THE MEMBERSHIP PROBLEM FOR IDEALS IN Z[X]

CARLOS E. ARRECHE

Abstract. There exists a feasible procedure to decide whether or not an arbitrary polynomial belongs to a given ideal in Z[x] if the ideal's minimal basis is known. However, when this is not the case there is no feasible procedure to decide whether or not an arbitrary polynomial belongs to a given ideal. There already exists an effective procedure to find an ideal's minimal basis, but it depends on solving the membership problem for the ideal (i.e. the problem of deciding whether an arbitrary polynomial belongs to the ideal). Therefore, we develop a modification of the existing algorithm to find an ideal's minimal basis so that there is no need to solve the membership problem to carry it out, and then we use this minimal basis to solve the membership problem for this ideal.

1. Introduction

Our purpose here is to solve the membership problem for ideals in the ring of polynomials over the integers $\mathbb{Z}[x]$. That is, to be able to determine feasibly and efficiently if an arbitrary polynomial with integer coefficients belongs to a finitely generated ideal in the ring of polynomials over the integers. We begin by defining an ideal's minimal basis as in [3]. If A is a principal ideal generated by $\langle f(x) \rangle$, its minimal basis is defined by $\{f(x)\}$ if the leading coefficient of $f(x)$ is positive and $\{-f(x)\}$ otherwise. If $A = f(x)B$, where the leading coefficient of $f(x)$ is positive and B has the minimal basis $\{h_1(x), \ldots, h_n(x)\}$, then the minimal basis for A is defined by $\{f(x)h_1(x), \ldots, f(x)h_n(x)\}$.

In [1] Cáceres-Duque gives an effective procedure for this using basic properties of the minimal basis of an ideal and the fact that ideals in $\mathbb{Z}[x]$ are detachable (an ideal of a ring R is detachable if we can decide effectively whether a given element of R belongs to the ideal).

The following Theorem is proved in [3].

Theorem 1. *If A is a primitive proper ideal of $\mathbb{Z}[x]$, there exists a constant c such that $c \in A - \{0\}$.*

Proof. See [3]. □

In [1] the following Lemma is also proved.

Lemma 1. *Given a primitive ideal A in $\mathbb{Z}[x]$ generated by $f_1(x), \ldots, f_n(x)$, there exists an effective procedure to find a nonzero constant in A.*

2000 *Mathematics Subject Classification.* 11C08, 13F20, 11Y99, 13P99.

Key words and phrases. detachable ideal, ideal, minimal bases for ideals, monic polynomial, noetherian ring, primitive ideal.

Very special thanks to Professor Cáceres-Duque for all his incredibly helpful advice, mentorship and collaboration.

Proof. We know the existence of such a constant by Theorem 1. Since A is primitive, $\gcd(f_1(x), \ldots, f_n(x)) = 1$; therefore, there exists an effective procedure for finding $u_1(x), \ldots, u_n(x) \in \mathbb{Q}[x]$ such that $1 = u_1(x)f_1(x) + \cdots + u_n(x)f_n(x)$. Finding common denominator on the right hand side and multiplying by it on both sides we obtain $c = cu_1(x)f_1(x) + \cdots + cu_n(x)f_n(x)$ where $cu_i(x) \in \mathbb{Z}[x]$ $(i = 1, \ldots, n)$. □

Since A contains a nonzero constant, it contains polynomials of an arbitrary degree k. As in [1], for every $k \geq 0$ we call the polynomials

$$g_k(x) = a_k x^k + \sum_{i=0}^{k-1} a_{ki} x^i$$

minimal, where a_k is the smallest positive number which is the leading coefficient of a polynomial of degree k in A. In [3] it is also proved that if A is a primitive proper ideal of $\mathbb{Z}[x]$, it possesses a minimal basis $\{g_m(x), \ldots, g_1(x), g_0(x)\}$ with the following properties

$$\begin{aligned} g_0 &= q_1 q_2 \cdots q_m \\ q_k g_k(x) &= x g_{k-1}(x) + \sum_{i=0}^{k-1} b_{ki} g_i(x) \end{aligned} \tag{1.1}$$

$$\text{where } q_k, b_{ki} \in \mathbb{Z} \text{ such that } q_k > 0;\ 0 \leq b_{ki} < q_k;\ 0 < k \leq m;\ 0 \leq i < k. \tag{1.2}$$

Note that this implies that $g_m(x)$ is monic. The number m is called the degree of A. The following propositions are proved as Theorem 1 in [3] and Proposition 1 in [1], respectively:

Theorem 2. *There is a one-to-one correspondence between the primitive proper ideals of $\mathbb{Z}[x]$ and the system of invariants* (1.2).

