Membership in Polynomial Ideals over $\mathcal{Q}$ Is Exponential Space Complete

Ernst Mayr
Fachbereich Informatik
Johann Wolfgang Goethe-Universität Frankfurt
and
Department of Computer Science
Stanford University

Abstract

A polynomial ideal membership problem is an $(n+1)$-tuple $P = \langle p, p_1, p_2, \ldots, p_n \rangle$ where p and the p_i are multivariate polynomials over some ring, and the problem is to determine whether p is in the ideal generated by the p_i. For polynomials over the integers or rationals, it is known that this problem is exponential space hard. Here, we show that the problem for multivariate polynomials over the rationals is solvable in exponential space, establishing its exponential space completeness.

1 Introduction

Polynomial rings and their ideals are fundamental in many areas of mathematics, and they also have a surprising number of applications in various areas of computer science, like language generating and term rewriting systems, tiling problems, the complexity of algebraic manifolds, and the complexity of some models for parallel systems. The decidability of the membership problem for polynomial ideals over a field or ring can, in a sense, be traced back to ideas in Hilbert's work, and was established in [He26], [Se74], and [Ri74]. The computational complexity of the polynomial ideal membership problem was first discussed in [MM82] where the special case of the word problem for commutative semigroups was investigated. The bounds derived there imply an exponential space lower bound for the membership problem in polynomial ideals over $\mathcal{Z}$ (the integers) or $\mathcal{Q}$ (the rationals), as well as a doubly exponential upper bound for the time requirements for any Turing machine solving the polynomial ideal membership problem over the rationals. Other, rather special cases of the polynomial ideal membership problem (given by restrictions on the form of the generators) and their complexity have been investigated in [Hu84].

In this paper, we give an algorithm establishing an exponential space upper bound for the polynomial ideal membership problem for multivariate polynomials over the rationals. And, given that some polynomial p is a member of the ideal generated by polynomials $p_1, \ldots, p_w \in \mathcal{Q}[x_1, \ldots, x_v]$, we also present an exponential space construction of a representation of p in the ideal, *i.e.*, we construct polynomials $g_1, \ldots, g_w$ such that

$$p = \sum_{1 \leq i \leq w} g_i p_i.$$

Our algorithms are based on the fact that the rank and the determinant of a matrix with rational entries can be determined in $\mathcal{NC}$, *i.e.*, by a parallel algorithm using a polynomial number of processors and running in polylogarithmic time. By the Parallel Computation Thesis [FW78], this implies sequential algorithms for these problems, using space polylogarithmic in the size of the input (and running in polynomial time). For a detailed analysis of the (sequential and parallel) complexity of these and other matrix problems, also see [Pa87].

2 Basic Definitions and Notation

If n is a positive integer, we denote by I_n the set $\{1, 2, \ldots, n\}$. Let X denote the finite set $\{x_1, \ldots, x_v\}$, and $\mathcal{Q}[X]$ the (commutative) ring of polynomials with indeterminates $x_1, \ldots, x_v$ and rational coefficients. For $p_1, \ldots, p_w \in \mathcal{Q}[X]$, let $(p_1, \ldots, p_w) \subseteq \mathcal{Q}[X]$ denote the ideal generated by $\{p_1, \ldots, p_w\}$, that is,

$$(p_1, \ldots, p_w) \overset{\text{def}}{=} \left\{ \sum_{1 \le i \le w} p_i g_i \mid g_i \in \mathcal{Q}[X],\ i \in I_w \right\}.$$

By the $(w+1)$-tuple $P = \langle p, p_1, p_2, \ldots, p_w \rangle$, we denote the decision problem P of determining whether a given $p \in \mathcal{Q}[X]$ is in $(p_1, \ldots, p_w)$. The *size* of P, denoted *size*(P), is taken to be the length of a list specifying P using distinct characters for the indeterminates, arabic base ten notation for exponents and coefficients, with unit size delimiters between the polynomials that comprise P. For example, if our polynomial ideal membership problem instance P were to ask if the polynomial $p = a^2b + c - 4d$ is in the ideal over $\mathcal{Q}$ generated by the polynomials $p_1 = a + b - 3d$, $p_2 = c + d$, and $p_3 = 4b^2$, then the problem P would be encoded as

$$\boxed{\texttt{A 2 B + C - 4 D , A + B - 3 D , C + D , 4 B 2}},$$

for which *size*$(P) = 23$. We call P a polynomial ideal membership problem, or PIMP.

