Gröbner bases and products of coefficient rings. *

Graham H. Norton, Dept. Mathematics, Univ. of Queensland, Brisbane

Ana Sălăgean, Dept. Mathematics, Nottingham Trent Univ., Nottingham, U.K.

September 21, 2001

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. Recall that if A is a principal ideal ring, any non-zero ideal of $A[\mathbf{x}]$ has an SGB, [3, Algorithm 6.4]. We give another proof of this fact.

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. In the final section, we assume that A is a principal ideal ring.

*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.

2 Preliminaries

We have $A = A_1 \times \cdots \times A_m$ and we write $A[\mathbf{x}]$ 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 $A_i[\mathbf{x}]$ as on $A[\mathbf{x}]$.*

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

Let $G \subset A[\mathbf{x}] \setminus \{0\}$ be finite. Then $f \in A[\mathbf{x}]$ *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 $t^{(j)} \mathrm{lt}(g^{(j)}) \leq \mathrm{lt}(f)$, [2, p. 218]. We write $\mathrm{Std}(G)$ for the polynomials which have a standard representation wrt. G.

Also, if $G \subset A[\mathbf{x}] \setminus \{0\}$ is finite, then G is a *Gröbner basis (GB)* for a non-zero ideal $I \subset A[\mathbf{x}]$ if and only if $I = \mathrm{Std}(G)$, [1, Theorem 4.1.12]. If A is Noetherian, every non-zero ideal of $A[\mathbf{x}]$ has a GB, [1, Corollary 4.1.17].

Recall that if $G \subset A[\mathbf{x}] \setminus \{0\}$ 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 $\mathrm{lm}(g) | \mathrm{lm}(f)$, [1, Definition 4.5.6]. If A is a principal ideal ring, Algorithm 6.4 of [3] constructs an SGB for any non-zero ideal of $A[\mathbf{x}]$. Also, an SGB G is called *minimal* if no proper subset of G is an SGB for $\langle G \rangle$.

3 The join

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

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

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

Definition 3.2 *Let $G_i \subset A_i[\mathbf{x}] \setminus \{0\}$ 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* $A_1[\mathbf{x}] \times A_2[\mathbf{x}]$.

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

PROOF. Note first that $0 \notin H = \kappa(G_1 \sqcup \cdots \sqcup G_m)$. We show $I \subset \mathrm{Std}(H)$ if each G_i is a GB. Let $f \in I \setminus \{0\}$. Since $\pi_i(f) \in \pi_i(I) = \mathrm{Std}(G_i)$, we can write $\pi_i(f) = \sum_{j=1}^{k_i} c_i^{(j)} t_i^{(j)} g_i^{(j)}$ for some $k_i \geq 1$, $c_i^{(j)} \in A_i \setminus \{0\}$, $t_i^{(j)} \in T$, $g_i^{(j)} \in G_i$ with $t_i^{(j)} \,\mathrm{lt}(g_i^{(j)}) \leq \mathrm{lt}(\pi_i(f)) \leq \mathrm{lt}(f)$. Then

$$\begin{aligned} f &= \kappa(\pi_1(f), \ldots, \pi_m(f)) \\ &= \kappa\left(\sum_{j=1}^{k_1} c_1^{(j)} t_1^{(j)} g_1^{(j)}, 0, \ldots, 0\right) + \cdots + \kappa\left(0, \ldots, 0, \sum_{j=1}^{k_m} c_m^{(j)} t_m^{(j)} g_m^{(j)}\right) \\ &= \sum_{j=1}^{k_1} c_1^{(j)} t_1^{(j)} \kappa(g_1^{(j)}, 0, \ldots, 0) + \cdots + \sum_{j=1}^{k_m} c_m^{(j)} t_m^{(j)} \kappa(0, \ldots, 0, g_m^{(j)}). \end{aligned}$$

