Gröbner bases and products of coefficient rings

This item was submitted to Loughborough University's Institutional Repository by the/an author.


Additional Information:

- This article was published in the journal, Bulletin of the Australian Mathematical Society [© Australian Mathematical Society]

Metadata Record: https://dspace.lboro.ac.uk/2134/2321

Publisher: © Australian Mathematical Society

Please cite the published version.
This item was submitted to Loughborough’s Institutional Repository by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
http://creativecommons.org/licenses/by-nc-nd/2.5/
Gröbner bases and products of coefficient rings. *

Graham H. Norton, Dept. Mathematics, Univ. of Queensland, Brisbane
Ana Sälēgean, Dept. Mathematics, Nottingham Trent Univ., Nottingham, U.K.

Abstract
Suppose that \( A \) is a finite direct product of commutative rings. We show from first principles that a Gröbner basis for an ideal of \( A[x_1, \ldots, x_n] \) can be easily obtained by 'joining' Gröbner bases of the projected ideals with coefficients in the factors of \( A \) (which can themselves be obtained in parallel). Similarly for strong Gröbner bases. This gives an elementary method of constructing a (strong) Gröbner basis when the Chinese Remainder Theorem applies to the coefficient ring and we know how to compute (strong) Gröbner bases in each factor.

Subject Classification: 13F10, 13M10, 13P10.

1 Introduction
Let \( A \) be a commutative ring with \( 1 \neq 0 \). We are interested in obtaining a (strong) Gröbner basis of a non-zero ideal \( I \) of \( A[x_1, \ldots, x_n] \) when \( A = A_1 \times \cdots \times A_m \) is a direct product of rings and we know how to obtain (strong) Gröbner bases of the projected ideals \( \pi_i(I) \) for \( i = 1, \ldots, m \). We show that this can be done by 'joining' (strong) Gröbner bases for the \( \pi_i(I) \) of \( A_i[x_1, \ldots, x_n] \). Thus we can compute a (strong) Gröbner basis for \( I \) when we know algorithms for computing a (strong) Gröbner basis for \( \pi_i(I) \). As an application, we compute a (strong) Gröbner basis for \( I \) when the Chinese Remainder Theorem applies to \( A \) and we can compute (strong) Gröbner bases in each factor. We also obtain another proof that strong Gröbner bases exist over a principal ideal ring.

The preliminary Section 2 recalls the necessary background on (strong) Gröbner bases from [1, 3]. Section 3 discusses the join of Gröbner bases while Section 4 describes the strong join of strong Gröbner bases. We conclude with some algorithmic remarks and examples.

2 Preliminaries

2.1 Gröbner bases

We have \( A = A_1 \times \cdots \times A_m \) and we write \( A[x] \) for \( A[x_1, \ldots, x_n] \). The monoid of terms in \( x_1, \ldots, x_n \) is denoted by \( T \). Let \( < \) be a fixed but arbitrary admissible order on \( T \). Throughout the paper, we use the same term order \( < \) on each \( A_i[x] \) as on \( A[x] \).

If \( f = \sum_{t \in T} f_t t \in A[x] \setminus \{0\} \) and \( v = \max\{t \in T : f_t \neq 0\} \) then \( v \) is the leading term, \( f_v \) the leading coefficient and \( f_v t \) the leading monomial of \( f \), denoted \( \text{lt}(f), \text{lc}(f) \) and \( \text{lm}(f) \) respectively. We also write \( \text{lm}(S) \) for \( \{\text{lm}(f) : f \in S\} \) where \( S \subset A[x] \setminus \{0\} \).

---

*Research supported by the U.K. Engineering and Physical Sciences Research Council under Grant L07680 in the Algebraic Coding Research Group, Centre for Communications Research, University of Bristol, U.K.
Let $G \subset A[x] \setminus \{0\}$ be finite. Then $f \in A[x]$ has a standard representation wrt. $G$ if $f = \sum_{j=1}^{k} c(j) t(j) g(j)$ for some $c(j) \in A \setminus \{0\}$, $t(j) \in T$, $g(j) \in G$ such that $t(j) \text{lt}(g(j)) \leq \text{lt}(f)$, [2, p. 218]. We write $\text{Std}(G)$ for the polynomials which have a standard representation wrt. $G$.