We assume in what follows that we are considering polynomial ideal membership problems over $\mathcal{Q}$. Recall that the *degree* of a multivariate polynomial p, denoted *deg*(p), is the greatest power appearing on some variable in the polynomial.

The answer to a problem instance P will be "yes" if and only if there exist polynomials g_i over $\mathcal{Q}$ such that

$$p = \sum_{1 \le i \le w} p_i g_i. \tag{1}$$

3 Reduction to a System of Linear Equations

Our method of determining if such polynomials g_i exist turns upon the following theorem, first given in [He26] (for an improved proof, see [MM82]:

Theorem 1 *Let $X = \{x_1, \ldots, x_v\}$, let $p, p_1, \ldots, p_w$ be polynomials $\in \mathcal{Q}[X]$, and let $d =_{\mathrm{df}} \max\{\deg(p_i);\ i \in I_w\}$. If $p \in (p_1, \ldots, p_w)$, then there exist $g_1, \ldots, g_w \in \mathcal{Q}[X]$ such that*

1. $p = \sum_{i=1}^{w} p_i g_i$; and

2. $(\forall i \in I_w)[\deg(g_i) \leq \deg(p) + (wd)^{2^v}]$.

We can obtain a more concise version of this upper bound as follows.

Taking the notation of Theorem 1, we know that the degree of each g_i appearing in any equation $p = \sum_{i=1}^{w} p_i g_i$ is at most $deg(p) + (wd)^{2^v}$. The following bounds follow immediately from the definitions of $deg(p)$, w, d, v, and $size(P)$:

$$\begin{aligned} deg(p) &\leq 10^{size(P)}, \\ w &\leq size(P), \\ d &\leq 10^{size(P)}, \text{ and} \\ v &\leq size(P). \end{aligned}$$

Temporarily letting $m = size(P)$, we have (via Theorem 1)

$$deg(g_i) \leq 10^m + (m10^m)^{2^m}.$$

Using this equation, one derives a simpler bound on $deg(g_i)$ doubly exponential in the size of the problem P; for example, we have for all i,

$$deg(g_i) \leq 2^{2^{4m}}.$$

In the worst case, each g_i will have all the distinct monomials of degree less than $M = 2^{2^{4m}}$ occuring inside it as terms (preceded by coefficients with which we are not immediately concerned). The number of such monomials is

$$(M+1)^v \leq (2^{2^{4m}} + 1)^m \leq 2^{2^{5m}}, \tag{2}$$

which is still a bound doubly exponential in $m = size(P)$. We let S be the set of all monomials whose degree is less than this bound, and assume this set of monomials to be linearly ordered arbitrarily (say lexicograpically) so that we may speak of the "jth monomial," for example, and have this be meaningful. We will use the notation $s(j)$ to stand for this monomial.

The answer to the problem P will be "yes" if and only if there exist rationals $c_{i,j}$, for $1 \leq i \leq w$ and $1 \leq j \leq |S|$, such that if we form the polynomials $g_i = \sum_{j=1}^{|S|} c_{i,j} s_j$, then we have $p = \sum_{i=1}^{w} p_i g_i$. Otherwise, the answer is "no."

Our approach is a naive one based upon expanding the right-hand side of the equation

$$p = \sum_{i=1}^{w} p_i g_i = \sum_{i=1}^{w} p_i \sum_{j=1}^{|S|} c_{i,j} s_j \tag{3}$$

into a sum of monomials, then collecting like terms so that the coefficients of the distinct monomials of the right-hand side may be compared with those that appear in front of the monomials that comprise p. That is, we reduce solving for the $c_{i,j}$ to solving a system of linear equations obtained by directly comparing the coefficients of the monomials of p with those that appear on the right-hand side of equation (3). A typical equation obtained in this way might look like

$$-3c_{1,2} + 14c_{10,7} + c_{2,3} = 4,$$

where the 4 would correspond to the coefficient appearing on some monomial of p, and the $-3c_{1,2} + 14c_{10,7} + c_{2,3}$ is the expression preceding the same monomial on the right-hand side of (3) after all simplifications have been performed.

To simplify notation in what follows, we relabel the unknown coefficients $c_{i,j}$ with a single subscript.

So far, we have transformed our problem into the problem of determining whether a solution exists to a certain system of linear equations with, say, r equations and q unknowns

$$AC = D, \tag{4}$$

where A is an r x q integer matrix $(a_{i,j})$, and C and D are column vectors $(c_1, \ldots, c_q)$ and $(d_1, \ldots, d_r)$. In the following paragraphs we establish upper bounds for r, q, and the size of the entries $a_{i,j}$.

