Proyecciones Journal of Mathematics
Vol. 33, N^o 1, pp. 1-12, March 2014.
Universidad Católica del Norte
Antofagasta - Chile
DOI: 10.4067/S0716-09172014000100001

A primality test for submodules using Grobner basis

Sandra Barragán Moreno
Universidad de Bogotá Jorge Tadeo Lozano, Colombia
Received : January 2012. Accepted : November 2013

Abstract

In this paper, an algorithm is presented to check if a submodule of the free module $R[\mathbf{X}]^s$ is prime, using Gröbner Basis.

Keywords : *Gröbner Basis, prime submodule, primality test, modules.*

Subjclass [2000] Primary : *13P10. Secondary: 13E05.*

1. Introduction

Gianni, Trager and Zacharias [3] present an algorithm to check whether an ideal of the polynomial ring $R[\mathbf{X}]$ is prime, where R is a commutative Noetherian ring with unit and $\mathbf{X}$ is the set of indeterminates $x_1, \dots x_n$. In this article, the Preliminary Results section presents some conclusions from that paper. The Primality Test section includes some important definitions and basic affirmations to enunciate and prove lemmas and theorems in support of the new algorithm for prime submodules. Finally, in the Examples section this algorithm is illustrated.

2. Preliminary results

Let R be a commutative Noetherian ring with identity. $R[\mathbf{X}]^s$ is a free module where $\mathbf{X}$ is the set of indeterminates $x_1, \dots x_n$.

Definition 2.1. *[4] A submodule N of a module M over a ring R is said to be a prime submodule if $N \neq M$, and $r \in R$ and $m \in M$ satisfy $rm \in N$, so that $r \in (N : M)$ or $m \in N$.*

Lemma 2.2. *[5] A submodule N of an R-module M is prime if and only if $P = (N : M)$ is a prime ideal of R and the RP-module MN is torsion-free.*

Example 2.3. *If N is a submodule of an R-module M such that $(N : M)$ is a maximal ideal of R, then N is a prime submodule. Also, if N is a maximal submodule of an R-module M, then N is a prime submodule. Moreover, let R be an integral domain and let N be a submodule of an R-module M such that $(N : M) = 0$. In this case, N is a prime submodule.*

The primality test of Gianni, Trager and Zacharias for ideals of a polynomial ring is directly quoted below from [3].

Algorithm 2.4. *ALGORITHM PT $(R; x; I)$ Primality test for ideals.*

INPUT:	Ring R; variables $x = x_1, \ldots x_n$; ideal $I \subset R[\mathbf{X}]$.
OUTPUT:	TRUE if I is prime, otherwise FALSE.
Step 1:	If $n = 0$ then $I \subset R$ is prime the return TRUE otherwise return FALSE.
Step 2:	Compute $J = I \cap R[x_2, \ldots x_n]$.
Step 3:	If $PT(R; x_2, \ldots x_n; J) =$ FALSE then return to FALSE.
Step 4:	Let $R' = R[x_2, \ldots x_n] J$; $I' = IR'[x_1]$, $K' =$ the quotient field of R'.
Step 5:	Compute $I'K'[x_1] = \langle f \rangle$.
Step 6:	If f is not irreducible over K' then return FALSE.
Step 7:	Compute $I^{ec} = I'K'[x_1] \cap R'[x_1]$.
Step 8:	If $I^{ec} \subset I'$ then return TRUE, otherwise return FALSE.

Definition 2.5. *$Lt(G) = \langle lt(g) : g \in G \rangle$, the submodule generated by the leading terms of G.*

The proofs of the statements below, for Lemma 2.6, Corollary 2.7 and Proposition 2.8 can be found in [6].

