbb{K}}(\mathsf{Homog})$ *is complete for* PSPACE. *The general problem is also in* PSPACE *when bounding the number of variables.*

All hardness results already hold for ideals generated by binomials $x^\alpha - x^\beta$.

Remark 2.13. Note that this uses the convention that in a computational problem with output, we only consider the working space and not the space needed to store the entire output. For example, one can enumerate the binary numbers $0, 1, \dots, 2^n - 1$ with only $\mathcal{O}(n)$ bits of working memory. Similarly, here the number of terms in a representation $(h_i)_i$ may be doubly exponential in the input length; this is unavoidable in the worst case [24].

Representation degree bounds are, in general, doubly exponential in the number of variables, which is asymptotically optimal. We also note the special case of complete intersections for later reference. For a definition of complete intersections see e. g. [7, Exercise 9.4.8] or [19, Definition 3.2.23].

Theorem 2.14. *Let $g \in \langle f_1, \dots, f_s \rangle \subseteq \mathbb{K}[x_1, \dots, x_n]$, $d \coloneqq \max_i \deg f_i$, and write $g = \sum_{i=1}^s h_i f_i$ with $h_i \in K[\underline{x}]$ of minimal representation degree $D \coloneqq \max_i \deg h_i$.*

(i) (Hermann [13], Mayr & Meyer [24]) $D \leq \deg g + (ds)^{2^n}$.

(ii) (Dickenstein, Fitchas, Giusti & Sessa [8]) *If $f_1, \dots, f_s$ define a complete intersection ideal, then $D \leq \deg g + d^s$.*

Both from a theoretical and computational point of view, effective degree bounds on *Gröbner bases* are important as well. We recall the classical *Dubé bound* as well as a dimension-refined version. Here, the dimension of an ideal $I \subseteq \mathbb{K}[\underline{x}]$ is the (Krull) dimension of the quotient ring $\mathbb{K}[\underline{x}]/I$, see [7, Chapter 9] for other characterizations of the dimension.

Theorem 2.15. *Let $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ be an ideal generated by $f_1, \dots, f_s$ of degree $d_i \coloneqq \deg f_i$, $d_1 \geq \cdots \geq d_s$, and consider any monomial order.*

(i) (Dubé [9]) *The degree of the reduced Gröbner basis GB of I, i. e. the largest degree of an element of GB, is bounded by*

$$\deg GB \leq 2 \left(\frac{1}{2} d_1^2 + d_1 \right)^{2^{n-1}}.$$

(ii) (Mayr & Ritscher [25]) *If I has dimension r, then the degree is bounded by*

$$\deg GB \leq 2\left(\frac{1}{2}(d_1 \cdots d_{n-r})^{2(n-r)} + d_1\right)^{2^r} \leq 2\left(\frac{1}{2}d_1^{2(n-r)^2} + d_1\right)^{2^r}.$$

These upper bounds are asymptotically sharp.

3 Upper bounds on subalgebra membership

In this section we provide various complexity upper bounds, that is, algorithms for variants of AlgMem$_{\mathbb{K}}$ which place these problems in PSPACE and EXPSPACE. Our complexity analysis of the membership problem for a subalgebra $A = \mathbb{K}[f_1, \ldots, f_s] \subseteq \mathbb{K}[\underline{x}]$ relies on the following classical elimination approach using tag variables, attributed to Spear [29, 30].

Let $\underline{t} = \{t_1, \ldots, t_s\}$ be additional variables, and consider an *elimination order* on $\mathbb{K}[\underline{x}, \underline{t}]$, i. e. a monomial order such that $x_i \succ t^\alpha$ for all x_i and $t^\alpha \in \mathbb{K}[\underline{t}]$, for example the lexicographical order $\prec_{\text{lex}}$.

Lemma 3.1 (Shannon & Sweedler [29])**.** *Let $f_1, \ldots, f_s, g \in \mathbb{K}[\underline{x}]$, $J \coloneqq \langle f_1 - t_1, \ldots, f_s - t_s\rangle$, then*

$$g \in \mathbb{K}[f_1, \ldots, f_s] \qquad \text{if and only if} \qquad p \coloneqq \operatorname{nf}_\prec(g, J) \in \mathbb{K}[\underline{t}].$$

If this is the case, then $g = p(f_1, \ldots, f_s)$, interpreting p as a polynomial in $t_1, \ldots, t_s$.