Proof. See [3]. □

Proposition 1. *Suppose A is a primitive proper ideal of $\mathbb{Z}[x]$ with minimal basis given by $\{g_m(x), g_{m-1}(x), \ldots, g_1(x), g_0(x)\}$. Then every element of A is of the form: $f(x)g_m(x) + c_{m-1}g_{m-1}(x) + \cdots + c_1 g_1(x) + c_0 g_0(x)$, for some unique $f(x) \in \mathbb{Z}[x]$ and some unique $c_{m-1}, \ldots, c_1, c_0 \in \mathbb{Z}$.*

Proof. Follows from the proof of Theorem 1, see [1] and [3]. □

Because of Proposition 1, all the computational difficulty in determining an arbitrary polynomial's membership in a given ideal is completed upon finding its minimal basis. This is stated as Lemma 4 in [1]:

Lemma 2. *Let A be a primitive proper ideal of $\mathbb{Z}[x]$ with minimal basis given by $\{g_m(x), \ldots, g_1(x), g_0(x)\}$. If $f(x)$ is an arbitrary polynomial of $\mathbb{Z}[x]$, there is a feasible procedure to decide whether or not $f(x) \in A$.*

Proof. If $\deg(f(x)) = n \leq m$, then using Proposition 1, $f(x) \in A$ if and only if there exist $a_0, a_1, \ldots, a_m, \ldots, a_n$ such that $f(x) = a_n x^{n-m} g_m(x) + \cdots + a_m g_m(x) + \cdots + a_0 g_0(x)$. If $\deg(f(x)) = n \leq m$, then, by Proposition 1.4, $f(x) \in A$ if and only if there exist $a_0, a_1, \ldots, a_m, \ldots, a_n$ such that: $f(x) = a_n x^{n-m} g_m(x) + \cdots + a_m g_m(x) + \cdots + a_0 g_0(x)$. In any case we can decide effectively whether or not a system of n equations with n variables has solution. □

Consider the following preliminary Lemma, proved as Lemma 2 in [1]:

Lemma 3. *If A is a primitive proper ideal of $\mathbb{Z}[x]$ with minimal basis given by $\{g_m(x), g_{m-1}(x), \ldots, g_1(x), g_0(x)\}$ and $\{f_1(x), \ldots, f_n(x)\}$ is a set of generators of A, then*

$$m \leq \max(\deg(f_i(x)) : i = 1, \ldots, n)$$

Proof. See proof for Lemma 2 in [1]. □

The following Theorem states the existence of an effective procedure for finding an ideal's minimal basis, this is crucial to our feasible procedure for the membership problem. It is proved as Theorem 2 in [1].

Theorem 3. *Given a set of generators $f_1(x), f_2(x), \ldots, f_n(x)$ of an ideal B in $\mathbb{Z}[x]$, there exists an effective procedure to find a minimal basis for B.*