Lemma 2.6. *Let $V \subset S$ be multiplicatively closed subsets of R, and $N \subset R[\mathbf{X}]^s$ be a submodule. If*

$$S^{-1}Lt(N) \cap R[\mathbf{X}]^s = V^{-1}Lt(N) \cap R[\mathbf{X}]^s$$

then

$$S^{-1}N \cap R[\mathbf{X}]^s = V^{-1}N \cap R[\mathbf{X}].$$

Corollary 2.7. *Let $S \subset R$ be a multiplicatively closed set and $N \subset R[\mathbf{X}]^s$ be a submodule. If $a \in S$ exists such that*

$$S^{-1}Lt(N) \cap R[\mathbf{X}]^s = (R_a[\mathbf{X}]\, Lt(N)) \cap R[\mathbf{X}]^s$$

then

$$S^{-1}N \cap R[\mathbf{X}]^s = R_a[\mathbf{X}]\, N \cap R[\mathbf{X}]^s.$$

Proposition 2.8. *Let R be an integral domain, $\langle p \rangle \subset R$ be a principal prime ideal, and N be a submodule of $R[\mathbf{X}]^s$. Then, it is possible to find a, $a \in R - \langle p \rangle$ such that*

$$R_{\langle p \rangle}[\mathbf{X}]\, N \cap R[\mathbf{X}]^s = R_a[\mathbf{X}]\, N \cap R[\mathbf{X}]^s.$$

3. Primality test

In this section, lemmas and theorems that justify the new algorithm for prime submodules are stated, as well as some explanations. At the end of this section, the algorithm is presented.

Corollary 3.1. *Let R be an integral domain and K be the quotient field of R. Then for a submodule N of $R[\mathbf{X}]^s$, $K[\mathbf{X}]N \cap R[\mathbf{X}]^s$ can be found.*

The proofs for the following results correspond to the ones used for ideals.

Lemma 3.2. *Let $f: M \longrightarrow N$ be an R-homomorphism of modules. If f is an epimorphism and B is a proper submodule of N, then*

$$B \text{ is a prime submodule} \Rightarrow f^{-1}(B) \text{ is a prime submodule.}$$

Lemma 3.3. *Let $f: M \longrightarrow N$ be an R-homomorphism of modules. If f is an epimorphism, B is a proper submodule of N and U is a proper submodule of M such that $\ker(f) \subseteq U$, then*

$$U \text{ is a prime submodule} \Rightarrow f^{-1}(U) \text{ is a prime submodule.}$$

Lemma 3.4. *Let N be a submodule of $R[\mathbf{X}]^s$. Then N is a prime submodule if and only if the image of N in $((R(N : R[\mathbf{X}]^s) \cap R)[\mathbf{X}])^s$ is a prime submodule. Moreover, $(N : R[\mathbf{X}]^s) \cap R$ is a prime ideal.*

Proof. Let $R' = R((N : R[\mathbf{X}]^s) \cap R)$. Now, five homomorphisms are defined

j: $\mathrm{R} \longrightarrow R'$
$r \mapsto j(r) = \overline{r}$

$t: \quad R[\mathbf{X}] \longrightarrow R'[\mathbf{X}]$
$f = \sum_{i=1}^{l} a_i X_i \mapsto t(f) = \overline{f} = \sum_{i=1}^{l} \overline{a_i} X_i$

T: $\mathrm{R}[\mathbf{X}]^s \longrightarrow R'[\mathbf{X}]^s$
$(f_1, \ldots, f_s) \mapsto T((f_1, \ldots, f_s)) = (t(f_1), \ldots, t(f_s))$

$\phi: \quad R'[\mathbf{X}] \longrightarrow R[\mathbf{X}](N : R[\mathbf{X}]^s)$

$\overline{f} = \sum_{i=1}^{l} \overline{a_i} X_i \mapsto \phi\left(\overline{f}\right) = \sum_{i=1}^{l} \widehat{a_i} X_i$

$$\begin{array}{ll} \Phi: & R'[\mathbf{X}]^s \longrightarrow (R[\mathbf{X}](N : R[\mathbf{X}]^s))^s \\ \left(\overline{f_1}, \ldots, \overline{f_s}\right) \mapsto \Phi\left(\left(\overline{f_1}, \ldots, \overline{f_s}\right)\right) & = \left(\phi\left(\overline{f_1}\right), \ldots, \phi\left(\overline{f_s}\right)\right). \end{array}$$

It is straightforward to prove that ϕ and Φ are well-defined, so their proofs are not presented here.