Subalgebra membership can thus be reduced to the task of calculating the normal form of a polynomial against an ideal in a larger polynomial ring. This approach is well-known, for example as a fall-back method in the `Macaulay2` [12] package `SubalgebraBases` [6]. Kühnle & Mayr [21] describe an exponential space algorithm for enumerating the normal form of a polynomial over a well-endowed field. Combining these results gives the first complexity upper bound:

Theorem 3.2. *For any well-endowed field $\mathbb{K}$, AlgMem$_{\mathbb{K}}$ is in EXPSPACE. Moreover a certificate $p \in \mathbb{K}[t_1, \ldots, t_s]$ such that $g = p(f_1, \ldots, f_s)$ can be output in exponential working space.*

Proof. Given $f_1, \ldots, f_s, g$, the algorithm computes the normal form $p \coloneqq \operatorname{nf}_\prec(g, J) \in \mathbb{K}[\underline{x}, \underline{t}]$ using Kühnle & Mayr's algorithm [21]. If there is a nonzero term in p involving some x_i, then $g \notin \mathbb{K}[f_1, \ldots, f_s]$. Otherwise, p is a certificate of subalgebra membership by Lemma 3.1, which can be enumerated to the output tape using single exponential working space.

Note that it might not be possible to fit the normal form in exponential working space as mentioned in Remark 2.13. Instead one has to enumerate the terms of p, which fit in exponential working space using and check for occurrences of x_i individually. □

To prove degree bounds and better complexity upper bounds for special classes of polynomials, we outline part of Kühnle & Mayr's upper bound constructions on normal forms [21].

Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal, $g \in \mathbb{K}[\underline{x}]$ and $\prec := \prec_{\text{lex}}$ the lexicographic order (for simplicity). Let $GB = GB(I)$ be the reduced Gröbner basis of I, then

$$\deg \operatorname{nf}_{\prec}(g, I) \leq \deg(g) + (\deg(GB) + 1)^{n^2+1} \deg(g)^n.$$

Let D be an upper bound on the degree of the coefficients $h_i \in K[\underline{x}]$ in a representation $g - \operatorname{nf}_{\prec}(g, I) = \sum_{i=1}^{s} h_i f_i$, for example the Hermann bound from Theorem 2.14, then Kühnle & Mayr reduce the normal form calculation into a linear algebra problem of size $\text{poly}(D) = D^{\mathcal{O}(1)}$. Using efficient parallel algorithms for matrix rank and the parallel computation hypothesis, this yields an algorithm in space $\text{polylog}(D) = (\log D)^{\mathcal{O}(1)}$. Using the Dubé bound for $\deg(GB)$ and the Hermann bound for D yields the mentioned exponential space algorithm for normal form calculation.

In our specialized setting $J = \langle t_1 - f_1, \ldots, t_s - f_s \rangle$ we have more refined upper bounds available regarding representation and Gröbner basis degrees. We apply this to the case of a fixed number of variables n and to the case of a fixed subalgebra A.

Theorem 3.3. *For a fixed subalgebra $A = \mathbb{K}[f_1, \ldots, f_s] \subseteq \mathbb{K}[\underline{x}]$ over a well-endowed field, the membership problem is in* PSPACE *(with respect to the input length of g). In fact, for a* fixed *number of variables n, we have* $\textsc{AlgMem}_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]) \in$ PSPACE.

Proof. The algorithm is the same as in Theorem 3.2, only the complexity analysis is slightly more elaborate. Using that normal form calculation with respect to a fixed ideal is possible in polynomial space, as remarked by Kühnle & Mayr [21, Section 6], the first assertion follows.

If only the number of variables $x_1, \ldots, x_n$ is fixed, then more care has to be taken, as the computation takes place in the ring $\mathbb{K}[x_1, \ldots, x_n, t_1, \ldots, t_s]$, whose number of variables $n + s$ still depends on the input length. However, the ideal $J = \langle t_1 - f_1, \ldots, t_s - f_s \rangle$ is a complete intersection of dimension n, hence using Theorem 2.15 its Gröbner basis degree is bounded above by

$$\deg GB(J) \leq G := 2 \left(\frac{1}{2} d^{2s^2} + d \right)^{2^n}.$$

Furthermore, the representation degree of $g - \operatorname{nf}_{\prec}(g, J)$ is bounded above by $D := G + d^s$ by Theorem 2.14. Since n is fixed, we see that D is single exponential in the input length, hence $\text{polylog}(D)$ is polynomial. This shows that the Meyer & Kühnle algorithm works in polynomial space for a bounded number of variables. □

Corollary 3.4. *If $g \in \mathbb{K}[f_1, \ldots, f_s] \subseteq \mathbb{K}[\underline{x}]$, then there exists a certificate $p \in \mathbb{K}[t_1, \ldots, t_s]$ with $g = p(f_1, \ldots, f_s)$ of degree*

$$\deg p \leq \deg(g) + \left(\left(\tfrac{1}{2} d^{2s^2} + d \right)^{2^n} + 1 \right)^{(n+s)^2+1} \deg(g)^{n+s}.$$

Proof. This is the degree bound on the normal form by Kühnle & Mayr evaluated for the ideal J (note that the ambient polynomial ring has $n + s$ variables). □

Remark 3.5. This degree can probably be improved by studying the derivation of the normal form degree bounds in this particular situation. We suspect that a "nicer" upper bound akin to the Hermann bound (Theorem 2.14) should hold.

Of great interest is the case of subalgebras generated by homogeneous polynomials. In this case, A is graded compatibly with the standard grading of the ambient ring.