There is one equation in (4) for every monomial appearing on the right-hand side of (3) after if has been expanded and simplified. Since $d \leq 10^m$ is an upper bound on $deg(p_i)$, and $2^{2^{4m}}$ is an upper bound on $deg(g_i)$, the degree of any monomial on the right-hand side (3) is at most

$$10^m + 2^{2^{4m}} \leq 2^{2^{5m}}.$$

In the worst case possible, all monomials of degree $\leq 2^{2^{5m}}$ would appear on the right-hand side of (3), giving rise to

$$(2^{2^{5m}} + 1)^v \leq (2^{2^{5m}} + 1)^m \leq 2^{2^{6m}}$$

equations in (4). Thus we have $r \leq 2^{2^{6m}}$, *i.e.*, r is doubly exponential in *size*(P).

The number of unknowns c_i in (4) corresponds to the number of undetermined coefficients $c_{i,j}$ in equation (3). We have

$$q \leq \sum_{1 \leq i \leq w} |S| \leq 2^{2^{6m}},$$

again at most doubly exponential in *size*(P).

Examining (3), we see that every entry $a_{i,j}$ in A is the sum of at most

$$wm|S| \leq 2^{2^{6m}}$$

rationals, each of whose size, as represented in the original problem description, is bounded by $m =$ *size*(P). Using this, one finds that the entire matrix A itself can be calculated and written down in space doubly exponential in *size*(P) as well.

The linear system (4) will have a solution C iff D is in the column space of A, or equivalently, if the rank of A remains unchanged after the column vector D is adjoined to it. Assume now that the matrices A and $A' = [A|D]$ have been padded with zero rows to make them square; it is now easy to see that our problem is effectively reduced to that of computing the ranks of these two matrices.

4 Efficient Parallel Rank Computations

Employing the earlier results of [Cs76], [IMR80] gives a $O(\log^2 n)$ parallel time algorithm for computing the rank of an order n complex matrix H using $O(n^4)$ processors (these algorithms are based on an arithmetic PRAM; see [Pa87] for the modifications required for bit model complexity). These algorithms presume that the whole matrix input data for H is present in memory before the computation begins. Unfortunately, for the problem at hand we can make no such assumption, since we have assumed that a polynomial ideal membership problem is given in the form of encoded polynomials that then give rise to the matrices A and A' above, whose size is doubly exponential in the size of the original problem instance. We would like to avoid paying the cost of computing the matrices A and A' in their entirety before these parallel algorithms can begin their operation. To avoid this problem, we simply start the parallel rank algorithms running *without* their input, then when any particular processor requires information about an entry of A or A', we pause to compute this value directly from the original problem description. We argue below that the bookkeeping and recomputation overhead implied by this approach does not alter the parallel time and space requirements of the algorithms in [IMR80] and [Cs76].

To justify these remarks, we first sketch the parallel rank computation algorithms alluded to above. The method of computing the rank of an $n \times n$ complex matrix A in parallel time $O(\log^2 n)$ breaks into the following three steps:

1. Calculate $B = A^H A$, where A^H denotes the conjugate transpose. This takes $O(\log n)$ time.
2. Calculate the coefficients $c_1, \ldots, c_n$ of the characteristic polynomial of B. (This is the polynomial $f_B(\lambda) = det(\lambda I - B) = \lambda^n + c_1\lambda^{n-1} + \cdots + c_{n-1}\lambda + c_n$).
3. Determine the largest integer i such that $c_{n-i} \neq 0$ and $c_{n-i+1} = \cdots = c_n = 0$. This can be done in in $O(\log n)$ time with $O(n)$ processors. Then rank$(A) = n - i$.

The resulting algorithm can be made to run in parallel time $O(\log^2 n)$ using $O(n^4)$ processors.

We will not elaborate on these algorithms any farther here. The important idea in what follows is that each of the stages in this computation consists of interleaved "lookup" and "computation" phases. In a "lookup" phase, the entries of A are consulted, and in a "computation" phase, something is actually done with these values. In the case when the whole matrix A is in memory before the computation begins, then the "lookup" cost is negligible and may be safely ignored.