Also, if $G \subset A[x] \setminus \{0\}$ is finite, then $G$ is a Gröbner basis (GB) for a non-zero ideal $I \subset A[x]$ if and only if $I = \text{Std}(G)$, [1, Theorem 4.1.12]. We refer the reader to [3, Sections 3.1, 4.3] for the notions of reduction wrt. $G$, $\rightarrow_G^*$, an S-polynomial $\text{Spol}(g_1, g_2)$ and an A-polynomial $\text{Apol}(g)$, where $g_1, g_2, g \in A[x] \setminus \{0\}$. We will need the following result:

**Theorem 2.1** ([3, Theorem 4.10]) Let $A$ be a principal ideal ring and $G \subset A[x] \setminus \{0\}$, $|G| < \infty$. Then $G$ is a GB if and only if (A) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in \text{Spol}(g_1, g_2)$ such that $h \rightarrow_G^* 0$ and (B) for any $g \in G$, there is an $h \in \text{Apol}(g)$ such that $h \rightarrow_G^* 0$.

2.2 Strong Gröbner bases

Recall that if $G \subset A[x] \setminus \{0\}$ is finite, then $G$ is a strong Gröbner basis (SGB) for $I = \langle G \rangle$ if and only if for any $f \in I$ there is a $g \in G$ such that $\text{lm}(g) \mid \text{lm}(f)$, [1, Definition 4.5.6]. We refer the reader to [3, Sections 3.1, 5.1] for the notions of strong reduction wrt. $G$, $\rightarrow_G^*$, the strong remainder $\text{SRem}(g)$ of a polynomial wrt. $G$ and a $G$-polynomial $\text{Gpol}(g_1, g_2)$ of $g_1, g_2 \in A[x] \setminus \{0\}$.

**Proposition 2.2** ([3, Proposition 3.9]) Let $A$ be a finite-chain ring. Then $G$ is a GB if and only if $G$ is an SGB.

**Corollary 2.3** ([3, Corollary 5.12]) Let $A$ be a principal ideal ring and let $G \subset A[x] \setminus \{0\}$ be a finite set. Then $G$ is an SGB if and only if

(A) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in \text{Spol}(g_1, g_2)$ such that $h \rightarrow_G^* 0$,

(B) for any $g \in G$, there is an $h \in \text{Apol}(g)$ such that $h \rightarrow_G^* 0$ and

(C) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$ some $h \in \text{Gpol}(g_1, g_2)$ is strongly reducible wrt. to $G$.

Recall that an SGB $G$ is called minimal if no proper subset of $G$ is an SGB for $\langle G \rangle$.

3 The join

The projections $\pi_i : A \rightarrow A_i$ induce maps $\pi_i : A[x] \rightarrow A_i[x]$. It is straightforward to check that the induced map $\pi : A[x] \rightarrow A_1[x] \times \cdots \times A_m[x]$ given by $\pi(f) = (\pi_1(f), \ldots, \pi_m(f))$ and the map $\kappa : A_1[x] \times \cdots \times A_m[x] \rightarrow A[x]$, which collects coefficients of like terms, are mutually inverse ring homomorphisms. We relate GB’s of $I \subset A[x]$ to GB’s of $\pi_i(I) \subset A_i[x]$, where $1 \leq j \leq m$.

**Proposition 3.1** If $G$ is a GB for a non-zero ideal $I \subset A[x]$, then $\pi_i(G) \setminus \{0\}$ is a GB for $\pi_i(I)$ in $A_i[x]$ for $i = 1, \ldots, m$.