Proof. Let B be an ideal of $\mathbb{Z}[x]$ with $B = \langle f_1(x), f_2(x), \ldots, f_n(x)\rangle$ and assume B is nonprincipal, otherwise the proof is trivial. Given $f_1(x), f_2(x), \ldots, f_n(x) \in \mathbb{Z}[x]$, there exists an effective procedure to find $\gcd(f_1(x), f_2(x), \ldots, f_n(x))$. Therefore we can write $B = \gcd(f_1(x), f_2(x), \ldots, f_n(x))A$, where A is a primitive proper ideal. Then we reduce the problem to finding a minimal basis for the primitive proper ideal A. Suppose $A = \langle h_1(x), h_2(x), \ldots, h_n(x)\rangle$, with $\gcd(h_1(x), h_2(x), \ldots, h_n(x)) = 1$. By Lemma 1, there is an effective procedure to find $c \in A - \{0\}$. Therefore $A = \langle h_1(x), h_2(x), \ldots, h_n(x), c\rangle$. By Theorem 2, there are finitely many ideals $\langle C\rangle$ that contain c of a given finite degree and we can enumerate them. In fact, by Lemma 3 there is a bound in the degree of the ideals that we have to consider. Suppose $\langle C\rangle$ is an ideal with minimal basis C that contains c. Using the fact that ideals of $\mathbb{Z}[x]$ are detachable, or even better using Lemma 2, we can decide effectively whether or not $h_1(x), h_2(x), \ldots, h_n(x) \in \langle C\rangle$. Since A is detachable, we can decide effectively whether or not $\langle C\rangle \subseteq A$. If we obtain a positive answer in both containments, the proof is complete, otherwise pick a different ideal $\langle C\rangle$ that contains c and note that in finitely many steps we obtain the desired minimal basis. □

The only inconvenience this procedure presents is that it doesn't say how to check if $\langle C\rangle \subseteq A$. It is known this can be done because of the fact that ideals in $\mathbb{Z}[x]$ are detachable (this has been proved by several authors, see [1]), but there is no known feasible procedure to do so.

Actually, in [2] Simmons gives an algorithm for the solution of the membership problem. This algorithm consists of performing two simultaneous procedures: the first procedure stops if and only if the polynomial in question belongs to the ideal, the other procedure stops if and only if the polynomial in question does not belong to the ideal. We proceed to describe both of these procedures:

Simmons' first procedure is trivial and is described in [2] as follows: Let $A = \langle f_1(x), \ldots, f_n(x)\rangle$, $f(x) \in \mathbb{Z}[x]$ be a polynomial. Now we enumerate all n-tuples $(g_1(x), \ldots, g_n(x))$ and compute $f_1(x)g_1(x) + \cdots + f_n(x)g_n(x)$. The procedure stops when $f(x) = f_1(x)g_1(x) + \cdots + f_n(x)g_n(x)$. And if $f(x)$ doesn't belong to A the procedure never stops.

The second procedure suggested in [2] goes as follows: First decide whether $f(x) \in A$ over $\mathbb{Q}[x]$; if not we are done. Otherwise, find an integer $c \in \mathbb{Z}$ such that $cf(x) \in A$. Note that this is possible because of Lemma 1. Now decide if $f(x) \in A + \langle c\rangle$, which is true iff $f(x) \in (\mathbb{Z}/c\mathbb{Z})[x]$. If this is not the case, then we are done. Otherwise, decide whether $f(x) \in A + \langle c^2\rangle$. If this is not the case, we are done. Otherwise, keep repeating this procedure. If $f(x)$ does not belong to A,

then it follows from the fact that $\mathbb{Z}[x]$ is noetherian that there exists a m such that $f(x)$ does not belong to $A + \langle c^m \rangle$ (see [2]). And if $f(x) \in A$ the procedure never stops.

2. The Membership Problem

It would be desirable to be able to find an ideal's minimal basis and then use Lemma 2 to decide whether $f(x)$ belongs to the ideal or not. Unfortunately, the only procedure we have for finding an ideal's minimal basis depends on being able to solve the membership problem. We will give an alternate procedure to find an ideal's minimal basis that relies only on basic properties of the minimal basis. It should be noted that this procedure is but a modification of the one described for the proof of Theorem 3, with the additional advantage that it can be carried out independently of the rather inefficient procedure described in [2].

Let $A = \langle f_1(x), \ldots, f_n(x) \rangle$ be a primitive proper ideal in $\mathbb{Z}[x]$. In order to apply Theorem 3 it is necessary to find a nonzero constant c in A (which always exists because of Theorem 1), so that: $A = \langle f_1(x), \ldots, f_n(x), c \rangle$. Now, because of Theorem 2, there are *finitely many* ideals $\langle C \rangle$ that contain a c of a given finite degree, and because of Lemma 3 there is a bound in the degree of the ideals that need to be considered. Suppose $\langle C \rangle$ is an ideal with minimal basis C that contains c. Then Theorem 3 requires us to verify for each ideal $\langle C \rangle$ if the following conditions hold:

$$f_1(x), \ldots, f_n(x) \in \langle C \rangle \Leftrightarrow A \subseteq \langle C \rangle \tag{2.1}$$

$$C \subseteq \langle f_1(x), \ldots, f_n(x), c \rangle \Leftrightarrow \langle C \rangle \subseteq A \tag{2.2}$$

Because of Lemma 2, there exists a feasible procedure to verify (2.1); but verifying (2.2) in simple cases turns out to be quite troublesome. As a matter of fact, in order to verify (2.2) it is necessary to decide if an arbitrary polynomial belongs to an ideal with unknown minimal basis, which is the problem at hand.

