TRANSITIVITY FOR WEAK AND STRONG GRÖBNER BASES

W. W. ADAMS, A. BOYLE, AND P. LOUSTAUNAU

Abstract. Let R be a Noetherian integral domain which is graded by an ordered group Γ and let $\mathbf{x}$ be a set of n variables with a term order. It is shown that a finite subset F of $R[\mathbf{x}]$ is a weak (respectively strong) Gröbner basis in $R[\mathbf{x}]$ graded by $\Gamma \times \mathbf{Z}^n$ if and only if F is a weak Gröbner basis in $R[\mathbf{x}]$ graded by $\{0\} \times \mathbf{Z}^n$ and certain subsets of the set of leading coefficients of the elements of F form weak (respectively strong) Gröbner bases in R. It is further shown that any Γ-graded ring R for which every ideal has a strong Gröbner basis is isomorphic to $k[x_1, \ldots, x_n]$, where k is a PID.

1. Introduction

Let $\mathbf{y}$ and $\mathbf{x}$ be sets of variables, each with a term order and an elimination order between them. Let k denote a Noetherian commutative ring. In several places in the literature (e.g. Adams and Boyle (1992), Bayer and Stillman (1987), Gianni, Trager, and Zacharias (1988), Spear (1977), Shtokhamer (1988)), the problem of lifting Gröbner bases from the ring $k[\mathbf{y}]$ to the ring $k[\mathbf{y}, \mathbf{x}]$ has been examined. This entails understanding the difference between a Gröbner basis in $(k[\mathbf{y}])[\mathbf{x}]$ and a Gröbner basis in $k[\mathbf{y}, \mathbf{x}]$. We refer to this as the transitivity question. This problem was examined in Adams and Boyle (1992) mainly for the case when $\mathbf{x} = x$ consisted of a single variable. There it was shown that certain subsets of the leading coefficients with respect to x must form Gröbner bases in $k[\mathbf{y}]$ in order to go from a Gröbner basis in $(k[\mathbf{y}])[x]$ to a Gröbner basis in $k[\mathbf{y}, x]$.

In this paper we are able to answer the transitivity question when $\mathbf{x}$ is more than one variable by considering so-called saturated sets of polynomials as introduced by Möller (1988) (where they were called maximal sets). We found that graded rings are a natural setting for this question. So, let R be a Noetherian integral domain and assume that R is graded by an ordered group Γ. The concept of Gröbner basis can be extended to such graded rings R (see, for example Miola and Mora (1988)). If $\mathbf{x}$ denotes a set of n variables, the ring $R[\mathbf{x}]$ can be graded both by $\Gamma \times \mathbf{Z}^n$ and $\{0\} \times \mathbf{Z}^n$. Then the transitivity question in this setting becomes: when is a Gröbner basis in $R[\mathbf{x}]$, graded by $\{0\} \times \mathbf{Z}^n$, also a Gröbner basis in $R[\mathbf{x}]$, graded by $\Gamma \times \mathbf{Z}^n$. The solution is stated in terms of certain sets of leading coefficients corresponding to the saturated subsets being Gröbner bases in R.

Gröbner bases for $k[x_1, \ldots, x_n]$, where k is a field, were originally defined by Buchberger, cf. Buchberger (1985). There, a finite set F is called a Gröbner basis for an ideal I, if given any element a of I, there is an $f \in F$ such that the leading term of f divides the leading term of a. When the concept of Gröbner bases was extended to a commutative ring k, the leading term of a was only required to be a linear combination of leading terms of elements of F. Following Möller (1988), we refer to the first concept as a strong Gröbner basis and the latter as a weak Gröbner basis. The transitivity question is answered in the current paper for both strong Gröbner bases and weak Gröbner bases. Using this we can take a Gröbner basis in $R[\mathbf{x}]$ graded with respect to $\{0\} \times \mathbf{Z}^n$ and explicitly show how to construct a Gröbner basis in $R[\mathbf{x}]$ graded with respect to $\Gamma \times \mathbf{Z}^n$.

The final section of this paper is concerned with graded rings in which every ideal has a strong Gröbner basis. Möller (1988) remarks that if every ideal in $k[x_1, \ldots, x_n]$, where k is a unique factorization domain (UFD), has a strong Gröbner basis, then k is necessarily a principal ideal domain (PID). We show that every Γ-graded ring R with this property must look like $R = k[x_1, \ldots, x_n]$, where k is a PID.

We now give a more detailed account of the sections in this paper. In Section 2 we give the basic definitions of weak and strong Gröbner bases with respect to graded rings; derive some of their elementary properties; and, in Theorem 2.7, give some of the usual characterizations of Gröbner bases. In Section 3 we consider the transitivity question for weak Gröbner bases. The main characterization is given in Theorem 3.2 where we show that a finite subset F of $R[\mathbf{x}]$ is a weak Gröbner basis with respect to $\Gamma \times \mathbf{Z}^n$ if and only if F is a weak Gröbner basis in $R[\mathbf{x}]$ with respect to $\{0\} \times \mathbf{Z}^n$ and for all saturated subsets S of $\{1, ..., s\}$, the set of leading coefficients of the polynomials indexed by S is a weak Gröbner basis in R with respect to Γ. We use this result to show in Corollary 3.3, that if we can compute weak Gröbner bases in $R[\mathbf{x}]$ with respect to $\{0\} \times \mathbf{Z}^n$, and in R with respect to Γ, then we can compute weak Gröbner bases in $R[\mathbf{x}]$ with respect to $\Gamma \times \mathbf{Z}^n$. We go on to give alternate characterizations of the conditions in Theorem 3.2. In Proposition 3.7 we determine certain subsets of a weak Gröbner basis that are also weak Gröbner bases. Examples are given illustrating some of these results. In Section 4 we give the analogous results for strong Gröbner bases. Theorem 4.1 gives the main result and Corollaries 4.2 and 4.3 show that if we can compute weak Gröbner bases in $R[\mathbf{x}]$ with respect to $\{0\} \times \mathbf{Z}^n$, and strong Gröbner bases in R with respect to Γ, then we can compute strong Gröbner bases in $R[\mathbf{x}]$ with respect to $\Gamma \times \mathbf{Z}^n$. In Corollary 4.6 we show that for a field k and a single variable y, a strong Gröbner basis in $(k[y])[\mathbf{x}]$ is automatically a (strong) Gröbner basis in $k[y, \mathbf{x}]$. Finally, in Section 5, we give some structure theorems for graded rings with strong Gröbner bases. We first show in Theorem 5.1, that if R is a Γ-graded UFD with only finitely many homogeneous irreducibles of positive value, then R is isomorphic to a polynomial ring over a UFD. We then show that this hypothesis is satisfied if the so-called irrelevant ideal of R has a strong Gröbner basis. This enables us to prove that if R is a Γ-graded UFD and every ideal has a strong Gröbner basis then R is a polynomial ring over a PID.