**Proof.** We can assume that $i = 1$. Let $f_1 \in \pi_1(I) \setminus \{0\} \subset A_1[x]$ and put $G_1 = \pi_1(G) \setminus \{0\}$. We show that $f_1 \in \text{Std}(G_1)$. For let $f = \kappa(f_1, 0, \ldots, 0) \in I \setminus \{0\}$. We have $\text{lm}(f) = (\text{lc}(f_1), 0, \ldots, 0) \text{lt}(f_1)$, so that $\text{lt}(f) = \text{lt}(f_1)$. Since $G$ is a Gröbner basis for $I$, $f = \sum_{j=1}^{k} c(j) t(j) g(j)$ for some $c(j) \in A \setminus \{0\}$, $t(j) \in T$, $g(j) \in G$ with $t(j) \text{lt}(g(j)) \leq \text{lt}(f) = \text{lt}(f_1)$. Then $f_1 = \sum_{j=1}^{k} \pi_1(c(j)) t(j) \pi_1(g(j))$ for some $1 \leq j_1 < \cdots < j_k \leq k$ with all $\pi_1(c(j))$ and $\pi_1(g(j))$ non-zero. We have $t(j) \text{lt}(\pi_1(g(j))) \leq t(j) \text{lt}(g(j)) \leq \text{lt}(f) = \text{lt}(f_1)$, i.e. $f_1 \in \text{Std}(G_1)$ and $G_1$ is a GB for $\pi_1(I)$. □

**Definition 3.2** Let $G_i \subset A_i[x] \setminus \{0\}$ for $i = 1, 2$. Then, $G_1 \sqcup G_2$, the join of $G_1$ and $G_2$ is the subset $G_1 \times \{0\} \cup \{0\} \times G_2$ of $A_1[x] \times A_2[x]$. 

2
Proposition 3.3 Let $I$ be a non-zero ideal of $A[x]$ and $G_i \subset A_i[x] \setminus \{0\}$ for $i = 1, \ldots, m$. Then \(\kappa(G_1 \sqcup \cdots \sqcup G_m)\) is a GB for $I$ if and only if each $G_i$ is a GB for $\pi_i(I)$ for $i = 1, \ldots, m$.

Proof. Note first that $0 \not\in H = \kappa(G_1 \sqcup \cdots \sqcup G_m)$. We show $I \subset \text{Std}(H)$ if each $G_i$ is a GB. Let $f \in I \setminus \{0\}$. Since $\pi_i(f) \in \pi_i(I) = \text{Std}(G_i)$, we can write $\pi_i(f) = \sum_{j=1}^{k_i} c_i^{(j)} t_i^{(j)} g_i^{(j)}$ for some $k_i \geq 1$, $c_i^{(j)} \in A \setminus \{0\}$, $t_i^{(j)} \in G_i$ with $t_i^{(j)} \lt(g_i^{(j)}) \leq \lt(\pi_i(f)) \leq \lt(f)$. Then

\[
f = \kappa(\pi_1(f), \ldots, \pi_m(f))
\]

\[
= \kappa\left(\sum_{j=1}^{k_1} c_1^{(j)} t_1^{(j)} g_1^{(j)}, 0, \ldots, 0\right) + \cdots + \kappa\left(0, \ldots, 0, \sum_{j=1}^{k_m} c_m^{(j)} t_m^{(j)} g_m^{(j)}\right)
\]

\[
= \sum_{j=1}^{k_1} c_1^{(j)} t_1^{(j)} \kappa(g_1^{(j)}, 0, \ldots, 0) + \cdots + \sum_{j=1}^{k_m} c_m^{(j)} t_m^{(j)} \kappa(0, \ldots, 0, g_m^{(j)}).
\]

Now $\kappa(0, \ldots, 0, g_i^{(j)}, 0, \ldots, 0) \in H$ and $t_i^{(j)} \lt(\kappa(0, \ldots, 0, g_i^{(j)}, 0, \ldots, 0)) = t_i^{(j)} \lt(g_i^{(j)}) \leq \lt(f)$ for $j = 1, \ldots, k_i$ and $i = 1, \ldots, m$, so that $f \in \text{Std}(H)$. The converse follows immediately from Proposition 3.1.