Given $\ker(\Phi) = T((N : R[\mathbf{X}]^s)^s)$, and using Lemmas 3.2 and 3.3, N is a prime submodule if and only if $T(N)$ is also prime.

Finally, if N is a prime submodule, then $(N : R[\mathbf{X}]^s)$ is a prime ideal of $R[\mathbf{X}]$ and the homomorphism

$$\begin{array}{rccc} i: & R & \longrightarrow & R[\mathbf{X}] \\ & r & \mapsto & i(r) = r \end{array}$$

$i^{-1}((N : R[\mathbf{X}]^s)) = (N : R[\mathbf{X}]^s) \cap R$ turns out to be prime. □

Lemma 3.5 is provided by [6]. Nevertheless, due to its importance, its proof is analyzed here.

Lemma 3.5. *Let R be an integral domain, N be a submodule of $R[\mathbf{X}]^s$, and $\langle p\rangle \subset R$ be a principal prime ideal. Thus it is possible to find $g \in R - \langle p\rangle$ such that*

$$N = (N + gR[\mathbf{X}]^s) \cap \left(R_{\langle p\rangle}[\mathbf{X}] N \cap R[\mathbf{X}]^s\right).$$

Proof. Recall from Proposition 2.8 that it is possible to find $a \in R - \langle p\rangle$, and therefore

$$R_{\langle p\rangle}[\mathbf{X}] N \cap R[\mathbf{X}]^s = R_a[\mathbf{X}] N \cap R[\mathbf{X}]^s.$$

Since $R[\mathbf{X}]^s$ is Noetherian, $m \geq 0$ exists so that

$$a^m \left(R_{\langle p\rangle}[\mathbf{X}] N \cap R[\mathbf{X}]^s\right) \subseteq N.$$

Letting $g = a^m$, it is observed that

$$N \subseteq (N + gR[\mathbf{X}]^s) \cap \left(R_{\langle p\rangle}[\mathbf{X}] N \cap R[\mathbf{X}]^s\right).$$

Let $\mathbf{F} \in (N + gR[\mathbf{X}]^s) \cap \left(R_{\langle p\rangle}[\mathbf{X}] N \cap R[\mathbf{X}]^s\right)$. Then $\mathbf{F} = \mathbf{w} + g\mathbf{v}$, $\mathbf{w} \in N$ and $\mathbf{v} \in R[\mathbf{X}]^s$. Now, $g\mathbf{F} \in N$ so that $g^2\mathbf{v} \in N$. As a result, $\mathbf{v} \in R_a[\mathbf{X}] N \cap R[\mathbf{X}]^s$ and $g\mathbf{v} \in N$, thus $\mathbf{F} \in N$. □

Corollary 3.6. *Let R be an integral domain with quotient field K and N be an $R[\mathbf{X}]^s$-submodule. Therefore, it is possible to find $g \in R - \{0\}$ such that*

$$N = (N + gR[\mathbf{X}]^s) \cap (K[\mathbf{X}]N \cap R[\mathbf{X}]^s).$$

Proof. This is merely a direct application of Lemma 3.5 with $p = 0$. □

Lemma 3.7. *Let R be an integral domain with quotient field K and $N \subseteq R[\mathbf{X}]^s$ be a submodule. If N is prime in $R[\mathbf{X}]^s$ within the $R[\mathbf{X}]$-module, then $K[\mathbf{X}]N$ is prime in $K[\mathbf{X}]^s$ as a $K[\mathbf{X}]$-module.*