2. Graded Rings

Let Γ be an additive abelian group which is totally ordered with respect to an order, denoted by "$<$", and where we assume that the order respects the group law. The latter means that for all $\gamma, \delta, \eta \in \Gamma$, we have that $\gamma < \delta$ implies that $\gamma + \eta < \delta + \eta$. Two examples are most important in this paper. One is the trivial group $\Gamma = \{0\}$. The other is $\Gamma = \mathbf{Z}^n$ (where $\mathbf{Z}$ denotes the integers and $n > 0$ is an integer) and Γ has a term order (c.f Buchberger (1985) and Robbiano (1989)).

We assume that R is a Noetherian integral domain graded by Γ. Thus $R = \bigoplus_{\gamma \in \Gamma} R_\gamma$, where each R_γ is an additive abelian group and $R_\gamma R_\delta \subseteq R_{\gamma+\delta}$ for all $\gamma, \delta \in \Gamma$. Let $\Gamma_0 = \{\gamma \in \Gamma | R_\gamma \neq 0\}$. Since $0 \in \Gamma_0$ $(1 = 1^2 \in R_0)$, we see that Γ_0

is, in fact, a submonoid of Γ. We will assume that Γ_0 generates Γ. We will also assume that Γ_0 is well ordered.

In the first example mentioned above we have for $\Gamma = \{0\}$ that $R = R_0$ for any integral domain R_0. In other words an important consideration for us is when the ring has a trivial grading. In the second example where $\Gamma = \mathbf{Z}^n$ with a term order, we consider $R = k[x_1, ..., x_n]$ for indeterminates $x_1, ..., x_n$ and an integral domain k. In this example $\Gamma_0 = \mathbf{N}^n$, where $\mathbf{N}$ denotes the natural numbers.

We first observe

Lemma 2.1. *Γ_0 is well ordered if and only if $0 \leq \gamma$ for all $\gamma \in \Gamma_0$.*

Proof. Assume that Γ_0 is well ordered and for some $\gamma \in \Gamma_0$ we have $\gamma < 0$. Choose $a \in R_\gamma$, $a \neq 0$. Then $a^n \in R_{n\gamma}$ and $a^n \neq 0$ so that $n\gamma \in \Gamma_0$, for all $n \in \mathbf{N}$. Also, $0 > \gamma$ implies that $\gamma > 2\gamma$, etc. So we have an infinite descending chain $\gamma > 2\gamma > 3\gamma > \cdots$ in Γ_0, which is a contradiction. Conversely, let $\gamma_1, \gamma_2, ...$ be in Γ_0 such that $\gamma_1 > \gamma_2 > \cdots$. Choose $a_i \neq 0$ in R_{γ_i} for each i. Consider the chain of ideals $\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \cdots$. We see that this chain is strict since $a_{\nu+1} \in \langle a_1, ..., a_\nu \rangle$ implies that $a_{\nu+1} = \sum_{i=1}^{\nu} r_i a_i$ where, since the a's are homogeneous, we may assume each r_i is homogeneous, say of degree δ_i. Then for all i such that $r_i \neq 0$, we have $\delta_i + \gamma_i = \gamma_{\nu+1}$. Also for all such i we have $\delta_i \in \Gamma_0$ and so $\delta_i \geq 0$. Thus $\gamma_{\nu+1} = \delta_i + \gamma_i \geq \gamma_i$, which is a contradiction. Thus the chain of ideals above is strictly increasing and this violates the assumption that the ring R is Noetherian. □

From Lemma 2.1 and our assumption that Γ_0 is well ordered, we are justified in using (complete) induction to prove results involving Γ_0.

Now for each $a \in R$ ($a \neq 0$) we may write $a = \sum_{\gamma \leq \gamma_0} a_\gamma$, with $a_\gamma \in R_\gamma$ and $a_{\gamma_0} \neq 0$. We define $lt(a) = a_{\gamma_0}$ and $v(a) = \gamma_0$. Set $lt(0) = 0$ and $v(0) = 0$. We call $lt(a)$ the *leading term* of a and $v(a)$ the *value* of a. Since R is an integral domain, we have, for all $a, b \in R$, $lt(ab) = lt(a)lt(b)$, and if $ab \neq 0$ then $v(ab) = v(a) + v(b)$. For a subset $F \subseteq R$, we set $Lt(F) = \langle lt(a) | a \in F \rangle$. (Here the symbol $\langle \cdots \rangle$ denotes the ideal generated by $\cdots$.) Clearly $Lt(F)$ is a homogeneous ideal.

In this paper we will study two different definitions of Gröbner bases (cf Möller (1988)). These definitions are given now.

Definition 2.2. *Let I be an ideal in R and let F be a subset of I. We call F a weak Gröbner basis for I provided that F is finite and $Lt(F) = Lt(I)$.*

Definition 2.3. *Assume that R is a unique factorization domain (UFD). Let I be an ideal in R and let F be a subset of I. We call F a strong Gröbner basis for I provided that F is finite and for all $a \in I$ there exists $b \in F$ such that $lt(b)|lt(a)$.*

We will say that a subset F of R is a *weak* (respectively *strong*) *Gröbner basis* provided that F is a weak (respectively strong) Gröbner basis of the ideal, $\langle F \rangle$, that it generates.