Example 3.4 Let $f = 2x^2 + 3x + 1 \in \mathbb{Z}_6[x]$. We obtain a GB for $\langle f \rangle$ as follows. The usual isomorphism $\chi : \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$ induces an isomorphism $\chi : \mathbb{Z}_6[x] \rightarrow (\mathbb{Z}_2 \times \mathbb{Z}_3)[x]$ and $\chi(f) = (0,2)x^2 + (1,0)x + (1,1)$. We have $\pi \chi(f) = x + 1 \in \mathbb{Z}_2[x] \times \mathbb{Z}_3[x]$ and clearly $\{x + 1\}$ and $\{x^2 + 1\}$ are GB’s in $\mathbb{Z}_2[x]$ and $\mathbb{Z}_3[x]$ respectively. By Proposition 3.3, $\kappa(\{x + 1\} \sqcup \{x^2 + 2\}) = \{1,0\}x + (1,0), (0,1)x^2 + (0,2)\}$ is a GB for $\langle \chi(f) \rangle$ and we deduce that $\chi^{-1} \kappa(\{x + 1\} \sqcup \{x^2 + 2\}) = \{3(x + 1), 4x^2 + 2\}$ is a GB for $\langle f \rangle$.

4 The strong join

First note that $G = \{3(x + 1), 4x^2 + 2\}$ is not an SGB for $\langle G \rangle$ in Example 3.4: $x^2 - 3x + 2 = 4x^2 + 2 - 3x(x + 1) \in \langle G \rangle$, but 3 and 4 are not units in $\mathbb{Z}_6$, so there is no $g \in G$ such that $\text{lcm}(g) \mid \text{lcm}(x^2 - 3x + 2)$. We now show how to obtain an SGB in $A[x]$ from SGB’s in the $A_i[x]$.

Proposition 4.1 If $G$ is a SGB for a non-zero ideal $I \subset A[x]$ then $\pi_i(G) \setminus \{0\}$ is a SGB for $\pi_i(I)$ in $A_i[x]$ for $i = 1, \ldots, m$.

Proof. We take $i = 1$. Let $G$ be an SGB and let $f_1 \in \pi_1(I) \setminus \{0\} \subset A_1[x]$. Put $f = \kappa(f_1, 0, \ldots, 0)$ as in Proposition 3.1. There is a $g \in G$ such that $\text{lcm}(g) \mid \text{lcm}(f)$, so $\pi_1(\text{lcm}(g)) \mid \text{lcm}(f_1)$. This means that $\pi_1(\text{lcm}(g)) \neq 0$, so $\pi_1(g) \neq 0$ and $\pi_1(\text{lcm}(g)) = \text{lcm}(\pi_1(g))$. Since $\pi_1(g) \in \pi_1(G) \setminus \{0\}$, $\pi_1(G) \setminus \{0\}$ is an SGB for $\langle \pi_1(G) \rangle = \pi_1(I)$.

Definition 4.2 Let $G_i \subset A_i[x] \setminus \{0\}$ for $i = 1, 2$. Then $G_1 \sqcup G_2$, the strong join of $G_1, G_2$ is the subset $G_1 \sqcup G_2 \cup \{g_1 \cdot t_2 g_2 : g_i \in G_i, t_i = \text{lcm}(\text{lcm}(g_1), \text{lcm}(g_2))/\text{lcm}(g_i)\}$ of $A_1[x] \times A_2[x]$.

Proposition 4.3 $\kappa(G_1 \sqcup G_2 \sqcup G_3) = \kappa(G_1 \sqcup \kappa(G_2 \sqcup G_3))$.

Proof. Use the fact that in $\kappa(G_1 \sqcup G_2)$, $\text{lcm}(\text{lcm}(g_1), \text{lcm}(g_2)) = \text{lcm}(\text{lcm}(g_1), \text{lcm}(g_2))$ and that the lcm of leading terms is associative.