Theorem 3.6. *For any well-endowed field* $\mathbb{K}$, $\textsc{AlgMem}_{\mathbb{K}}(\mathsf{Homog})$ *is in* PSPACE.

Proof. As a consequence of the grading, we see that a certificate p of lowest degree (if it exists) has degree at most $\deg g$. Thus either $\deg \operatorname{nf}_{\prec}(g, J) > \deg g$, in which case $g \notin K[f_1, \ldots, f_s]$, or $\deg \operatorname{nf}_{\prec}(g, J) \leq \deg g$ and $g \in \mathbb{K}[f_1, \ldots, f_s]$ if and only if $\operatorname{nf}_{\prec}(g, J) \in K[\underline{t}]$. This leads to a variation of the algorithm of Theorem 3.2 except we only attempt to compute the normal form up to degree $\deg g$. The complexity analysis is analogous to Theorem 3.3, noting that $\deg \operatorname{nf}_{\prec}(g, J) \leq \deg g$, hence a representation degree bound here is $D \coloneqq \deg g + d^s$. □

Remark 3.7. Degree bounds on certificates for elimination problems have been studied before, for example by Galligo & Jelonek [11]. Their results are not necessarily applicable here, as our ideal J has dimension n in a ring of $n + s$ variables, while the results of Galligo & Jelonek only apply to intersections of an ideal with $K[x_1, \ldots, x_n]$ if the ideal has dimension at least $n + 1$.

4 Lower bounds on subalgebra membership

In this section, we prove matching complexity lower bounds for the subalgebra membership problem and its homogeneous variant, relating them to the construction for homogeneous ideals. The hardness results for $\textsc{IdealMem}_{\mathbb{K}}$ and $\textsc{IdealMem}_{\mathbb{K}}(\mathsf{Homog})$ were constructed by embedding the word problem for commutative semigroups resp. its homogeneous variant into binomial ideals [24, 23]. We now describe how to embed (binomial) ideal membership into subalgebra membership.

Theorem 4.1. *Let* $f_1, \ldots, f_s, g \in \mathbb{K}[x_1, \ldots, x_n]$ *and let* t *be a new variable. The following are equivalent:*

(a) $g \in \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{K}[\underline{x}]$;

(b) $tg \in \mathbb{K}[tf_1, \ldots, tf_s, x_1, \ldots, x_s]$.

Proof. If $g = h_1 f_1 + \cdots + h_s f_s$ with $h_i \in \mathbb{K}[\underline{x}]$, then

$$tg = h_1 \cdot (tf_1) + \cdots + h_s \cdot (tf_s),$$

which certifies that tg is in $\mathbb{K}[tf_1, \ldots, tf_s, \underline{x}]$.

Conversely, assume $tg = p(tf_1, \ldots, tf_s, x_1, \ldots, x_n)$ with $p \in R \coloneqq \mathbb{K}[u_1, \ldots, u_s, x_1, \ldots, x_n]$. Declare a (non-standard) grading on R and $S = \mathbb{K}[t, x_1, \ldots, x_n]$ by giving $\deg t = \deg u_j = 1$ and $\deg x_i = 0$, so

$$R_d \coloneqq \bigoplus_{\substack{\alpha \in \mathbb{N}^s \\ |\alpha| = d}} u_1^{\alpha_1} \cdots u_s^{\alpha_s} \mathbb{K}[x_1, \ldots, x_n], \qquad S_d \coloneqq t^d \mathbb{K}[x_1, \ldots, x_n].$$

The evaluation homomorphism $R \to S$ substituting $x_i \mapsto x_i$, $u_j \mapsto t_j f_j$ respects this grading. Since $tg \in S_1$ is homogeneous of degree 1, decomposing p into its graded components $p = \sum_d p_d$ ($p_d \in R_d$) reveals that

$$p_d(tf_1, \ldots, tf_s, x_1, \ldots, x_n) = \begin{cases} p(tf_1, \ldots, x_n) = tg & \text{if } d = 1 \\ 0 & \text{if } d \neq 1. \end{cases}$$

Thus by replacing p by p_1, we may assume that every term in p involves exactly one u_j. Setting $t = 1$, we read

$$p(f_1, \ldots, f_s, x_1, \ldots, x_n) = g,$$

which, by the structure of p, is a representation for $g \in \langle f_1, \ldots, f_s \rangle$. □

Corollary 4.2. *Follow the notation from the previous theorem and set* $A \coloneqq \mathbb{K}[tf_1, \ldots, tf_s, \underline{x}]$.

(i) *The representation degree of* $g \in \langle f_1, \ldots, f_s \rangle$ *is one less than the certification degree of* $tg \in A$.

(ii) *The smallest possible number of non-zero terms of all* h_i *in a representation* $g = h_1 f_1 + \cdots + h_s f_s$ *equals the smallest possible number of terms of a certificate for* $tg \in A$.