As an example let $R = k[x_1, ..., x_n]$, where k is a UFD and $\Gamma = \mathbf{Z}^n$ with a term order (so $\Gamma_0 = \mathbf{N}^n$). If k is a field, then it is well known that these two concepts coincide, c.f. Buchberger (1985) and Robbiano (1989). However, if k is not a field, then these concepts are different (c.f. the example after Proposition 2.6 and Corollary 4.3).

As a second example let $\Gamma = \{0\}$. Then one easily sees that any subset of R is a weak Gröbner basis. On the other hand, in Möller (1988) it is noted that for a UFD

R, every ideal can have a strong Gröbner basis if and only if R is a principal ideal domain (PID). In this case F is a strong Gröbner basis if and only if $gcd(F) \in F$. We will give a generalization of this result in Theorem 5.4 below.

We will now make a few observations concerning these definitions.

Proposition 2.4. *Let R be a UFD, I be an ideal in R and F be a subset of I. If F is a strong Gröbner basis for I, then it is also a weak Gröbner basis for I.*

Proof. If $a \in I$, then we can find $b \in F$ such that $lt(b)|lt(a)$ and so $lt(a) \in Lt(F)$. $\square$

Proposition 2.5. *If F is a subset of the ideal I in R and F is a weak Gröbner basis of I, then $I = \langle F \rangle$.*

Proof. Let $F = \{f_1, \ldots, f_s\}$. Let $a \in I$. We use induction on $v(a)$ to show that $a \in \langle F \rangle$. By assumption $lt(a) = \sum_{i=1}^{s} b_i lt(f_i)$ for some $b_i \in R$. Since $lt(a)$ is homogeneous, we may assume that each b_i is homogeneous and $v(f_i) \leq v(a)$ for all i such that $b_i \neq 0$. If $v(a) = 0$, then $v(lt(f_i)) = v(f_i) = 0$ for all i with $b_i \neq 0$, and so $lt(f_i) = f_i$, $lt(a) = a$ and $a = \sum_{i=1}^{s} b_i f_i$. On the other hand, if $v(a) > 0$ we have $a - \sum_{i=1}^{s} b_i f_i \in I$ and $v(a - \sum_{i=1}^{s} b_i f_i) < v(a)$ and so we are done by induction. $\square$

Proposition 2.6. *Every ideal I in R has a weak Gröbner basis.*

Proof. Since R is Noetherian, there are $b_1, \ldots b_t \in Lt(I)$ such that $Lt(I) = \langle b_1, \ldots, b_t \rangle$. Now each of the b_i can be written as $b_i = \sum c_{ij} lt(a_{ij})$ with $a_{ij} \in I$. Then $F = \{a_{ij}\}$ is a weak Gröbner basis for I. $\square$

As noted above the existence of strong Gröbner bases is more problematical. For example, let $R = k[x, y, z]$ graded with the integers $\mathbf{Z}$ on the z variable (i.e. the z degree of a polynomial in R; so $R_0 = k[x, y]$). Consider the ideal $I = \langle x, y, z \rangle$ in R. This ideal does not have a strong Gröbner basis. This is because there are an infinite number of homogeneous non-associate irreducible polynomials in the two variables x, y in I and each of these would have to have leading term (which is the irreducible polynomial itself) divisible by the leading term of an element of a strong Gröbner basis. This forces an infinite number of elements in the strong Gröbner basis which violates the definition of strong Gröbner basis. The results in Section 5 bring out this point more clearly.

Finally the following Theorem provides in our context a couple of the usual equivalent conditions for a set to be a weak Gröbner basis. The third condition is the usual statement about the module of syzygies of the leading terms of the elements of the weak Gröbner basis F. As usual it would have sufficed to replace statement 3 in the Theorem below by making the same statement about a finite homogeneous basis of the syzygy module.

Theorem 2.7. *Let $F = \{f_1, \ldots, f_s\}$ be a finite subset of R. Then the following three statements are equivalent:*

1. *F is a weak Gröbner basis*
2. *for every $a \in \langle F \rangle$ we can write*

$$a = \sum_{i=1}^{s} r_i f_i \text{ where } v(a) = \max_{1 \leq i \leq s} (v(r_i f_i)) \tag{1}$$

and $r_i \in R$

3. *for all sequences* $(b_1, \ldots, b_s)$ *where* $b_i \in R$ *is homogeneous, and where for some* $\gamma \in \Gamma$, $v(b_i lt(f_i)) = \gamma$ *for all* i *such that* $b_i \neq 0$*, and where* $\sum_{i=1}^{s} b_i lt(f_i) = 0$*; we have that*
$$a = \sum_{i=1}^{s} b_i f_i$$
has a representation as in Equation 1 above.