Now $\kappa(0, \ldots, 0, g_i^{(j)}, 0, \ldots, 0) \in H$ and $t_i^{(j)} \,\mathrm{lt}(\kappa(0, \ldots, 0, g_i^{(j)}, 0, \ldots, 0)) = t_i^{(j)} \,\mathrm{lt}(g_i^{(j)}) \leq \mathrm{lt}(f)$ for $j = 1, \ldots, k_i$ and $i = 1, \ldots, m$, so that $f \in \mathrm{Std}(H)$. 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* $\chi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ *induces an isomorphism* $\chi : \mathbb{Z}_6[x] \to (\mathbb{Z}_2 \times \mathbb{Z}_3)[x]$ *and* $\chi(f) = (0,2)x^2 + (1,0)x + (1,1)$. *We have* $\pi\chi(f) = (x+1, 2x^2+1) \in \mathbb{Z}_2[x] \times \mathbb{Z}_3[x]$ *and clearly* $\{x+1\}$ *and* $\{x^2+2\}$ *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 $\mathrm{lm}(g) | \,\mathrm{lm}(x^2 - 3x + 2)$. We will now show how to obtain an SGB in $A[\mathbf{x}]$ from SGB's in the $A_i[\mathbf{x}]$.

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

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

Definition 4.2 *Let $G_i \subset A_i[\mathbf{x}] \setminus \{0\}$ for $i = 1, 2$. Then $G_1 \sqcup G_2$, the* strong join *of G_1, G_2 is the subset $G_1 \sqcup G_2 \cup \{(t_1 g_1, t_2 g_2) \ : \ g_i \in G_i, \ t_i = \mathrm{lcm}(\mathrm{lt}(g_1), \mathrm{lt}(g_2))/\mathrm{lt}(g_i)\}$ of $A_1[\mathbf{x}] \times A_2[\mathbf{x}]$.*

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

Proof. Use the fact that in $\kappa(G_1 \sqcup G_2)$, $\mathrm{lt}(\kappa(t_1 g_1, t_2 g_2)) = \mathrm{lcm}(\mathrm{lt}(g_1), \mathrm{lt}(g_2))$ and that the lcm of leading terms is associative. □

For $m \geq 3$ we define $\kappa(G_1 \sqcup \cdots \sqcup G_m)$ inductively to be $\kappa(\kappa(G_1 \sqcup \cdots \sqcup G_{m-1}) \sqcup G_m)$.

Theorem 4.4 *Let I be a non-zero ideal in $A[\mathbf{x}]$ and $G_i \subseteq \pi_i(I) \setminus \{0\}$ for $i = 1, \ldots, m$. Then $\kappa(G_1 \sqcup \cdots \sqcup G_m)$ is an SGB for I if and only if G_i is an SGB for $\pi_i(I)$ for $i = 1, \ldots, m$.*

Proof. It suffices to prove the result for $m = 2$, as the general case follows inductively. Assume that G_i is an SGB for $\pi_i(I)$ for $i = 1, 2$. We will prove that for any $f \in I \setminus \{0\}$ there is a $g \in \kappa(G_1 \sqcup G_2)$ such that $\mathrm{lm}(g) | \mathrm{lm}(f)$. For $i = 1, 2$, put $\pi_i(f) = f_i$. We consider several cases:

(i) $f_1 \neq 0$ and $f_2 = 0$. Then $\mathrm{lm}(f) = (\mathrm{lc}(f_1), 0)\,\mathrm{lt}(f_1)$. Since G_1 is a SGB for $\pi_1(I)$, there is a $g_1 \in G_1$ such that $\mathrm{lm}(g_1) | \mathrm{lm}(f_1)$. Putting $g = \kappa(g_1, 0) \in \kappa(G_1 \sqcup G_2)$, we have $\mathrm{lm}(g) = (\mathrm{lc}(g_1), 0)\,\mathrm{lt}(g_1)$ and so $\mathrm{lm}(g) | \mathrm{lm}(f)$.

(ii) $f_1 \neq 0$, $f_2 \neq 0$ and $\mathrm{lt}(f_1) > \mathrm{lt}(f_2)$: this is similar to case (i) since $\mathrm{lm}(f) = (\mathrm{lc}(f_1), 0)\,\mathrm{lt}(f_1)$. (iii) $f_1 = 0$ and $f_2 \neq 0$: this is analogous to case (i). (iv) $f_1 \neq 0$, $f_2 \neq 0$ and $\mathrm{lt}(f_1) < \mathrm{lt}(f_2)$: see case (iii).