Proof. The forward direction in the previous proof gives that the total degree and number of terms for representation of ideal membership are a lower bound for the respective values for the subalgebra (the total degree increases by 1 by attaching the u_j to the h_j). Conversely, the grading argument shows that if p is a certificate, then so is its graded component p_1, which has a lower or equal degree and number of terms. Finally, setting $t \mapsto 1$ in p_1 gives a representation for $g \in \langle f_1, \ldots, f_s \rangle$, showing the desired equalities. □

With this result we can deduce matching complexity lower bounds for subalgebra membership and its homogeneous variant. We can rephrase Theorem 4.1 as a complexity-theoretic reduction.

Theorem 4.3. *The map*

$$(f_1, \ldots, f_s; g \in \mathbb{K}[\underline{x}]) \;\mapsto\; (tf_1, \ldots, tf_s, x_1, \ldots, x_n; tg \in \mathbb{K}[t, \underline{x}])$$

provides a reduction $\textsc{IdealMem}_{\mathbb{K}} \leq_{\mathrm{m}}^{\mathsf{L}} \textsc{AlgMem}_{\mathbb{K}}$. *More generally, it provides a reduction* $\textsc{IdealMem}_{\mathbb{K}}(\mathsf{C}) \leq_{\mathrm{m}}^{\mathsf{L}} \textsc{AlgMem}_{\mathbb{K}}(\mathsf{C})$ *for any class of polynomials* C *containing single variables and closed under multiplication with variables.*

With this we can complete the proof of our main theorem.

Proof of Theorem 1.1. The complexity-theoretic upper bounds have been established in Theorem 3.2 and Theorem 3.6. The lower bounds now follow from the hardness of $\textsc{IdealMem}_{\mathbb{K}}$ and its homogeneous variant (Theorem 2.12) in conjunction with the reduction in Theorem 4.3. □

As mentioned in the beginning of this section, the complexity lower bounds for ideal membership were achieved by studying the word problem for commutative semigroups. Let $\mathcal{R} = \{(x^{\alpha_i}, x^{\beta_i})\}_{i=1}^{s}$ be a set of pairs of monomials, called *replacement rules*. Let $\equiv_{\mathcal{R}}$ be the congruence relation on $\mathsf{Mon}(\underline{x})$ generated by

$$x^{\gamma}x^{\alpha} \equiv_{\mathcal{R}} x^{\gamma}x^{\beta} \qquad (x^{\alpha}, x^{\beta}) \in \mathcal{R},\ x^{\gamma} \in \mathsf{Mon}(\underline{x}).$$

Concretely, two monomials m, m' are equivalent if one can be turned into the other by repeatedly replacing a factor $x^{\alpha} \mid m$ by the corresponding x^{β} or by replacing $x^{\beta} \mid m$ by x^{α}.

Word problem for Commutative Semigroups, CSG	
Input:	Replacement rules $\mathcal{R} = \{(x^{\alpha_i}, x^{\beta_i})\}_{i=1}^{s}$, Monomials $m, m' \in \mathsf{Mon}(\underline{x})$
Output:	Is $m \equiv_{\mathcal{R}} m'$?

Mayr & Meyer [24] prove EXPSPACE-hardness of CSG and provide a reduction CSG $\leq_{\mathrm{m}}^{\mathsf{L}}$ IdealMem$_{\mathbb{K}}$(Binom) via the map

$$(\mathcal{R}, m, m') \ \mapsto\ (x^{\alpha_1} - x^{\beta_1}, \ldots, x^{\alpha_s} - x^{\beta_s}; m - m').$$

More precisely, the minimal number of terms in a representation for this ideal membership problem equals the minimal number of replacement steps necessary in showing the congruence $m \equiv_{\mathcal{R}} m'$. Using the known double-exponential examples from [24], we can prove worst-case certification degree lower bounds for subalgebra membership. For an accessible exposition of the double-exponential lower bounds compare [2] or the author's Master's thesis [17].

Theorem 4.4. *For given k there exist polynomials $f_1, \ldots, f_s, g \in \mathbb{K}[x_1, \ldots, x_n]$ of degree ≤ 6, $n = \mathcal{O}(k)$, $s = \mathcal{O}(k)$, such that $g \in \mathbb{K}[f_1, \ldots, f_s]$, but every certificate $p \in \mathbb{K}[t_1, \ldots, t_s]$ has degree at least 2^{2^n} and at least 2^{2^n} terms. These f_i and g can be chosen as binomials and monomials.*

Proof. The CSG instances from [24] lead to ideal membership of $\mathcal{O}(k)$ binomials in $\mathcal{O}(k)$ variables of degree ≤ 5 (to obtain this exact degree bound, use the slightly improved degree bound from [2]) such that every representation has degree and number of terms bounded below by 2^{2^n}. Applying the reduction from Theorem 4.3, we obtain an instance of AlgMem$_{\mathbb{K}}$, whose smallest certificate p has the same number of terms and greater total degree by Corollary 4.2. □

Remark 4.5. Following [2], this construction can be easily adapted to prove lower bounds of the form d^{2^k} at the expense of increasing the algebra generator degree to $d + \mathcal{O}(1)$. This asymptotically matches the double-exponential upper bounds from Corollary 3.4. It would be interesting to get more refined lower bounds in terms of other properties of the algebra. For example, what could analogous statements of Theorem 2.14 and Theorem 2.15 be?