Proof. We first assume that $Lt(F) = Lt(\langle F \rangle)$, that is, F is a weak Gröbner basis and show statement 2 is valid. Let $a \in \langle F \rangle$. Then $lt(a) \in Lt(F)$ and so $lt(a) = \sum_{i=1}^{s} c_i lt(f_i)$ for some $c_i \in R$. Since $lt(a)$ is homogeneous, we may assume c_i is homogeneous and is either zero or lies in $R_{v(a)-v(f_i)}$. Setting $b = a - \sum_{i=1}^{s} c_i f_i$, we have that $v(b) < v(a)$ and we may proceed by induction. (The case where $v(a) = 0$ is trivial.) That statement 2 implies statement 3 is clear since it is a special case of statement 2. Finally we show that statement 3 implies statement 1. So, let $a \in \langle F \rangle$ and write $a = \sum_{i=1}^{s} r_i f_i$ where $r_i \in R$. Set $\gamma = \max_{1 \leq i \leq s} v(r_i f_i)$. If $v(a) = \gamma$, we are done, since then
$$lt(a) = \sum_{v(r_i f_i)=\gamma} lt(r_i) lt(f_i).$$
If not, then $v(a) < \gamma$ and so
$$\sum_{v(r_i f_i)=\gamma} lt(r_i) lt(f_i) = 0.$$
Then by hypothesis we can write
$$\sum_{v(r_i f_i)=\gamma} lt(r_i) f_i = \sum_{i=1}^{s} t_i f_i$$
such that for all i, $v(t_i f_i) < \gamma$. Then we have
$$\begin{aligned} a &= \sum_{i=1}^{s} r_i f_i - \sum_{v(r_i f_i)=\gamma} lt(r_i) f_i + \sum_{i=1}^{s} t_i f_i \\ &= \sum_{v(r_i f_i)=\gamma} (r_i - lt(r_i) + t_i) f_i + \sum_{v(r_i f_i)<\gamma} (r_i + t_i) f_i. \end{aligned}$$
Every term in the second sum has value $< \gamma$ as does every term in the first, and so we may proceed by induction. ☐

3. Transitivity for Weak Gröbner Bases.

Let $\mathbf{x} = \{x_1, ..., x_n\}$ be variables. Assume that we have a term order "$<$" on $\mathbf{Z}^n$. (We note that this is just an order on the group $\mathbf{Z}^n$ in the sense given in the previous section.) Given any integral domain R there is the natural $\mathbf{Z}^n$ grading on $R[\mathbf{x}]$ whose non-zero homogeneous summands are indexed precisely by $\mathbf{N}^n$. Now assume that R is, in fact, a Γ-graded ring as above. Set $\Lambda = \Gamma \times \mathbf{Z}^n$. Then we can define a Λ-grading on $R[\mathbf{x}]$ where, for $\gamma \in \Gamma$ and $\nu \in \mathbf{Z}^n$ we have
$$R[\mathbf{x}]_{(\gamma,\nu)} = R_\gamma \mathbf{x}^\nu$$
provided that $\nu \in \mathbf{N}^n$ and is $\{0\}$ otherwise. (By $\mathbf{x}^\nu$ we mean $x_1^{\nu_1} \cdots x_n^{\nu_n}$, where $\nu = (\nu_1, ..., \nu_n)$.) We see that $\Lambda_0 = \Gamma_0 \times \mathbf{N}^n$. We will define an order on Λ as follows.

Definition 3.1. *The elimination order on* Λ *is defined as* $(\gamma_1, \nu_1) < (\gamma_2, \nu_2)$ *if and only if* $\nu_1 < \nu_2$ *or* $\nu_1 = \nu_2$ *and* $\gamma_1 < \gamma_2$.

This generalizes the concept of elimination order that occurs in the literature, for example, in the computer algebra system Macaulay, and also in Adams and Boyle (1992). It is easily seen that Definition 3.1 makes Λ into an ordered group satisfying the conditions assumed above.

We note that we are using the symbol "$<$" in (at least) three contexts, but it should always be clear from what is being compared which context is the correct one. We will also, as is usual in the theory of Gröbner bases, use the term order "$<$" on $\mathbf{Z}^n$ on the variables themselves. That is, we will say that $\mathbf{x}^{\nu_1} < \mathbf{x}^{\nu_2}$ if and only if $\nu_1 < \nu_2$.

Now given $a \in R$ we use the notation $lt_\Gamma(a)$ and $v_\Gamma(a)$ to specify the leading term and value of a as defined in the previous section. If $f \in R[\mathbf{x}]$ we denote the same concepts with respect to Λ by $lt_\Lambda(f)$ and $v_\Lambda(f)$ respectively. Write $f = a\mathbf{x}^\nu +$ lower terms in $\mathbf{x}$, where $a \in R$ and $a \neq 0$. Then set $lt_x(f) = a\mathbf{x}^\nu$, $lp_x(f) = \mathbf{x}^\nu$, $lc_x(f) = a$ and $v_x(f) = \nu$. Of course, lt_x and v_x are the leading term and value concepts in $R[\mathbf{x}]$ with respect to the group $\{0\} \times \mathbf{Z}^n$. Also, $lp_x(f)$ is called the *leading power product* of f and $lc_x(f)$ is called the *leading coefficient* of f. We note that $lt_\Lambda(f) = lt_\Lambda(lt_x(f)) = lt_\Gamma(lc_x(f))lp_x(f)$ and $v_\Lambda(f) = (v_\Gamma(lc_x(f)), v_x(f))$. We also define Lt_Γ, Lt_x and Lt_Λ as in the last section. The former will give homogeneous ideals in R and the latter will give ideals in $R[\mathbf{x}]$, homogeneous with respect to $\{0\} \times \mathbf{Z}^n$ and Λ respectively.

We are interested in the following transitivity question: let F be a finite subset of $R[\mathbf{x}]$; is there a relation between the following two statements:

- Is F a weak Gröbner basis in $R[\mathbf{x}]$ with respect to $\Lambda = \Gamma \times \mathbf{Z}^n$?
- Is F a weak Gröbner basis in $R[\mathbf{x}]$ with respect $\{0\} \times \mathbf{Z}^n$?

Relationships such as these have been examined in Adams and Boyle (1992), Bayer and Stillman (1987), Gianni, Trager, and Zacharias (1988), Spear (1977), Shtokhamer (1988). (We will consider similar questions for strong Gröbner bases in the next section.)

The relationship between them involves certain subsets of R as well, which we will now define. Let $F = \{f_1, ..., f_s\}$ be a set of polynomials in $R[\mathbf{x}]$. We adopt the notation that

$$f_i = a_i X_i + \text{ lower terms in the } \mathbf{x} \text{ variables},$$

where X_i is a power product in the $\mathbf{x}$ variables, and $a_i \in R$. That is, $lc_x(f_i) = a_i$ and $lp_x(f_i) = X_i$. We also define $G = \{a_1, .., a_s\}$. We will continue using this notation throughout the paper.