The following is proved as Lemma 1 in [1]:

Lemma 4. *Let A be a primitive proper ideal of $\mathbb{Z}[x]$ with minimal basis given by $\{g_m(x), \ldots, g_1(x), g_0(x)\}$. If $f(x)$ is a primitive polynomial of $\mathbb{Z}[x]$ with $\deg(f(x)) = k$, then $f(x) \in A$ implies that the degree of the ideal A is less or equal than k.*

Proof. See the proof for Lemma 1 in [1]. □

Before proceeding, consider another preliminary Lemma:

Lemma 5. *Let A and B be primitive proper ideals of $\mathbb{Z}[x]$. If $A \subseteq B$, then the degree of the ideal A is less or equal than the degree of the ideal B.*

Proof. Let $\{f_n(x), \ldots, f_1(x), f_0(x)\}$ be the minimal basis of A and let $\{g_m(x), \ldots, g_1(x), g_0(x)\}$ be the minimal basis of B. By hypothesis $A \subseteq B$, therefore, $f_n(x) \in B$. Since $f_n(x)$ is monic (property (1.1) of the minimal basis of an ideal), it is also primitive. And now Lemma 4 can be applied to the ideal B: since B contains a primitive polynomial of degree n, the degree of the ideal B is less or equal than n, which is the degree of the ideal A. □

Lemma 3 and Lemma 5 shall be used to find out the value m of the degree of A. Lemma 3 gives an upper bound for the degree of the ideal A and Lemma 5 gives a lower bound if an ideal with a known degree that contains A can be found. Let

$m_0 = \max\{\deg(f_i(x)) : i = 1, \ldots, n\}$. Consider the full list of all the ideals with degree m_0 (note that by Lemma 3, we don't need to consider ideals with degree greater than m_0) that contain the constant c. If at least one of them satisfies (2.1), then by Lemma 5 the degree of the ideal A is equal to m_0; if none of them satisfies (2.1), then we have just manually verified that the degree of A is less or equal than $m_0 - 1$. Now make the full list of ideals with degree $m_0 - 1$ that contain the constant c, and do the same as with the ideals with degree m_0. Note that this is a finite process that will go on until the value m of the degree of the ideal A is found.

Now let $\langle C_1\rangle, \ldots, \langle C_p\rangle$ (with minimal bases $C_1, \ldots, C_p$, respectively) be the full list of the ideals of degree m that contain c and satisfy (2.1). Because of Theorem 2, A has a unique minimal basis and it is one from the list $C_1, \ldots, C_p$ (which are all different from each other); let C_q be the minimal basis for A, so that $A = \langle C_q\rangle$. By hypothesis, all of the ideals in the list $\langle C_1\rangle, \ldots, \langle C_p\rangle$ contain A, that is: $A \subseteq \langle C_1\rangle, \ldots, A \subseteq \langle C_p\rangle$. This implies that $\langle C_q\rangle \subseteq \langle C_1\rangle, \ldots, \langle C_q\rangle \subseteq \langle C_p\rangle$. And we have reduced the problem to finding an unknown ideal $\langle C_q\rangle$ with minimal basis C_q that belongs to all of the other ideals in the list, for which we know their minimal bases. This gives us a criterion to eliminate unwanted ideals from the list of possible ideals equal to A.

