AN EFFECTIVE PROCEDURE FOR MINIMAL BASES OF IDEALS IN $\mathbb{Z}[x]$

LUIS F. CÁCERES-DUQUE

Mathematics Department, University of Puerto Rico at Mayagüez, PO BOX 9018 Mayagüez, PR 00681, USA

e-mail: lcaceres@math.uprm.edu

Abstract

We give an effective procedure to find minimal bases for ideals of the ring of polynomials over the integers.

Keywords: ideals, minimal bases for ideals, polynomials over integers.

2000 Mathematics Subject Classification: 11C08, 13F20, 11A07, 11Y99.

1. Introduction

As in [5], we say that the ideals of the ring $R$ are detachable if one can decide effectively whether or not a given element of the ring is in a given finitely generated ideal of $R$. Using the fact that ideals of $\mathbb{Z}[x]$ are detachable we give an effective procedure to find a minimal basis for an ideal $A$ of $\mathbb{Z}[x]$, from a given finite set of generators for $A$. Moreover, given a minimal basis for the ideal $A$ of $\mathbb{Z}[x]$, it is very easy to determine effectively and efficiently whether or not an arbitrary polynomial $f(x)$ of $\mathbb{Z}[x]$ belongs to $A$. Indeed, all the computational difficulty of determining membership in $A$ is completed upon finding its minimal basis.

This problem was solved by Hurd in [3]. In his Ph.D. dissertation he developed an algorithm for determining the minimal basis for an ideal in $\mathbb{Z}[x]$ with a given set of generators, actually he worked with primitive ideals, but his results can be generalized to other ideals. However, as is pointed
out by his adviser in [1], his method is complicated. We give a solution of the problem using basic properties of the minimal basis of an ideal and the fact that ideals in \( \mathbb{Z}[x] \) are detachable. The fact that ideals of \( \mathbb{Z}[x] \) are detachable has been proved by several authors, in fact in [6] is given an easy description of an effective procedure which given a finite subset \( B \) of \( \mathbb{Z}[x] \) and \( f(x) \in \mathbb{Z}[x] \) decides whether or not \( f(x) \) belongs to the ideal generated by \( B \). Detachability of ideals in \( \mathbb{Z}[x] \) is also proved in [5] using the concept of Tennenbaum rings.

2. Minimal basis for ideals of \( \mathbb{Z}[x] \)

We define a minimal basis of an ideal \( A \) of the ring of polynomials \( \mathbb{Z}[x] \) as in [7]. If \( A \) is a principal ideal \( \langle f(x) \rangle \), then we call \( \{f(x)\} \) the minimal basis for \( A \) if the leading coefficient of \( f(x) \) is positive, otherwise we say that \( \{-f(x)\} \) is the minimal basis for \( A \). If \( A = \langle f(x) \rangle B \), where the leading coefficient of \( f(x) \) is positive and \( B \) has the minimal basis \( \{h_1(x), h_2(x), \ldots, h_n(x)\} \), then the minimal basis for \( A \) is defined by \( \{f(x)h_1(x), f(x)h_2(x), \ldots, f(x)h_n(x)\} \).

Let \( A \) be a primitive proper ideal of \( \mathbb{Z}[x] \). By Theorem 2.1.2 of [2], \( A \) contains a nonzero constant, hence it contains polynomials of an arbitrary degree \( k \). As in [7] for each \( k \geq 0 \) 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 [7] it is proved that given a primitive proper ideal \( A \) of \( \mathbb{Z}[x] \), it possesses a minimal basis \( \{g_m(x), \ldots, g_1(x), g_0(x)\} \) with the following properties

\[
g_0 = q_1 q_2 \cdots q_m,
\]

\[
q_k g_k(x) = x g_{k-1}(x) + \sum_{i=0}^{k-1} b_{ki} g_i(x),
\]

\[
q_k > 0, \ 0 \leq b_{ki} < q_k, \ 0 < k \leq m, \ 0 \leq i < k.
\]
In some cases it’s useful to represent the system of invariants (2.2) with a matrix notation as follows

\[
0 \leq \begin{bmatrix}
  b_{10} & b_{21} \\
  b_{20} & b_{21} \\
  \vdots & \vdots & \ddots \\
  b_{m0} & b_{m1} & \cdots & b_{m(m-1)}
\end{bmatrix} \prec \begin{bmatrix}
  q_1 \\
  q_2 \\
  \vdots \\
  q_m
\end{bmatrix}
\]

The number \( m \) is called the \textit{degree} of \( A \). Moreover, in [7] the following theorem is proved.