Proof. If $r \in K[\mathbf{X}]$ and $\mathbf{m} \in K[\mathbf{X}]^s$ with $r\mathbf{m} \in K[\mathbf{X}]N$, then $r \in (K[\mathbf{X}]N : K[\mathbf{X}]^s)$ or $\mathbf{m} \in K[\mathbf{X}]N$. Supposing that

$$r \notin (K[\mathbf{X}]N : K[\mathbf{X}]^s),$$

since $r\mathbf{m} \in K[\mathbf{X}]N$, then $r = \frac{r'}{d'}$ where $r' \in R[\mathbf{X}]$ and $d' \in R - \{0\}$; in this way, $r\mathbf{m} = \frac{r'}{d'}\mathbf{m} = \frac{u}{d}$, $\mathbf{u} \in N$ and $d \in R - \{0\}$, so $dr'\mathbf{m} = d'\mathbf{u} \in \mathbf{N}$. When N is prime, it is possible to affirm that $dr' \in (N : R[\mathbf{X}]^s)$ or $\mathbf{m} \in N$.

If $dr' \in (N : R[\mathbf{X}]^s)$ then $dr' = a \in (N : R[\mathbf{X}]^s)$; thus $r' = \frac{a}{d}$. Let $q \in K[\mathbf{X}]^s$, where $q = \frac{w}{t}$, $w \in R[\mathbf{X}]^s$, and $t \in R - \{0\}$. In this case, $rq = \frac{r'}{d'}\frac{w}{t} = \frac{aw}{d'dt}$ with $aw \in N$ and $d'dt \in R - \{0\}$. This means that $rq \in K[\mathbf{X}]N$ for all $q \in K[\mathbf{X}]^s$, which is a contradiction. Thus, $m \in N$ which makes $m \in K[\mathbf{X}]N$. □

Lemma 3.8. *Let R be an integral domain with quotient field K, and $N \subseteq R[\mathbf{X}]^s$ be a submodule such that $N \cap R^S = \{0\}$. If N is prime as an $R[\mathbf{X}]^s$ within the $R[\mathbf{X}]$-module then $N = K[\mathbf{X}]N \cap R[\mathbf{X}]^s$.*

Proof. Applying Corollary 3.6, $N = (N + gR[\mathbf{X}]^s) \cap (K[\mathbf{X}]N \cap R[\mathbf{X}]^s)$. With the hypotheses of Lemma 3.8, $K[\mathbf{X}]N \cap R[\mathbf{X}]^s \subset N + gR[\mathbf{X}]^s$ must be proven so that

$$N = K[\mathbf{X}]N \cap R[\mathbf{X}]^s.$$

By Corollary 2.7 $K[\mathbf{X}]N \cap R[\mathbf{X}]^s = R_a[\mathbf{X}]N \cap R[\mathbf{X}]^s$ for some $a \in R - \{0\}$. Furthermore, in proof of Lemma 3.5, $R[\mathbf{X}]^s$ is Noetherian and $m \geq 0$ exists, such that

$$a^m \left(R_a \left[\mathbf{X}\right] N \cap R \left[\mathbf{X}\right]^s\right) \subseteq N.$$

Corollary 3.6 defines $g = a^m$, so that

$$R_a \left[\mathbf{X}\right] N \cap R \left[\mathbf{X}\right]^s \subseteq N + a^m R \left[\mathbf{X}\right]^s \quad (3.1)$$

where $a \in R - \{0\}$. Therefore, (3.1) is proven below.

If $a^m \left(R_a \left[\mathbf{X}\right] N \cap R \left[\mathbf{X}\right]^s\right) \subseteq N$ then $a^m \in (N : R_a \left[\mathbf{X}\right] N \cap R \left[\mathbf{X}\right]^s)$. This indicates that for all $u \in R_a \left[\mathbf{X}\right] N \cap R \left[\mathbf{X}\right]^s$, $a^m u \in N$.

For $h \in R_a \left[\mathbf{X}\right] N \cap R \left[\mathbf{X}\right]^s$, $a^m h \in N$. Now, since N is prime, $a^m \in (N : R \left[\mathbf{X}\right]^s)$ or $h \in N$.