For $m \geq 3$ we will write $\kappa(G_1 \sqcup \cdots \sqcup G_m)$ for $\kappa(\kappa(G_1 \sqcup \cdots \sqcup G_{m-1}) \sqcup G_m)$.
Corollary 4.5 If A is a principal ideal ring then any non-zero ideal of A[x] has an SGB.

Proof. We have \( A \cong \prod_{i=1}^{m} A_i \), where each \( A_i \) a principal ideal domain or a finite-chain ring by [4, Theorem 33, Section 15, Ch. 4]. We can obtain an SGB over a principal ideal domain using e.g. [2, Algorithm D-Gröbner, p. 461]) and an SGB over an finite-chain rings using Algorithm SGB-FCR recalled in the Appendix. Hence by Theorem 4.4 we can compute an SGB for \( I \) over \( A \).

The SGB computation in each component can be done in parallel and is likely to be faster than computing an SGB over \( A \) directly. (The complexity of computing \( G_1 \sqcup \cdots \sqcup G_m \) from \( G_1, \ldots, G_m \) is \( O(\prod_{i=1}^{m} |G_i|) \)). The complexity of computing the strong join in Theorem 4.4 can be improved by minimising each \( G_i \) first. However, \( \kappa(G_1 \sqcup \cdots \sqcup G_m) \) may not be minimal and in general, a further minimisation step will be necessary. We formalise this as follows:

Algorithm 4.6

Input: \( F \subset A[x] \setminus \{0\} \), \( F \) finite, \( A = \prod_{i=1}^{m} A_i \) and we can compute an SGB over each \( A_i \).

Output: \( G \), a minimal SGB for \( \langle F \rangle \).

begin
for \( i \leftarrow 1 \) to \( m \) do
   \( G_i \leftarrow SGB_{\kappa}(\pi_i(F)) \)
   minimise \( G_i \)
end for

\( G \leftarrow G_1 \)

for \( i \leftarrow 2 \) to \( m \) do
   \( G \leftarrow \kappa(G \sqcup G_i) \)
end for

minimise \( G \)
Let $\vdash \bigcup$ and apply Algorithm 4.6 to $C \leftarrow G \leftarrow \begin{array}{l}
\end{array}$

Notes:

Output:

$G \leftarrow G \leftarrow \begin{array}{l}
\end{array}$

Algorithm 5.1

We specialise [3, Algorithm 6.4] to a finite-chain ring for the convenience of the reader.

5 Appendix

Council (EPSRC) under Grant L07680 is gratefully acknowledged.

Acknowledgements. Financial support from the U.K. Engineering and Physical Sciences Research Council (EPSRC) under Grant L07680 is gratefully acknowledged.

5 Appendix

We specialise [3, Algorithm 6.4] to a finite-chain ring for the convenience of the reader.

Algorithm 5.1

$G \leftarrow \text{SGB} - \text{FCR}(F)$

Input: $F$ a finite subset of $A[x] \setminus \{0\}$, where $A$ is a computable finite-chain ring.

Output: $G$ a strong Gröbner basis for $\langle F \rangle$.

Notes: $B$ is the set of pairs of polynomials in $G$ whose S-polynomials still have to be computed.

$C$ is the set of polynomials in $G$ whose A-polynomials still have to be computed.

begin $G \leftarrow F$

$B \leftarrow \{\{f_1, f_2\} : f_1, f_2 \in G, f_1 \neq f_2\}$

$C \leftarrow F$

In computing the strong join, we can first compute $\text{lm}(\kappa(G_1 \sqcup \cdots \sqcup G_m))$ to decide which polynomials will belong to a minimal SGB. Only these polynomials of $\kappa(G_1 \sqcup \cdots \sqcup G_m)$ need then be computed in full.