While the worst-case examples for CSG are too complicated to recall here, we can give more details in the homogeneous case. Here the certification degree can not blow up, however, we can still produce $\textsc{AlgMem}_{\mathbb{K}}(\mathsf{Homog})$ instances that require exponentially many terms in their certificates.

Theorem 4.6. *There exist a subalgebra $A = \mathbb{K}[f_1, \dots, f_{5n}] \subseteq \mathbb{K}[x_1, \dots, x_{3n+3}]$ generated by single variables and homogeneous binomials of degree ≤ 3, and a binomial g of degree $n+2$ with the following property: $g \in A$, but every polynomial $p \in \mathbb{K}[\underline{t}]$ with $g = p(f_1, \dots, f_{5n})$ has at least 2^{n+1} terms.*

Proof. The construction is based on the binary-counting LBA from Example 2.7. In [23, Theorem 17] Mayr describes how to reduce $\textsc{LBAHalt}$ to commutative semigroups/ideals, proving PSPACE-hardness of $\textsc{IdealMem}_{\mathbb{K}}(\mathsf{Homog})$. Applying our reduction (Theorem 4.3), we obtain a binary-counting subalgebra. The configuration $(q, i, b_0, \dots, b_{n+1})$ of the LBA is represented by the monomial $qh_i x_{0,\triangleright} x_{1,b_1} \cdots x_{n,b_n} x_{n+1,\triangleleft}$ and the replacement rules/binomial generators mimic the transition function δ.

We can simplity the resulting algebra significantly: We can remove redundant transitions (for example, we don't actually need $\triangleright, \triangleleft$ since the head position variable knows the current position), and the new variable t introduced in Theorem 4.1 can also be omitted, as the combined variables qh_i have a similar effect. This leads to the following subalgebra:

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

Then $g \in A$ by construction, since the binary counter will go from $(q_0, 1, \triangleright \mathtt{0} \dots \mathtt{0} \triangleleft)$ to $(q_0, 1, \triangleright \mathtt{1} \dots \mathtt{1} \triangleleft)$ and then walk to the right, erasing the $\mathtt{1}$'s until it reaches the configuration $(q_0, n, \triangleright \mathtt{0} \dots \mathtt{01} \triangleleft)$. On the way it writes every number $0, \dots, 2^{n-1}$ on the tape, taking at least 2 steps each time, for a total of $\geq 2^{n+1}$ steps. By Corollary 4.2 any certificate for $g \in A$ must essentially contain this derivation, hence has at least 2^{n+1} terms. □

An implementation of the homogeneous binary-counting subalgebra in `Macaulay2` can be found at `mathrepo.mis.mpg.de/ComplexityOfSubalgebras`.

5 Monomial subalgebras and SAGBI bases

In this final section, we consider the complexity of monomial algebra membership and consider some questions related to SAGBI bases. Monomial subalgebras A are $\mathbb{N}^n$-graded in the sense that

$$A = \bigoplus_{\substack{\alpha \in \mathbb{N}^n \\ x^\alpha \in A}} \mathbb{K} x^\alpha \subseteq \mathbb{K}[\underline{x}].$$

This has the useful consequence that a polynomial $\sum_\alpha c_\alpha x^\alpha$ is in A if and only if every monomial x^α, $c_\alpha \neq 0$, is in A. Furthermore, monomial algebras are related to linear programming and linear Diophantine equations [27, Remark 1.9], as

$$x^\beta \in K[x^{\alpha_1}, \ldots, x^{\alpha_s}] \quad \iff \quad \exists c \in \mathbb{N}^s \text{ s.t. } \beta = \sum_{i=1}^{s} c_i \alpha_s. \tag{1}$$

Theorem 5.1. *For any $\mathbb{K}$ the problem* AlgMem$_\mathbb{K}$(Mon) *is* NP*-complete. This is true even when restricting to square-free monomials.*

Proof. For NP membership one immediately reduces to the case where the polynomial to test f is a monomial due to the $\mathbb{N}^n$-grading. In Equation (1) we have $c_j \leq \max_i \beta_i$, so the bit length of c_j is bounded by the bit length of β. Hence, non-deterministically guessing c yields a NP-algorithm.