(v) $f_1 \neq 0$, $f_2 \neq 0$ and $\mathrm{lt}(f_1) = \mathrm{lt}(f_2)$. Then $\mathrm{lm}(f) = (\mathrm{lc}(f_1), \mathrm{lc}(f_2))\,\mathrm{lt}(f_1)$. For $i = 1, 2$, let $g_i \in G_i$ be such that $\mathrm{lm}(g_i) | \mathrm{lm}(f_i)$. Putting $g = \kappa(t_1 g_1, t_2 g_2) \in \kappa(G_1 \sqcup G_2)$, where t_i is as in Definition 4.2, we have $\mathrm{lm}(g) = (\mathrm{lc}(g_1), \mathrm{lc}(g_2))\,\mathrm{lcm}(\mathrm{lt}(g_1), \mathrm{lt}(g_2))$ and so $\mathrm{lm}(g) | \mathrm{lm}(f)$.

For the converse, assume that $\kappa(G_1 \sqcup G_2)$ is an SGB for I and fix $i \in \{0, 1\}$. Let $H_i = \pi_i(G_1 \sqcup G_2) \setminus \{0\}$, which is an SGB for $\pi_i(I)$ by Proposition 4.1. From the definition of $G_1 \sqcup G_2$, $G_i \subseteq H_i$ and any $h_i \in H_i \setminus G_i$ is of the form $h_i = t_i g_i$ for some $t_i \in T$. Thus $\langle G_i \rangle = \langle H_i \rangle$ and for any $f \in \pi_i(I) = \langle G_i \rangle$, there is an $h_i \in H_i$ and a $g_i \in G_i$ such that $\mathrm{lm}(g_i) | \mathrm{lm}(h_i) | \mathrm{lm}(f)$. Hence G_i is an SGB for $\pi_i(I)$. □

Theorem 4.4 thus gives an iterative algorithm for computing an SGB in $A[\mathbf{x}]$, provided we have an algorithm (SGB_i say) that computes an SGB in each $A_i[\mathbf{x}]$ for $1 \leq i \leq m$. The SGB_i can be done in parallel and the complexity of computing $\kappa(G_1 \sqcup \cdots \sqcup G_m)$ from $G_1, \ldots, G_m$ is $\mathcal{O}(\prod_{i=1}^{m} |G_i|)$. The latter can be improved by first minimising each G_i. We note that $\kappa(G_1 \sqcup \cdots \sqcup G_m)$ may not be minimal, so in general, a further minimisation step will be necessary. We formalise this as follows:

Algorithm 4.5

Input: $F \subset A[\mathbf{x}] \setminus \{0\}$, F finite, $A = \prod_{i=1}^{m} A_i$ and we have an algorithm SGB_i which computes an SGB in $A_i[\mathbf{x}]$ for $1 \leq i \leq m$.

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

begin
for $i \leftarrow 1$ to m **do**
    $G_i \leftarrow SGB_i(\pi_i(F))$
    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
return(G)
end

Finally, we note that in computing $G = \kappa(G_1 \sqcup \cdots \sqcup G_m))$ we can first compute $\mathrm{lm}(G)$ to preselect the polynomials of G belonging to a minimal SGB. Only these polynomials need then be computed in full. See Example 5.3.

5 The principal ideal ring case

In this final section, we restrict A to be a principal ideal ring. We give an alternative proof that any non-zero ideal of $A[\mathbf{x}]$ has an SGB and conclude with some examples.

Corollary 5.1 *(cf. [3, Algorithm 6.4]) If A is a principal ideal ring then any non-zero ideal of $A[\mathbf{x}]$ has an SGB.*

Proof. We have $A \cong \prod_{i=1}^{m} A_i$, where each A_i is 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]). Over a finite-chain ring any GB is a SGB by [3, Proposition 3.9], so it suffices to compute a GB, using for example [3, Algorithm 6.1] which computes a GB over any principal ideal ring. Hence by Theorem 4.4 we can compute an SGB for any non-zero ideal of $A[\mathbf{x}]$. □

An improved SGB algorithm for finite-chain rings is described in the Appendix.