If $a^m \in (N : R \left[\mathbf{X}\right]^s)$, then $a^m R \left[\mathbf{X}\right]^s \subseteq N$. Thus $a^m \left(1, 1, \ldots, 1\right) \in N$ implies that

$$(a^m, a^m, \ldots, a^m) \in N \cap R^S$$

due to $a \in R - \{0\}$, however $N \cap R^S = \{0\}$. As a result, $a^m = 0$, so $a = 0$, which is a contradiction, thus $h \in N \subseteq N + a^m R \left[\mathbf{X}\right]$. □

Lemma 3.9. *Let R be an integral domain with quotient field K, and $N \subseteq R \left[\mathbf{X}\right]^s$ be a submodule. If $K \left[\mathbf{X}\right]^s$ is considered to be a $K \left[\mathbf{X}\right]$-module and $N = K \left[\mathbf{X}\right] N \cap R \left[\mathbf{X}\right]^s$, then N is prime in $R \left[\mathbf{X}\right]^s$ as an $R \left[\mathbf{X}\right]$-module.*

Proof. Let $r \in R \left[\mathbf{X}\right]$ and $m \in R \left[\mathbf{X}\right]^s$ such that $rm \in N$; hence $r \in (N : R \left[\mathbf{X}\right]^s)$ or $m \in N$ should be proven. It is assumed that $r \notin (N : R \left[\mathbf{X}\right]^s)$; as a consequence, $m' \in R \left[\mathbf{X}\right]^s$ exists such that $rm' \notin N$. Because $rm \in N$, $rm \in K \left[\mathbf{X}\right] N$, implying that $r \in (K \left[\mathbf{X}\right] N : K \left[\mathbf{X}\right]^s)$ or $m \in K \left[\mathbf{X}\right] N$.

If $r \in (K \left[\mathbf{X}\right] N : K \left[\mathbf{X}\right]^s)$, since $m' \in R \left[\mathbf{X}\right]^s \subseteq K \left[\mathbf{X}\right]^s$, then $rm' \in K \left[\mathbf{X}\right] N \cap R \left[\mathbf{X}\right]^s = N$, but this is a contradiction.

Therefore, $m \in K \in \left[\mathbf{X}\right] N$ and since $m \in R \left[\mathbf{X}\right]^s$, then $m \in K \left[\mathbf{X}\right] N \cap R \left[\mathbf{X}\right]^s = N$. □

Theorem 3.10. *Let R be an integral domain with quotient field K, and $N \subseteq R \left[\mathbf{X}\right]^s$ be a submodule such that $N \cap R^s = \{0\}$. Thus, N is prime in $R \left[\mathbf{X}\right]^s$ as an $R \left[\mathbf{X}\right]$-module if and only if $K \left[\mathbf{X}\right] N$ is prime in $K \left[\mathbf{X}\right]^s$ within the $K \left[\mathbf{X}\right]$-module and $N = K \left[\mathbf{X}\right] N \cap R \left[\mathbf{X}\right]^s$.*

Proof. This follows immediately from Lemmas 3.7, 3.8 and 3.9. □

Corollary 3.11. *Let N be a submodule of $R[x]^s$. Thus N is a prime submodule if and only if*

(i) $(N : R[x]^s) \cap R$ is a prime ideal of R.

(ii) Letting $R' = R((N : R[x]^s) \cap R)$, K' be the quotient field of R' and N' be the image of N in $R'[x]^s$, then $K'[x]N'$ is prime in $K'[x]^s$ as a $K'[x]$-module and $N' = K'[x]N' \cap R'[x]^s$.

Proof. ($\Leftarrow$ Using Lemma 3.9 with those hypotheses, it is clear that N' is a prime submodule of $R'[x]^s$ within the $R'[x]$-module, and with Lemma 3.4, it is possible to see that N is prime.

$\Rightarrow$) Applying Lemma 3.4, it is possible to prove that $(N : R[x]^s) \cap R$ is a prime ideal of R.

$N' \cap R'^s = \{\overline{\mathbf{0}}\}$ is proven, using Lemma 3.8.