In our case, we pause to compute the appropriate entry of A or A' each time such a value is needed in a "lookup" phase. How much does this add to the computation time required by the parallel rank algorithm? In the worst possible case, at each parallel time step, every processor will require some value of A or A' to proceed. Such an entry is directly computable from the problem description in the following way. Every entry of A and A' is determined by its row and column position. The row corresponds to a monomial on the right-hand-side of equation (3) above, and the column indexes a particular $c_{i,j}$. The entry of A indexed in this way will be zero except if the monomial indexed by j, when multiplied by some monomial of p_i, yields the monomial indexed by this row. Then in this case the entry of A is just equal to some coefficient on a monomial of p_i. Thus the "computation" involved in a "lookup" phase is just an indexing process which is up to a constant factor no harder than finding the value stored at a particular point in an array. We conclude that this "lookup" cost is negligible and can be absorbed into the bookkeeping implied in the presentation of the algorithms in [Cs76] and [IMR80]. We have the following theorem:

Theorem 2 *Let P be a polynomial ideal membership problem over Q, and let $m =$ size(P). Then there is an algorithm which solves P in parallel time 2^{cm} using $2^{2^{c'm}}$ processors, for some universal constants c and c'.*

5 Complexity of Membership in Polynomial Ideals

We take the deterministic CREW PRAM as our model of parallel computation (see, [FW78].

Since we are interested in the sequential space requirements of PIMP problems, the following lemma from [FW78] is useful to us:

Lemma: *Let L be accepted by a $T(n)$ time-bounded PRAM. Then L is accepted by a $O(T^2(n))$ space-bounded (deterministic) Turing machine.*

The essential idea of the proof of this lemma is that after $T(n)$ time steps of such a parallel algorithm, at most $2^{T(n)}$ processors are running, a complete description of any of which occupies space $O(T(n))$. By a recursive-call simulation and recomputation technique whose depth never exceeds $T(n)$, we obtain a sequential simulation of the parallel computation which requires total space $O(T^2(n))$. We have our main theorem as a result:

Theorem 3 *The polynomial ideal membership problem is solvable in sequential space exponential in the size of the problem instance, and it is thus complete for exponential space.*

6 Determining a Representation

Using similar ideas, we can also determine a representation

$$p = \sum_{1 \le i \le w} g_i p_i$$

if p is in the ideal generated by the p_i. Again, we use low space sequential versions of parallel methods for solving linear systems of equations (based on computing the determinant and Cramer's method) [Pa87]. We obtain a sequential algorithm running in space exponential in the size of the problem instance. Note that the length of the output can be double exponential in the input size. For this extended abstract, we omit further details of the construction.

Theorem 4 *Let p and $p_1, \ldots, p_w$ be multivariate polynomials over the rationals. If p is an element of the ideal generated by the p_i then a representation*

$$p = \sum_{1 \le i \le w} g_i p_i$$

can be found in exponential space.

7 Conclusion and Open Problems

Using space efficient algorithms for the rank and determinant problem for matrices, we were able to show that the polynomial ideal membership problem for multivariate polynomials over the rationals can be solved in exponential space. Together with the previously known lower bound, this establishes the completeness of this variant of PIMP for exponential space.

The following two open problems are of immediate interest.

1. Are there relevant subclasses of PIMP (other than those studied in [Hu84]) which are complete for lower complexity classes?

2. What is the complexity of the polynomial ideal membership problem for multivariate polynomials over the integers, or other effective integral domains? It is known that the membership problem is decidable in the case of Noetherian rings [Ri74], however, no non-trivial upper bounds for the complexity are known. The exponential space lower bound given in [MM82] also holds for polynomial ideals over the integers.

References

[Cs76] L. Csanky: Fast Parallel Matrix Inversion Algorithms.*SIAM J. Comput.* **5** (1976), 618–623.

[FW78] S. Fortune and J. Wyllie: Parallelism in Random Access Machines. *Proceedings of the 10th Ann. ACM STOC* (1978), 114–118.

[He26] G. Hermann: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.* **95** (1926), 736–788.

[Hu84] Huynh, Dung T.: The Complexity of the Membership Problem for Two Subclasses of Polynomial Ideals. Preprint, Computer Science Department, Iowa State University (1984).

[IMR80] O.H. Ibarra, S. Moran, and L E. Rosier: A Note on the Parallel Complexity of Computing the Rank of Order n Matrices. *Information Processing Letters* **11** (1980), 162.

[MM82] E.W. Mayr and A.R. Meyer: The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals. Adv. in Math. **46** (1982), 305–329.

[Pa87] V. Pan: Complexity of Parallel Matrix Computations. *Theoretical Computer Science* **54** (1987).

[Ri74] F. Richman: Constructive Aspects of Noetherian Rings. *Proc. Amer. Math. Soc.* **44**, 2 (1974), 436–441.

[Se74] Seidenberg, A.: Constructions in Algebra. *Trans. Amer. Math. Soc.* **44** (1974), 273–313.