For NP-hardness, one can reduce from the NP-complete problem 1in3Sat (Section 2.2). Indeed, given sets $S_1, \ldots, S_n \subseteq \{1, \ldots, s\}$, then let $\alpha_1, \ldots, \alpha_s \in \{0,1\}^n$ be the integer vectors with $(\alpha_i)_j = 1$ when $i \in S_j$. Set $\beta = (1, \ldots, 1) \in \mathbb{N}^n$. Then Equation (1) encodes exactly the question for 1in3Sat, a solution corresponding to $T = \{\, i \mid c_i = 1 \,\}$. In this construction, all monomials x^{α_i}, x^β are square-free. □

We see that AlgMem$_\mathbb{K}$(Mon) is NP-complete even for polynomials of degree $\leq n$. The same is true if we instead bound the number of variables – if the exponents are encoded in binary.

Theorem 5.2. *The problem* AlgMem$_\mathbb{K}$(Mon$(x_1, \ldots, x_n)$) *for* fixed $n \geq 1$ *is* NP*-complete for binary exponent encoding and in* TC^0 *with unary encoding.*

Here $\mathsf{TC}^0 \subsetneq \mathsf{P}$ is a low uniform circuit complexity class. This model of computation solves a decision problem on input $b_1 \ldots b_n$ by evaluating a n-ary boolean function $f_{C_n}(b_1, \ldots, b_n)$. The function is described by a Boolean circuit C_n of size polynomial in n with a bounded number of layers. The gates of the circuits compute the boolean functions `not` and `and`, `or`, `maj` of any arity $\{0,1\}^n \to \{0,1\}$, where the majority gate is the function

$$\texttt{maj}(b_1, \ldots, b_n) = \begin{cases} 1 & \text{if } \#\{\, i \mid b_i = 1 \,\} \geq \frac{n}{2} \\ 0 & \text{otherwise.} \end{cases}$$

For more information on TC^0 and circuit complexity classes, see [31, Chapter 4].

Proof. Encoding the exponents as binary, the unary case $n = 1$ is a direct translation of the UnboundedSubsetSum problem, which is NP-hard.

On the other hand, if the monomials are encoded in unary, then a generating-function approach as in [16] provides a family of circuits in TC^0 deciding AlgMem$_K$(Mon$(x_1, \ldots, x_n)$). In more detail, Kane describes TC^0 circuits deciding the unary vector-valued subset sum problem, which corresponds to solutions of Equation (1) with $c_i \in \{0,1\}$. We can reduce the case of arbitrary $c_i \in \mathbb{N}$ to the $\{0,1\}$ case by replacing every generator x^{α_i} by $x^{\alpha_i}, x^{2\alpha_i}, x^{4\alpha_i}, \ldots, x^{2^\kappa \alpha_i}$,

$\kappa = \lfloor \log_2 |\beta| \rfloor$. Since the numbers are encoded in unary, the input size is proportional to $C = |\beta| + \sum_{i=1}^{s} |\alpha_i|$, and this larger generating set has size $\mathcal{O}(C^2)$.

Alternatively, one can apply a TC^0-variant of Courcelle's theorem to obtain TC^0-membership, compare [10, Theorem 13]. □

Remark 5.3. The NP-hardness results from Theorem 5.1 and 5.2 are in stark contrast to the analogous results for monomial *ideals*: Monomial ideal membership is computationally trivial, as $x^\beta \in \langle x^{\alpha_1}, \dots, x^{\alpha_s} \rangle$ if and only if component-wise $\beta \geq \alpha_i$ for some i.

5.1 Some remarks on SAGBI bases

We return to a general subalgebra $A = \mathbb{K}[f_1, \dots, f_s] \subseteq \mathbb{K}[\underline{x}]$ equipped with a monomial order $\prec$. In Section 2.1 we defined the concept of SAGBI bases $S \subseteq A$ as subsets with $\mathbb{K}[\{ \operatorname{in}_\prec f \mid f \in S \}] = \operatorname{in}_\prec A$. SAGBI stands for "Subalgebra Analog to Gröbner Bases for Ideals" [27] and they are used in practice for deciding subalgebra membership [6]. Much of the theory of Gröbner bases is paralleled for SAGBI bases, such as the *subduction algorithm* deciding subalgebra membership, reminiscent of the division algorithm for Gröbner bases [20, Section 6.6].

The previous results in this section provide a modest complexity lower bound of deciding subalgebra membership in the presence of SAGBI bases. The author is not aware of an analogous result for ideal membership given a Gröbner basis.

Corollary 5.4. *The problem* $\textsc{AlgMem}_K$ *is* NP*-hard, even if the input polynomials* $f_1, \dots, f_s$ *form a finite SAGBI basis of* $\mathbb{K}[f_1, \dots, f_s]$.

Proof. Subalgebras generated by a finite set S of monomials have S as a SAGBI basis. Hence Theorem 5.1 provides the NP lower bound. □

A major difference to the ideal world is that not every finitely generated subalgebra has a *finite* SAGBI basis.

Example 5.5. The subalgebra $\mathbb{K}[x_1, x_1x_2 - x_2^2, x_1x_2^2] \subseteq \mathbb{K}[x_1, x_2]$ has the non-finitely generated initial algebra $\mathbb{K}[\{ x_1x_2^k \mid k \geq 0 \}]$ for any monomial order with $x_1 \succ x_2$ [27, Example 4.11].