Example 4.7 (cf. [3, Example 7.3]) Let $F = \{2x^2 + 3x + 1\} \subset \mathbb{Z}_6[x]$ as in Example 3.4. We obtain an SGB for $\langle F \rangle$ by applying Algorithm 4.6 to $\chi(F)$. Firstly, $\pi\chi(F) = (x + 1, 2x^2 + 1)$ and trivially $\{x + 1\}$ and $\{x^2 + 2\}$ are minimal SGB’s in $\mathbb{Z}_2[x]$ and $\mathbb{Z}_3[x]$ respectively. We have $\{x + 1\} \sqcup \{x^2 + 2\} = \{(x + 1, 0), (0, x^2 + 2), (x^2 + x, x^2 + 2)\}$ and $G = \kappa(\{x + 1\} \sqcup \{x^2 + 2\}) = \{(1, 0)x + (1, 0), (0, 1)x^2 + (0, 2), (1, 1)x^2 + (1, 0)x + (0, 2)\}$ is an SGB for $\langle \chi(F) \rangle$. We minimise $G$ to obtain $H = \{(1, 0)x + (1, 0), (1, 1)x^2 + (1, 0)x + (0, 2)\}$. Finally $\chi^{-1}(H) = \{x^2 + 3x + 2, 3(x + 1)\}$ is a minimal SGB for $\langle F \rangle$. ![](https://s3.amazonaws.com/courses/560/560_images/560_560_560.png)

Example 4.8 (cf. [1, Example 4.2.12]) Let $F = \{4xy + x, 3x^2 + y\} \subset \mathbb{Z}_{20}[x,y]$. To compute an SGB for $\langle F \rangle$ wrt. lexicographic order with $x \succ y$, we use the usual isomorphism $\chi: \mathbb{Z}_{20} \rightarrow \mathbb{Z}_4 \times \mathbb{Z}_5$ and apply Algorithm 4.6 to $\chi(F)$. We have $\pi\chi(F) = \{(x, 4xy + x), (3x^2 + y, 3x^2 + y)\} \subset \mathbb{Z}_4[x] \times \mathbb{Z}_5[x]$.

We obtain $G_1 = \{x, y\}$ as an SGB for $\{x, 3x^2 + y\}$ using Algorithm SGB-FCR; alternatively $G_1$ is a GB by Theorem 2.1 and it is a (minimal) SGB by Proposition 2.2. In $\mathbb{Z}_5[x,y]$, we work with $\{xy + 4x, x^2 + 2y\}$. A minimal SGB is $G_2 = \{xy + 4x, x^2 + 2y, y^2 + 4y\}$. First computing $\text{lm}(\kappa(G_1 \sqcup G_2))$ yields $H = \{(1, 1)x^2 + (0, 2)y, (1, 1)xy + (0, 4)x, (1, 0)x, (1, 1)y^2 + (0, 4)y, (1, 0)y\}$ as a minimal SGB for $\langle \chi(F) \rangle$. So $\chi^{-1}(H) = \{x^2 + 12y, xy + 4x, 5x, y^2 + 4y, 5y\}$ is a minimal SGB for $\langle F \rangle$. If we write $\chi^{-1}(H) = \{g_1, \ldots, g_5\}$ using decreasing order of leading terms, then the minimal SGB $\{3(g_1 - g_5), g_2 + g_3, g_3, g_4 + 3g_5, g_5\}$ was given in [3, Example 7.3]. Note that the GB $\{3(g_1 - g_5), 4g_2, g_3, 4g_4, 3g_5\}$ of [1, Example 4.2.12] obtained using syzygy modules is not an SGB.
while $B \cup C \neq \emptyset$ do
    if $C \neq \emptyset$ then
        select $f$ from $C$
        $C \leftarrow C \setminus \{f\}$
        compute $h \in \text{Apol}(f)$
    else
        select $\{f_1, f_2\}$ from $B$
        $B \leftarrow B \setminus \{f_1, f_2\}$
        compute $h \in \text{Spol}(f_1, f_2)$
    end if
    compute $g \in \text{SRem}(h, G)$
    if $g \neq 0$ do
        $B \leftarrow B \cup \{g, f \in G\}$
        $C \leftarrow C \cup \{g\}$
        $G \leftarrow G \cup \{g\}$
    end if
end while
return($G$)
end

References