For an illustration of how this is helpful in finding the minimal basis of A, consider $\langle C_i\rangle$ and $\langle C_j\rangle$, which are both in the list of possible ideals equal to A. Now we will check whether $\langle C_i\rangle \subseteq \langle C_j\rangle$. If this is the case, then we can conclude that $\langle C_j\rangle \neq A$ and we can discard it from our list. For, assume that $\langle C_j\rangle = A$. This implies that $\langle C_j\rangle \subseteq \langle C_i\rangle$, which in turn implies that $\langle C_j\rangle = \langle C_i\rangle$; leading to a contradiction. If, on the other hand, it is not the case that $\langle C_i\rangle \subseteq \langle C_j\rangle$, then $\langle C_i\rangle \neq A$ and we can discard it from our list. For, if $\langle C_i\rangle = A$ then $\langle C_i\rangle \subseteq \langle C_j\rangle$ because we know that $A \subseteq \langle C_j\rangle$.

Hence, it is possible to find the ideal $\langle C_q\rangle = A$ by checking for containment by pairs as described above; and note that in finitely many steps we find the desired ideal with known minimal basis. With this alternate proof of Theorem 3, an alternate procedure to find an ideal's minimal basis has been developed which does not depend on solving the problem of determining if an arbitrary polynomial in the ring of polynomials over the integers belongs to a given ideal (the membership problem). Therefore, it is now possible to solve the general case.

Theorem 4. *Let $A = \langle f_1(x), \ldots, f_n(x)\rangle$ be a proper ideal of $\mathbb{Z}[x]$ and $f(x) \in \mathbb{Z}[x]$ be an arbitrary polynomial. There exists a feasible procedure to decide whether or not $f(x) \in A$.*

Proof. Applying Theorem 3, there exists an effective procedure to find a minimal basis for A. If A is primitive, then applying Lemma 2 there exists a feasible procedure to decide whether or not $f(x) \in A$. If A is not primitive, then the minimal basis for A is given by $g(x)B$, where $g(x) \in \mathbb{Z}[x]$ and B is a primitive proper ideal. Therefore $f(x) \in A$ if and only if $f(x) = g(x)q(x)$ and $q(x) \in B$. Divide $f(x)$ by $g(x)$ in $\mathbb{Q}[x]$, if there is no residue, then decide if the quotient belongs to B using Lemma 2. □

Since ideals of $\mathbb{Z}[x]$ are detachable, this Theorem was already known to be true, but there was no way to apply it because there was no feasible way to apply Theorem 3, since the previous procedure depended on carrying out the solution to the membership problem described in [2]. Lemma 5 isn't necessary to carry out the

procedure described here, but it makes application of Theorem 4 easier, as does this next Lemma:

Lemma 6. *Let A and B be two distinct primitive proper ideals of $\mathbb{Z}[x]$ with minimal bases given by: $\{g_m(x), \ldots, g_1(x), g_0(x)\}$ and $\{h_m(x), \ldots, h_1(x), h_0(x)\}$ respectively, satisfying:*

$$g_0 = q_1 q_2 \cdots q_m \qquad h_0 = r_1 r_2 \cdots r_m$$

$$q_k g_k(x) = x g_{k-1}(x) + \sum_{i=0}^{k-1} a_{ki} g_i(x) \qquad r_k h_k(x) = x h_{k-1}(x) + \sum_{i=0}^{k-1} b_{ki} h_i(x)$$

$$q_k, r_k > 0;\ 0 \leq a_{ki} < q_k;\ 0 \leq b_{ki} < r_k;\ 0 < k \leq m;\ 0 \leq i < k$$

If $q_k = r_k$ for all $k = 1, \ldots, m$; then $A \nsubseteq B$ and $B \nsubseteq A$.

Proof. It suffices to show that if $A \subset B$ then $B \subset A$ leading to a contradiction and hence obtaining the desired result. Assuming $A \subset B$, the desired contradiction follows from strong induction on m. □

References

1. L.F. Cáceres-Duque, *An Effective Procedure for Minimal Bases of Ideals in Z[x]*, Discussiones Mathematicae General Algebra and Applications, 23 (1), 2003, pp. 5-11.
2. H. Simmons, *The Solution of a Decision Problem for Several Classes of Rings*, Pacific J. Math. 34, 1970, pp. 547-557.
3. G. Szekeres, *A Canonical Basis for the Ideals of a Polynomial Domain*, Amer. Math. Monthly 59, 1952, pp. 379-386.

37 Holder Hall, Princeton, NJ 08544
E-mail address: carreche@princeton.edu