For each subset S of $\{1, ..., s\}$, we define

- $D_S = lcm_{i \in S} X_i = lcm_{i \in S}\{lp_x(f_i)\}$,
- $F_S = \{f_i | X_i \text{ divides } D_S\}$, and
- $G_S = \{a_i | f_i \in F_S\}$.

Also let $S^* = \{i | f_i \in F_S\}$. We say that S is *saturated* in $\{1, \ldots, n\}$ if $S^* = S$.

We are now in a position to state our main result on transitivity of weak Gröbner basis. This result is a generalization of Theorem 3.2 in Adams and Boyle (1992). The important difference here is that in the previous paper we had to assume that there was only one $\mathbf{x}$ variable, that is, $n = 1$. Another difference was that here we have the more general situation of the graded ring R. The proof of the first part of the theorem below was given in Adams and Boyle (1992) for arbitrary n but for a polynomial ring instead of the graded ring R and the proof given here parallels it fairly closely, but for the sake of completeness we will include it.

Theorem 3.2. *F is a weak Gröbner basis in $R[\mathbf{x}]$ with respect to $\Lambda = \Gamma \times \mathbf{Z}^n$ if and only if*

1. *F is a weak Gröbner basis in $R[\mathbf{x}]$ with respect to $\{0\} \times \mathbf{Z}^n$ and*
2. *For all saturated subsets S of $\{1, ..., s\}$, G_S is a weak Gröbner basis in R with respect to Γ.*

Proof. Let us first assume that F is a weak Gröbner basis in $R[\mathbf{x}]$ with respect to Λ. We need to prove that $Lt_x(F) = Lt_x(\langle F\rangle)$. One inclusion is trivial, so let $f \in \langle F\rangle$. Since F is a weak Gröbner basis, we may apply Theorem 2.7 to Λ, and write

$$f = \sum_{j=1}^{t} r_j T_j f_{i_j},$$

where $r_j \in R$ is homogeneous, T_j is a power product in $\mathbf{x}$, the $v_\Lambda(r_j T_j f_{i_j})$'s are decreasing (not necessarily strictly), and $v_\Lambda(f) = v_\Lambda(r_1 T_1 f_{i_1})$. Let j_0 be least such that $v_\Lambda(r_{j_0} T_{j_0} f_{i_{j_0}}) > v_\Lambda(r_{j_0+1} T_{j_0+1} f_{i_{j_0+1}})$. Then, since $v_\Lambda(f) = v_\Lambda(r_1 T_1 f_{i_1})$, we see that

$$lt_\Lambda(f) = \sum_{j=1}^{j_0} r_j T_j lt_\Lambda(f_{i_j}) = T_1 X_{i_1} \sum_{j=1}^{j_0} r_j lt_\Gamma(a_{i_j}) \neq 0.$$

Choose $j_1 \geq j_0$ least such that $T_{j_1} lp_x(f_{i_{j_1}}) = T_{j_1} X_{i_{j_1}} > T_{j_1+1} X_{i_{j_1+1}} = T_{j_1+1} lp_x(f_{i_{j_1+1}})$. From the definition of the order $>$ on Λ, we have that $T_{j_1} X_{i_{j_1}} > T_j X_{i_j}$ for all $j > j_1$. It then follows that

$$lt_x(f) = \sum_{j=1}^{j_1} r_j T_j a_{i_j} X_{i_j} = (\sum_{j=1}^{j_1} r_j a_{i_j}) T_1 X_{i_1}$$

provided that $h = \sum_{j=1}^{j_1} r_j a_{i_j} \neq 0$. However

$$lt_\Gamma(h) = \sum_{j=1}^{j_0} r_j lt_\Gamma(a_{i_j}) \neq 0,$$

as was noted above. Since $lt_x(f_i) = a_i X_i$, we see that $lt_x(f) \in Lt_x(F)$, as desired.

To prove statement 2, we need to show that for every saturated set S, $Lt_\Gamma(G_S) = Lt_\Gamma(\langle G_S\rangle)$. Let S be a saturated subset of $\{1, ..., s\}$, and let $a \in \langle G_S\rangle$. Then $a = \sum_{i\in S} b_i a_i$, where $b_i \in R$. Set

$$f = \sum_{i\in S} b_i \frac{D_S}{X_i} f_i = \sum_{i\in S} b_i \frac{D_S}{X_i}(a_i X_i + \text{ lower } \mathbf{x} \text{ terms })$$
$$= aD_S + \text{ lower } \mathbf{x} \text{ terms }.$$

Note that f is in $\langle F\rangle$. Furthermore, by definition of our elimination ordering

$$lt_\Lambda(f) = lt_\Lambda(aD_S) = lt_\Gamma(a) D_S.$$

By assumption $Lt_\Lambda(F) = Lt_\Lambda(\langle F\rangle)$, and hence we can write

$$lt_\Lambda(f) = \sum_{i=1}^{s} k_i lt_\Lambda(f_i),$$

where $k_i \in R[\mathbf{x}]$. As usual we may assume that each k_i is homogeneous, say $k_i = c_i X_i'$, where $c_i \in R$, is homogeneous, and X_i' is a power product in $\mathbf{x}$. We can also assume that $D_S = lp_x(f) = X_i' X_i$, for all i such that $c_i \neq 0$. Then

$$lt_\Gamma(a) D_S = lt_\Lambda(f) = \sum_{c_i \neq 0} c_i lt_\Gamma(a_i) X_i' X_i.$$

Now for all i such that $c_i \neq 0$, X_i divides D_S, and so a_i is in G_S, by the definition of G_S. Thus $lt_\Gamma(a) = \sum_{i \in S} c_i lt_\Gamma(a_i)$ as desired.