Example 5.2 *(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 4.5 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* $\{x + 1\} \underline{\sqcup} \{x^2 + 2\}) = \{(x + 1, 0), (0, x^2 + 2), (x^2 + x, x^2 + 2)\}$ *and* $G = \kappa(\{x + 1\} \underline{\sqcup} \{x^2 + 2\}) = \{(1, 0)x + (1, 0), (0, 1)x^2 + (0, 2), (1, 1)x^2 + (1, 0)x + (0, 2)\}$ *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* $\langle F \rangle$*.*

In the next example, we use Algorithm SGB-FCR of the Appendix.

Example 5.3 *As in [1, Example 4.2.12], let* $F = \{4xy + x, 3x^2 + y\} \subset \mathbb{Z}_{20}[x, y]$*. Using lexicographic order with* $x > y$*, they obtain a GB* $G' = \{3x^2 + y, 4xy + x, 5x, 4y^2 + y, 15y\}$ *via the method of syzygy modules. This is not an SGB since* $xy - x = 5xy - (4xy + x)$ *is not strongly reducible wrt.* G'*. Likewise for* $y^2 - y = 5y^2 - (4y^2 + y)$*. (We note that [3, Corollary 5.12] shows that* $\{x^2 + 7y, xy - x, 5x, y^2 - y, 5y\}$ *is a minimal SGB.)*

Instead, we compute an SGB for $\langle F \rangle$ *from scratch using the usual isomorphism* $\chi : \mathbb{Z}_{20} \to \mathbb{Z}_4 \times \mathbb{Z}_5$ *and Algorithm 4.5. 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 [3, Theorem 4.10] and it is a (minimal) SGB by [3, Proposition 3.9]. 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* $\mathrm{lm}(\kappa(G_1 \underline{\sqcup} G_2))$ *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* $\langle F \rangle$*.*

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

6 Appendix

We derive an algorithm for computing an SGB over a finite-chain ring R from [3, Algorithm 6.1], using the definitions and notation of [3, Sections 3.1, 4.3]. In particular, for $f, f_1, f_2 \in R[\mathbf{x}] \setminus \{0\}$ and G a finite set of non-zero polynomials, $\mathrm{Spol}(f_1, f_2)$, $\mathrm{Apol}(f)$, $\mathrm{Rem}(f, G)$, $\mathrm{SRem}(f, G)$ denote the set of S-polynomials of f_1, f_2, the set of A-polynomials of f, the remainder and the strong remainder of f wrt. G, respectively.

Algorithm 6.1 of [3] computes a GB over any principal ideal ring, so over R in particular. We know that any GB over R is an SGB by [3, Proposition 3.9]. We also know that f is reducible wrt. G if and only if f is strongly reducible wrt. G by [3, Proposition 3.2], so that $\mathrm{SRem}(f, G) \subseteq \mathrm{Rem}(f, G)$. So

over R we only need to use strong reduction, which is more efficient than reduction. The improved algorithm follows:

Algorithm 6.1

$G \leftarrow$ SGB-FCR(F)

Input: F a finite subset of $R[\mathbf{x}] \setminus \{0\}$, where R 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
$G \leftarrow F$
$B \leftarrow \{\{f_1, f_2\} \ : \ f_1, f_2 \in G, f_1 \neq f_2\}$
$C \leftarrow F$
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**
    $B \leftarrow B \cup \{\{g, f\} \ : \ f \in G\}$
    $C \leftarrow C \cup \{g\}$
    $G \leftarrow G \cup \{g\}$
  end if
end while
return(G)
end

References

[1] W. Adams and P. Loustaunau. *An Introduction to Gröbner bases.* Graduate Studies in Mathematics 3. American Mathematical Society, 1994.

[2] T. Becker and V. Weispfenning. *Gröbner Bases, Graduate Texts in Mathematics 141.* Springer, 1993.

[3] G. H. Norton and A. Salagean. Strong Gröbner bases for polynomials over a principal ideal ring. Bull. Australian Mathematical Society, vol. 64, 505–528, 2001.

[4] O. Zariski and P. Samuel. *Commutative Algebra*, Volume 1. Springer, 1979.