Letting $\left(\overline{f_1}, \ldots, \overline{f_s}\right) \in N' \cap R'^s = T(N) \cap R'^s$ with T defined as in Lemma 3.4, then

$$\left(\overline{f_1}, \ldots, \overline{f_s}\right) \in T(N) \text{ and } \left(\overline{f_1}, \ldots, \overline{f_s}\right) \in R'^s.$$

In this way $(n_1, \ldots, n_s) \in N$ exists, such that
$T((n_1, \ldots, n_s)) = \left(\overline{f_1}, \ldots, \overline{f_s}\right)$ where $\overline{f_i}$ is constant in R'^s; thus $f_i \in R'$, and $T((n_1, \ldots, n_s)) = (t(n_1), \ldots, t(n_s)) = \left(\overline{f_1}, \ldots, \overline{f_s}\right)$ with t defined as in Lemma 3.4, which implies that $t(n_i) = \overline{f_i} = \overline{0}$. Therefore,
$T((n_1, \ldots, n_s)) = (\overline{0}, \ldots, \overline{0})$. □

Algorithm 3.12. *ALGORITHM PTM $(R; \mathbf{X}; N; s)$ Primality Test for Submodules.*

4. Examples

Two examples are presented below to illustrate how the algorithm works. Firstly, the algorithm is used to show a submodule that is not prime, and secondly, it is used to identify a prime submodule.

Example 4.1. *Let* $N = \langle \mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4 \rangle \subseteq (Q[x,y])^3$, *where*

$$\begin{aligned} \mathbf{f}_1 &= (xy, y, x), \quad & \mathbf{f}_2 &= \left(x^2 + x, y + x^{2,y}\right), \\ \mathbf{f}_3 &= (-y, x, y), \quad & \mathbf{f}_4 &= \left(x^2, x, y\right). \end{aligned}$$

Using TOP ordering on $(Q[x,y])^3$ *with* $\mathbf{e}_1 > \mathbf{e}_2 > \mathbf{e}_3$ *and considering the order lex on* $Q[x,y]$, $x > y$, *with the algorithm PTM it is concluded that* N *is not a prime submodule of* $(Q[x,y])^3$.

Example 4.2. *Consider the following vectors*

$$\begin{array}{lll} \mathbf{f}_1 = (0, x^3), & \mathbf{f}_2 = (y - x^2, 0), & \mathbf{f}_3 = (x^3 + 1, x), \\ \mathbf{f}_4 = (0, y - x^2), & \mathbf{f}_5 = (x^2 - x + 1, 0), & \mathbf{f}_6 = (0, x^2 - x + 1) \end{array}$$

All of them belong to $((Q[x])[y])^2$. *Using POT ordering on* $((Q[x])[y])^2$ *with* $\mathbf{e}_1 > \mathbf{e}_2$, *considering the order lex on* $(Q[x])[y]$ *with* $y > x$, *and letting* $N = \{\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4, \mathbf{f}_5, \mathbf{f}_6\}$, *the algorithm PTM is implemented to determine whether* N *is a prime submodule of* $((Q[x])[y])^2$.

$PTM\left(Q\left[x\right], y, N, 2\right)$

References

[1] Adams, W., & Loustaunau, P. An Introduction to Gröbner Bases. Providence, Rhode Island, United States of America: American Mathematical Society, (1994).

[2] Barragán, S. La Condición de Noether para el espectro primo de un módulo sobre un anillo conmutativo. Universidad Nacional de Colombia. Tesis de Maestría, (2001).

[3] Gianni, P., Trager, B., & Zacharias, G. Gröbner Bases and Primary Decomposition of Polinomial Ideals. Journal of Symbolic Computation, pp. 149-167, (1988).

[4] Lu, C. P. Prime Submodules of Modules. Commentarii Mathematici Universitastis Sancti Pauli, pp. 61-69, (1984).

[5] McCasland, R., Moore, M., & Smith, P. On the spectrum of a module over commutative ring. Communications in Algebra, pp. 79-103, (1997).

[6] Rutman, E. Gröbner Bases and Primary Decomposition of Modules. Journal of Symbolic Computation, pp. 483-503, (1992).

Sandra Patricia Barragán Moreno
Universidad de Bogotá Jorge Tadeo Lozano
Colombia
e-mail : sandra.barragan@utadeo.edu.co