We therefore propose the study of the following two decision problems related to the initial algebra.

$\textsc{SAGBIfinite}_\mathbb{K}(\mathsf{C})$, $\textsc{SAGBIfinite}$	
Input:	$f_1, \dots, f_s \in \mathsf{C}$ (or $\mathbb{K}[\underline{x}]$)
Output:	Does $\mathbb{K}[f_1, \dots, f_s]$ have a finite SAGBI basis?

$\textsc{InAlgMem}_\mathbb{K}(\mathsf{C})$, $\textsc{InAlgMem}_\mathbb{K}$	
Input:	$f_1, \dots, f_s \in \mathsf{C}$ (or $\mathbb{K}[\underline{x}]$); $x^\alpha \in \mathsf{Mon}(\underline{x})$
Output:	Is $x^\alpha \in \operatorname{in}_\prec \mathbb{K}[f_1, \dots, f_s]$?

Robbiano & Sweedler showed that an algorithm somewhat analogous to Buchberger's algorithm for Gröbner bases can be used to enumerate a SAGBI basis, which will terminate if (and only if) A has a *finite* SAGBI basis. A procedure that returns `yes` if the output is yes, but never terminates if the output is no, is called a *semi-algorithm*, and a problem is *semi-decidable* or *recursively enumerable* if there is a semi-algorithm "solving" it.

Theorem 5.6 (Robbiano & Sweedler [27]). InAlgMem$_{\mathbb{K}}$ *and* SAGBIfinite$_{\mathbb{K}}$ *are semi-decidable (over a computable field).*

We are not aware of any general better complexity bounds, or even just if these problems are computable at all (though a negative answer would be quite surprising). Future work will provide a more detailed study of the structure and complexity of (infinitely generated) initial algebras.

Acknowledgments

I would like to thank my advisor, Simon Telen, as well as Markus Bläser, Peter Bürgisser, Florian Chudigiewitsch, and Fulvio Gesmundo for helpful discussions, in particular Florian for suggesting Courcelle's theorem for Theorem 5.2. I am also indebted to the anonymous reviewers, whose reports helped to improve the presentation and significantly simplify the treatment of Section 4. My interest in the complexity of ideals and subalgebras originated from my Master's thesis [17] supervised by Heribert Vollmer & Sabrina Gaube at Leibniz University Hannover.

References

[1] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge: Cambridge University Press, 2009. ISBN: 9780521424264. DOI: 10.1017/CBO9780511804090.

[2] David Bayer and Michael Stillman. "On the complexity of computing syzygies". In: *Journal of Symbolic Computation* 6.2 (1988), pp. 135–147. ISSN: 0747-7171. DOI: 10.1016/S0747-7171(88)80039-7.

[3] Barbara Betti, Marta Panizzut, and Simon Telen. "Solving equations using Khovanskii bases". In: *Journal of Symbolic Computation* 126 (2025), p. 102340. ISSN: 0747-7171. DOI: https://doi.org/10.1016/j.jsc.2024.102340.

[4] A. Borodin, S. Cook, and N. Pippenger. "Parallel computation for well-endowed rings and space-bounded probabilistic machines". In: *Information and Control* 58.1 (1983), pp. 113–136. ISSN: 0019-9958. DOI: 10.1016/S0019-9958(83)80060-6.

[5] Bruno Buchberger. "Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal". In: *Journal of Symbolic Computation* 41.3 (2006), pp. 475–511. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2005.09.007.

[6] Michael Burr et al. "SubalgebraBases in Macaulay2". In: *Journal of Software for Algebra and Geometry* 14.1 (May 2024), pp. 97–109. ISSN: 1948-7916. DOI: 10.2140/jsag.2024.14.97. URL: http://dx.doi.org/10.2140/jsag.2024.14.97.

[7] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer International Publishing, Oct. 2016. DOI: 10.1007/978-3-662-41154-43.

[8] Alicia Dickenstein et al. "The membership problem for unmixed polynomial ideals is solvable in single exponential time". In: *Discrete Applied Mathematics* 33.1 (1991), pp. 73–94. ISSN: 0166-218X. DOI: 10.1016/0166-218X(91)90109-A.

[9] Thomas W. Dubé. "The Structure of Polynomial Ideals and Gröbner Bases". In: *SIAM Journal on Computing* 19.4 (Aug. 1990), pp. 750–773. DOI: 10.1137/0219053.

[10] Michael Elberfeld, Andreas Jakoby, and Till Tantau. "Algorithmic Meta Theorems for Circuit Classes of Constant and Logarithmic Depth". In: *STACS 2012*. Vol. 14. LIPIcs. Dagstuhl, Germany, 2012, pp. 66–77. ISBN: 978-3-939897-35-4. DOI: 10.4230/LIPIcs.STACS.2012.66.

[11] Andre Galligo and Zbigniew Jelonek. "Elimination ideals and Bézout relations". In: *Journal of Algebra* 562 (2020), pp. 621–626. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2020.06.022.