To prove the converse we need to show that $Lt_\Lambda(F) = Lt_\Lambda(\langle F \rangle)$. Let $f \in \langle F \rangle$. By hypothesis 1 and Theorem 2.7,

$$f = \sum_{i=1}^{s} h_i f_i, \text{ where } lp_x(f) = \max_{1 \leq i \leq s} v_x(h_i) + v_x(f_i).$$

Define $X = lp_x(f)$ and $S_0 = \{i \in \{1, ..., s\} \mid lp_x(h_i) lp_x(f_i) = X\}$. Set $S = \{i \in \{1, ..., s\} \mid X_i \text{ divides } X\}$. Then S is saturated and $S \supseteq S_0$. Now

$$f = \sum_{i \in S_0} lc_x(h_i) a_i X + \text{ lower } \mathbf{x} \text{ terms}.$$

Hence $lc_x(f) = \sum_{i \in S_0} lc_x(h_i) a_i$ is in $\langle G_S \rangle$. By hypothesis 2, G_S is a weak Gröbner basis and hence $Lt_\Gamma(G_S) = Lt_\Gamma(\langle G_S \rangle)$. Thus we can write

$$lt_\Gamma(lc_x(f)) = \sum_{i \in S} c_i lt_\Gamma(a_i),$$

where for all i such that $c_i \neq 0$,

$$v_\Gamma(c_i lt_\Gamma(a_i)) = v_\Gamma(lc_x(f)).$$

Finally $lt_\Lambda(f) = lt_\Gamma(lc_x(f)) lp_x(f) = \sum_{i \in S} c_i lt_\Gamma(a_i) X$. By definition of X, X_i divides X for all $i \in S$. So

$$lt_\Lambda(f) = \sum_{i \in S} c_i \frac{X}{X_i} lt_\Gamma(a_i) X_i = \sum_{i \in S} c_i \frac{X}{X_i} lt_\Lambda(f_i).$$

Thus $lt_\Lambda(f)$ is in $Lt_\Lambda(F)$ as desired. $\square$

Note. Let S be any subset of $\{1, ..., s\}$ and let S^* be its saturation. Since $G_S = G_{S^*}$, statement 2 in Theorem 3.2 can be replaced by "For all subsets S of $\{1, ..., s\}, G_S$ is a weak Gröbner basis in R with respect to Γ."

Möller (1988) has shown how to construct weak Gröbner bases in $R[\mathbf{x}]$ with respect to $\{0\} \times \mathbf{Z}^n$ for a certain class of rings, the so-called computable rings (see Möller (1988) and Zacharias (1978)). Our next result shows that if we can compute weak Gröbner bases in $R[\mathbf{x}]$ with respect to $\{0\} \times \mathbf{Z}^n$, and in R with respect to Γ, then we can compute weak Gröbner bases in $R[\mathbf{x}]$ with respect to $\Gamma \times \mathbf{Z}^n$.

Corollary 3.3. *Let R be a Γ-graded ring, and $F = \{f_1, \ldots, f_s\}$ be a weak Gröbner basis in $R[\mathbf{x}]$ with respect to $\{0\} \times \mathbf{Z}^n$. For each saturated subset S of $\{1, \ldots, s\}$ let $\{a^*_{S,1}, \ldots, a^*_{S,t_S}\}$ be a weak Gröbner basis of G_S in R with respect to Γ. Write*

$$a^*_{S,i} = \sum_{j \in S} b_{S,i,j} a_j$$

and define

$$f^*_{S,i} = \sum_{j\in S} b_{S,i,j}\frac{D_S}{X_j} f_j$$

for all $i = 1, \dots, t_S$. *Then*

$$F^* = \bigcup_{S \text{ saturated}} \{f^*_{S,1}, \dots, f^*_{S,t_S}\} \cup F$$

is a weak Gröbner basis with respect to Λ.

Proof. We need to show statements 1 and 2 of Theorem 3.2. Note first that $\langle F\rangle = \langle F^*\rangle$, and since F is a weak Gröbner basis with respect to $\{0\}\times \mathbf{Z}^n$, so is F^*. To prove statement 2, let T be a saturated subset of

$$\bigcup_{S \text{ saturated}} \{(S,1), \dots, (S,t_S)\} \cup \{1, \dots, s\}.$$

Note that if (S,i) is in T, then $S \subseteq T$, and $(S,j) \in T$, for $j = 1, \dots, t_S$, since T is saturated. Therefore $D_T = D_S$ for the saturated subset $S = T \cap \{1, \dots, s\}$ of $\{1, \dots, s\}$. But then

$$G_T = \bigcup_{\substack{S' \subseteq S \\ S' \text{ saturated}}} \{a^*_{S',1}, \dots, a^*_{S',t_{S'}}\} \cup \{a_i \mid i \in S\},$$

and hence G_T is a weak Gröbner basis in R with respect to Γ, since $\langle G_T\rangle = \langle G_S\rangle$ and $\{a^*_{S,1}, \dots, a^*_{S,t_S}\}$ was defined to be a weak Gröbner basis of $G_S = \{a_i \mid i \in S\}$. ☐

If we specialize to the case $R = k[\mathbf{y}]$, where k is an integral domain, $\mathbf{y} = \{y_1, ..., y_m\}$ are variables with a term order, and we have an elimination order between the $\mathbf{y}$ variables and the $\mathbf{x}$ variables with the $\mathbf{x}$ variables bigger than the $\mathbf{y}$ variables, then we have the following immediate consequence of Theorem 3.2.

Corollary 3.4. *A subset* F *of* $k[\mathbf{y},\mathbf{x}]$ *is a weak Gröbner basis in* $k[\mathbf{y},\mathbf{x}]$ *over* k *if and only if*

1. F *is a weak Gröbner basis in* $(k[\mathbf{y}])[\mathbf{x}]$ *over* $k[\mathbf{y}]$ *and*
2. *For all saturated subsets* S *of* $\{1, ..., s\}$, G_S *is a weak Gröbner basis in* $k[\mathbf{y}]$ *over* k.