\textbf{Theorem 1.} There is a one to one correspondence between the primitive proper ideals of \( \mathbb{Z}[x] \) and the system of invariants (2.2).

\textbf{Proposition 1.} Suppose \( A \) is a primitive proper ideal of \( \mathbb{Z}[x] \) with minimal basis given by \( \{g_m(x), \ldots, g_1(x), g_0(x)\} \). Every element of \( A \) is of the form \( f(x)g_m(x) + c_{m-1}g_{m-1}(x) + \ldots + c_0g_0(x) \), for some unique \( f(x) \in \mathbb{Z}[x] \) and some unique \( c_{m-1}, \ldots, c_1, c_0 \in \mathbb{Z} \).

\textbf{Proof.} Follows from the proof of Theorem 1, see [7].

The following result shows that if \( A \) is a primitive proper ideal of \( \mathbb{Z}[x] \), then the degree of \( A \) is less or equal than the degree of any primitive polynomial in \( A \). It’s easy to find examples to show that we can obtain either equality or strictly inequality.

\textbf{Lemma 1.} 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 \( \deg f(x) = k \) and

\[
h_i(x) = \begin{cases} 
  g_i(x), & \text{for } i = 0, 1, \ldots, m, \\
  x^{i-m}g_m(x), & \text{for } i = m + 1, \ldots,
\end{cases}
\]

then \( f(x) \in A \) implies \( h_k(x) \) is monic, i.e., the degree of the ideal \( A \) is less or equal than \( k \).
Proof. Suppose \( A \) is a primitive proper ideal of \( \mathbb{Z}[x] \) with minimal basis
\[
\{g_m(x), \ldots, g_1(x), g_0(x)\}.
\]
Let \( f(x) \) be a primitive polynomial of \( \mathbb{Z}[x] \) with \( \deg f(x) = k \). If \( f(x) \in A \), then, by Proposition 1, there exist \( b_0, b_1, \ldots, b_k \in \mathbb{Z} \) such that \( f(x) = b_k h_k(x) + \ldots + b_1 h_1(x) + b_0 h_0(x) \). Let \( a_k \) be the leading coefficient of \( h_k(x) \), then \( a_k \mid h_j(x) \) for \( j = 0, 1, \ldots, k \), hence \( a_k \mid f(x) \). Since \( f(x) \) is primitive we obtain \( a_k = 1 \), so \( h_k(x) \) is monic.

The following lemma shows how to obtain a bound in the degree of an ideal, knowing a set of generators.

Lemma 2. If \( A \) is a primitive proper ideal of \( \mathbb{Z}[x] \) with minimal basis given by \( \{g_m(x), \ldots, g_1(x), g_0(x)\} \) and \( \{f_1(x), f_2(x), \ldots, f_n(x)\} \) is a set of generators of \( A \), then
\[
m \leq \max \{\deg f_i(x) : i = 1, 2, \ldots, n\}.
\]

Proof. Suppose \( A \) is a primitive proper ideal of \( \mathbb{Z}[x] \) with minimal basis
\[
(2.3) \quad \{g_m(x), \ldots, g_1(x), g_0(x)\}
\]
and \( \{f_1(x), f_2(x), \ldots, f_n(x)\} \) is a set of generators of \( A \). If
\[
m > \max \{\deg f_i(x) : i = 1, 2, \ldots, n\},
\]
then
\[
A = \langle f_1(x), f_2(x), \ldots, f_n(x) \rangle \subseteq \langle g_{m-1}(x), \ldots, g_1(x), g_0(x) \rangle \subseteq A.
\]
Therefore \( A = \langle g_{m-1}(x), \ldots, g_1(x), g_0(x) \rangle \). This contradicts the definition of minimal basis.

In [4] there is a generalization of minimal basis for ideals of \( \mathbb{Z}[x] \) in the sense that we have studied here, for ideals of a ring of polynomials over an arbitrary PID. In fact, in [4] is only considered primitive ideals but results can easily be generalized to other ideals.