[12] D. R. Grayson and M. E. Stillman. *Macaulay2, a software system for research in algebraic geometry*. Available at http://www.math.uiuc.edu/Macaulay2/. (version 1.24.11).

[13] Grete Hermann. "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale". In: *Mathematische Annalen* 95 (1926), pp. 736–788.

[14] John E Hopcroft and Jeffrey D Ullman. *An introduction to automata theory, languages, and computation*. Addison-Wesley series in computer science. Pearson, Jan. 1979. ISBN: 978-0201029888.

[15] Jürgen Gerhard Joachim von zur Gathen. *Modern Computer Algebra*. Cambridge University Press, Mar. 2017. 812 pp. ISBN: 1107039037. DOI: 10.1017/CBO9781139856065.

[16] Daniel M. Kane. *Unary Subset-Sum is in Logspace*. 2017. arXiv: 1012.1336 [cs.CC].

[17] Leonie Kayser. "Gröbner Bases and Their Complexity". MA thesis. Oct. 2022.

[18] Dexter Kozen. "Complexity of Finitely Presented Algebras". In: *Proceedings of the 9th Annual ACM Symposium on Theory of Computing, May 4-6, 1977, Boulder, Colorado, USA*. Ed. by John E. Hopcroft, Emily P. Friedman, and Michael A. Harrison. ACM, 1977, pp. 164–177. DOI: 10.1145/800105.803406.

[19] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1*. Springer Berlin Heidelberg, 2000. DOI: 10.1007/978-3-540-70628-1.

[20] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 2*. Springer Berlin Heidelberg, 2005. DOI: 10.1007/3-540-28296-3.

[21] Klaus Kühnle and Ernst W. Mayr. "Exponential Space Computation of Gröbner Bases". In: *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*. ISSAC '96. Zurich, Switzerland: Association for Computing Machinery, 1996, pp. 63–71. ISBN: 0897917960. DOI: 10.1145/236869.236900.

[22] Ernst W. Mayr. "Membership in polynomial ideals over Q is exponential space complete". In: *STACS 89*. Ed. by B. Monien and R. Cori. Berlin, Heidelberg: Springer Berlin Heidelberg, 1989, pp. 400–406. ISBN: 978-3-540-46098-5.

[23] Ernst W. Mayr. "Some Complexity Results for Polynomial Ideals". In: *Journal of Complexity* 13.3 (1997), pp. 303–325. ISSN: 0885-064X. DOI: 10.1006/jcom.1997.0447.

[24] Ernst W. Mayr and Albert R. Meyer. "The complexity of the word problems for commutative semigroups and polynomial ideals". In: *Advances in Mathematics* 46.3 (Dec. 1982), pp. 305–329. DOI: 10.1016/0001-8708(82)90048-2.

[25] Ernst W. Mayr and Stephan Ritscher. "Dimension-dependent bounds for Gröbner bases of polynomial ideals". In: *Journal of Symbolic Computation* 49 (2013). The International Symposium on Symbolic and Algebraic Computation, pp. 78–94. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2011.12.018.

[26] Ernst W. Mayr and Stefan Toman. "Complexity of Membership Problems of Different Types of Polynomial Ideals". In: *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory*. Ed. by Gebhard Böckle, Wolfram Decker, and Gunter Malle. Cham: Springer International Publishing, 2017, pp. 481–493. ISBN: 978-3-319-70566-8. DOI: 10.1007/978-3-319-70566-8_20.

[27] Lorenzo Robbiano and Moss Sweedler. "Subalgebra bases". In: *Commutative Algebra*. Ed. by Winfried Bruns and Aron Simis. Berlin, Heidelberg: Springer Berlin Heidelberg, 1990, pp. 61–87. ISBN: 978-3-540-47136-3.

[28] Thomas J. Schaefer. "The complexity of satisfiability problems". In: *Proceedings of the Tenth Annual ACM Symposium on Theory of Computing*. STOC '78. San Diego, California, USA: Association for Computing Machinery, 1978, pp. 216–226. ISBN: 9781450374378. DOI: 10.1145/800133.804350. URL: https://doi.org/10.1145/800133.804350.

[29] David Shannon and Moss Sweedler. "Using Gröbner bases to determine algebra membership, split surjective algebra homomorphisms determine birational equivalence". In: *Journal of Symbolic Computation* 6.2 (1988), pp. 267–273. ISSN: 0747-7171. DOI: 10.1016/S0747-7171(88)80047-6.

[30] David Spear. "A constructive approach to commutative ring theory". In: 1977. URL: https://api.semanticscholar.org/CorpusID:117037310.

[31] Heribert Vollmer. *Introduction to Circuit Complexity: A Uniform Approach*. Springer Berlin Heidelberg, 1999. ISBN: 9783662039274. DOI: 10.1007/978-3-662-03927-4.

Author's address:

Leonie Kayser, MPI-MiS Leipzig leo.kayser@mis.mpg.de