We note that the statement F is a weak Gröbner basis in $R[\mathbf{x}]$ with respect to $\{0\}\times\mathbf{Z}^n$ in Theorem 3.2 is just the usual concept in the literature of a (weak) Gröbner basis over a commutative ring. We will now give an equivalent condition for a set to satisfy this condition involving the concept of saturated sets above. Although the result does not involve the grading on the domain R, in fact does not require that we have a domain, but just a commutative ring, we will state it in the terminology above to have notational consistency throughout the paper.

Proposition 3.5. *Let* $F = \{f_1, ..., f_s\}$ *be a subset of* $R[\mathbf{x}]$. *Then the following statements are equivalent:*

1. F *is a weak Gröbner basis in* $R[\mathbf{x}]$ *with respect to* $\{0\}\times\mathbf{Z}^n$;
2. *For all* $f \in \langle F\rangle$, *there exists a saturated subset* S *of* $\{1, ..., s\}$ *such that* D_S *divides* $lp_x(f)$ *and* $lc_x(f) \in \langle G_S\rangle$.

Proof. Assume 1, and let $f \in \langle F \rangle$. Then $lt_x(f) = \sum_{i=1}^{s} h_i lt_x(f_i)$, where we may assume that h_i is a monomial in $R[\mathbf{x}]$. Now define S to be the saturation of $\{i \in \{1, ..., s\} \mid h_i \neq 0\}$. Since each X_i such that $h_i \neq 0$ divides $lp_x(f)$, their least common multiple, D_S, divides $lp_x(f)$. Moreover after cancelling $lp_x(f)$ from both sides of the above equation, we have $lc_x(f)$ expressed as a linear combination of the a_i, with $i \in S$. Conversely, assume 2. Let $f \in \langle F \rangle$. Then, by hypothesis there exists a saturated subset S of $\{1, ..., s\}$ such that $lp_x(f) = XD_S$, where X is a power product in $\mathbf{x}$, and $lc_x(f) = \sum_{i \in S} b_i a_i$, where $b_i \in R$, for all $i \in S$. Now

$$lt_x(f) = lc_x(f) lp_x(f) = \sum_{i \in S} b_i a_i X D_S = \sum_{i \in S} b_i X \frac{D_S}{X_i} lt_x(f_i).$$

Therefore $lt_x(f)$ is in $Lt_x(F)$. □

The next proposition provides an equivalent condition for statement 2 of theorem 3.2 in terms of a different transitivity property. This extends Proposition 2.4 of Adams and Boyle (1992) where it is assumed that $\mathbf{x}$ is a single variable. Moreover the proof that the second statement implies the first is contained in Lemma 2.2 in Adams and Boyle (1992) in the slightly less general situation where the domain R is not a graded ring but is a polynomial ring over a commutative ring.

Proposition 3.6. *The following statements are equivalent:*

1. *For all saturated subsets S of $\{1, ..., s\}$, G_S is a weak Gröbner basis in R;*
2. *For all saturated subsets S of $\{1, ..., s\}$, $Lt_\Lambda(Lt_x(F_S)) = Lt_\Lambda(F_S)$.*

Proof. We first assume statement 1 and let S be a saturated subset of $\{1, ..., s\}$. Clearly $Lt_\Lambda(F_S) \subseteq Lt_\Lambda(Lt_x(F_S))$. Conversely, let h be in $Lt_x(F_S)$, say

$$h = \sum_{j \in S} h_j lt_x(f_j) = \sum_{j \in S} h_j a_j X_j$$

where h_j belongs to $R[\mathbf{x}]$. Set $h_j = \sum_{k=0}^{d_j} h_{j,k} X'_k$, where $h_{j,k} \in R$, and X'_k is a power product in $\mathbf{x}$. Then $h = \sum_{j \in S} \sum_{k=0}^{d_j} h_{j,k} a_j X'_k X_j$. Let $X = lp_x(h)$, and let $a = lc_x(h) = \sum_{X'_k X_j = X} h_{j,k} a_j$. Note that $lt_\Lambda(h) = lt_\Gamma(a) X$. Let $T_0 = \{j \in S \mid X_j X'_k = X \text{ for some k, } 0 \leq k \leq d_j\}$. Let T be the saturation of T_0. Since S is saturated we see that $T \subseteq S$. Since X_j divides X for all $j \in T$, we have that D_T divides X. We have that $a \in \langle G_T \rangle$ and by hypothesis, G_T is a weak Gröbner basis. Hence $lt_\Gamma(a) = \sum_{j \in T} r_j lt_\Gamma(a_j)$, where the r_j's are in R. Finally,

$$lt_\Lambda(h) = \sum_{j \in T} r_j lt_\Gamma(a_j) X = \sum_{j \in T} r_j \frac{X}{X_j} lt_\Lambda(f_j).$$

Thus $lt_\Lambda(h)$ is in $Lt_\Lambda(F_T) \subseteq Lt_\Lambda(F_S)$.

Conversely assume statement 2. Let S be a saturated subset of $\{1, ..., s\}$. Let $a \in \langle G_S \rangle$, $a \neq 0$, and write $a = \sum_{i \in S} b_i a_i$ for $b_i \in R$. Set $f = aD_S$. Then

$$f = \sum_{i \in S} b_i \frac{D_S}{X_i} a_i X_i = \sum_{i \in S} b_i \frac{D_S}{X_i} lt_x(f_i) \in Lt_x(F_S).$$

So $lt_\Lambda(f) \in Lt_\Lambda(Lt_x(F_S)) = Lt_\Lambda(F_S)$, by hypothesis. Hence we can write $lt_\Lambda(f) = \sum_{i \in S} h_i lt_\Lambda(f_i)$. Since $lt_\Lambda(f)$ is homogeneous with respect to Λ we may assume that $h_i = c_i X'_i$ where c_i is homogeneous in R and X'_i is a power product in $\mathbf{x}$. Of course, $lt_\Lambda(f) = lt_\Gamma(a) D_S$, and so we obtain that $lt_\Gamma(a) D_S = \sum_{i \in S} c_i X'_i lt_\Gamma(a_i) X_i$.