Lemma 3. Given a primitive ideal \( A \) in \( \mathbb{Z}[x] \) generated by \( f_1(x), f_2(x), \ldots, f_n(x) \), there exists an effective procedure to find a nonzero constant in \( A \).
Proof. We know the existence of such a constant by Theorem 2.1.2 of [2]. Polynomials $f_1(x), f_2(x), \ldots, f_n(x)$ are elements of $\mathbb{Q}[x]$, the PID of polynomials with coefficients in the field of rational numbers. Therefore there is an effective procedure to find $u_1(x), u_2(x), \ldots, u_n(x) \in \mathbb{Q}[x]$ such that $1 = u_1(x)f_1(x) + u_2(x)f_2(x) + \ldots + u_n(x)f_n(x)$. Find common denominator in the right hand side and multiply by it both sides to obtain $c = u_1'(x)f_1(x) + u_2'(x)f_2(x) + \ldots + u_n'(x)f_n(x)$, where $u_i'(x) \in \mathbb{Z}[x]$ for $i = 1, 2, \ldots, n$, and $c \in A - \{0\}$.

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 an arbitrary polynomial of $\mathbb{Z}[x]$, there is an effective procedure to decide whether or not $f(x) \in A$.

Proof. Suppose $A$ is a primitive proper ideal of $\mathbb{Z}[x]$ with minimal basis given by $\{g_m(x), \ldots, g_1(x), g_0(x)\}$. Let $f(x) \in \mathbb{Z}[x]$.

If $\deg f(x) = n \leq m$, then using Proposition 1, $f(x) \in A$ if and only if there exist $a_0, a_1, \ldots, a_n$ such that $f(x) = a_0g_m(x) + \ldots + a_0g_0(x)$.

If $\deg f(x) = n > m$, then, by Proposition 1, $f(x) \in A$ if and only if there exist $a_0, a_1, \ldots, a_m, \ldots, a_n$ such that $f(x) = a_0x^n - m g_m(x) + \ldots + a_m g_m(x) + \ldots + a_0 g_0(x)$.

In any case we can decide effectively whether or not a system of $n$ equations with $n$ variables has solution.

Theorem 2. 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 $\gcd(f_1(x), f_2(x), \ldots, f_n(x))$. To show this, given $f_1(x), f_2(x) \in \mathbb{Z}[x]$, we give an effective procedure to find $\gcd(f_1(x), f_2(x))$. If $\deg f_1(x) = \deg f_2(x) = 0$, use the Euclidean Algorithm in $\mathbb{Z}$. If $\deg f_1(x) = 0$ and $\deg f_2(x) \geq 1$, then $f_2(x) = C(f_2(x))f'_2(x)$, with $f'_2(x)$ primitive. Then $\gcd(f_1(x), f_2(x)) = \gcd(f_1(x), C(f_2(x)))$ and we can use the Euclidean Algorithm in $\mathbb{Z}$. If $\deg f_1(x), \deg f_2(x) \geq 1$, then $f_1(x) = C(f_1(x))f'_1(x)$ and $f_2(x) = C(f_2(x))f'_2(x)$, with $f'_1(x), f'_2(x)$ primitive. Therefore

$$\gcd(f_1(x), f_2(x)) = \gcd(C(f_1(x)), C(f_2(x))) \gcd(f'_1(x), f'_2(x)).$$
To find \( \gcd(C(f_1(x)), C(f_2(x))) \) we can use the Euclidean algorithm in \( \mathbb{Z} \) and to find the \( \gcd(f'_1(x), f'_2(x)) \) we can use a modification of the Euclidean algorithm in \( \mathbb{Q}[x] \). Since \( \gcd(a, b, c) = \gcd(\gcd(a, b), c) \), then the claim is proved. 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 find 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 3, 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 1, 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 2 there is a bound in the degree of the ideals \( \langle C \rangle \) 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 4, 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 \( \langle C \rangle \subseteq \langle h_1(x), h_2(x), \ldots, h_n(x) \rangle \).

If we obtain positive answer in both containments, the proof is complete, otherwise pick a different minimal basis \( C \) such that \( \langle C \rangle \) contains \( c \) and note that in finitely many steps we obtain the desired minimal basis.

Note that in order to verify \( \langle C \rangle \subseteq \langle h_1(x), h_2(x), \ldots, h_n(x) \rangle \) in the previous theorem, it is not necessary to use an algorithm for detachability of ideals of \( \mathbb{Z}[x] \). Since there are finitely many ideals \( \langle C \rangle \) that we have to consider, it is enough to have a list of the elements of \( \mathbb{Z}[x] \times \mathbb{Z}[x] \times \ldots \times \mathbb{Z}[x] \) \( n \) times.

**References**


Received 18 April 2002
Revised 12 February 2003