Since then $D_S = X_i' X_i$ for all i such that $c_i \neq 0$ we cancel these terms to obtain $lt_\Gamma(a) = \sum_{i \in S} c_i lt_\Gamma(a_i)$, as desired. □

In Theorem 3.1 in Adams and Boyle (1992) the sets F_S defined right above Theorem 3.2 also turned out to be weak Gröbner bases. It is unfortunately not true that for saturated sets S the sets F_S are weak Gröbner bases as the following example shows.

Example. Let k be the rational numbers and let $R = k[y]$ with the usual $\mathbf{Z}$ grading. Let $n = 2$ and consider $R[x_1, x_2]$ with the lexicographical ordering on x_1, x_2 with $x_1 > x_2$. Thus $k[y, x_1, x_2]$ has the lexicographical ordering with $x_1 > x_2 > y$. Let $f_1 = y^2x_2^4 + x_2^3$, $f_2 = yx_1 + x_2$, $f_3 = x_1x_2^2 - yx_2^4$, $f_4 = x_1^2x_2 + x_2^4$, $f_5 = x_1^3 + x_2^5y$ and let $F = \{f_1, f_2, f_3, f_4, f_5\}$. Then F is a weak Gröbner basis in $k[y, x_1, x_2]$. $S = \{2, 5\}$ is a saturated set, but $\{f_2, f_5\}$ is not a weak Gröbner basis.

However, F_S is a weak Gröbner basis for certain saturated sets S. Let $F = \{f_1, ..., f_s\}$ be a subset of $R[\mathbf{x}]$. A subset S of $\{1, ..., s\}$ is called *full* if for all j not in S we have $D_S < lp_x(f_j)$.

Proposition 3.7. *If F is a weak Gröbner basis in $R[\mathbf{x}]$ with respect to Λ, then F_S is also a weak Gröbner basis in $R[\mathbf{x}]$ with respect to Λ for all full subsets S of $\{1, ..., s\}$.*

Proof. We will use the third criterion in Theorem 2.7. So let S be a full subset of $\{1, ..., s\}$, and suppose that $\sum_{i \in S} c_i X_i' lt_\Lambda(f_i) = 0$, where $c_i \in R$, homogeneous, X_i' is a power product in $\mathbf{x}$, and $v_\Lambda(c_i X_i' lt_\Lambda(f_i))$ is constant for all i such that $c_i \neq 0$. Set $f = \sum_{i \in S} c_i X_i' f_i$. We need a representation as in Equation 1 of Theorem 2.7 for f with respect to Λ. It is clear that we may assume that $\gcd(X_i' \mid c_i \neq 0) = 1$. It then follows that for all i such that $c_i \neq 0$, we get $X_i' X_i \mid D_S$, and so $lp_x(f) \leq D_S$. Now F is a weak Gröbner basis in $R[\mathbf{x}]$ with respect to Λ implies that $f = \sum_{i=1}^s h_i f_i$ where $v_\Lambda(f) = \max_{1 \leq i \leq s} v_\Lambda(h_i f_i)$ (from Theorem 2.7). Then if there is an $i \notin S$ such that $h_i \neq 0$, we have $X_i > D_S$ and thus $lp_x(h_i) lp_x(f_i) \geq lp_x(f_i) > D_S \geq lp_x(f)$. This contradiction shows that the representation for f above is of the correct type for F_S and we are done. □

In the example above, the smallest full set containing $\{2, 5\}$ is in fact $\{1, 2, 3, 4, 5\}$. Also, in the same example, the set $\{1, 2, 3\}$ is full, and hence $F_S = \{f_1, f_2, f_3\}$ is a weak Gröbner basis.

It is now natural to ask whether Theorem 3.2 holds if in statement 2, saturated is replaced by full. It is not true in general as the following example shows.

Example. We use the same setup for R and the variables that we used in the previous example. Let $f_1 = x_2^3$, $f_2 = y(1+y)x_2^2x_1$, and $f_3 = y(2+y)x_2x_1^2$. Note that $F = \{f_1, f_2, f_3\}$ is a weak Gröbner basis in $(k[y])[x_1, x_2]$, since the three polynomials are monomials in $(k[y])[x_1, x_2]$. So statement 1 of Theorem 3.2 is satisfied. The full subsets of $\{1, 2, 3\}$ are $\{1\}$ and $\{1, 2, 3\}$. For S equal to either of these sets, G_S is a weak Gröbner basis in $k[y]$. However F is not a weak Gröbner basis in $k[y, x_1, x_2]$, since the S-polynomial of f_2 and f_3 is $yx_2^2x_1^2$ which cannot be reduced by F. Note that $S = \{2, 3\}$ is saturated and G_S is not a weak Gröbner basis.

We give another example to illustrate some of the ideas of this section. It is a continuation of the example at the end of Möller (1988).

Example. We consider the polynomials in $\mathbf{Z}[x, y, z]$, $f_1 = -6x^3 + 51x$, $f_2 = (2x^2y - 17y)z$, $f_3 = (-85y^2 + 6x^2)z^2$, and $f_4 = (5xy^2 - 3x)z^2$. We will use the lexicographical ordering with $x < y < z$. We consider, in the notation above, $R =$

$\mathbf{Z}[x,y]$, $\Gamma = \mathbf{Z}^2$, $\Lambda = \mathbf{Z}^3$, and $a_1 = -6x^3 + 51x, a_2 = 2x^2y - 17y, a_3 = -85y^2 + 6x^2$, and $a_4 = 5xy^2 - 3x$. Let $F = \{f_1, f_2, f_3, f_4\}$. We will use Theorem 3.2 to prove that F is a weak Gröbner basis in $\mathbf{Z}[x,y,z]$. First note that since the polynomials in F are homogeneous in the variable z, condition 1 of Theorem 3.2 is trivially satisfied. Also, the saturated subsets of $\{1,2,3,4\}$ are $\{1\}, \{1,2\}$, and $\{1,2,3,4\}$, and hence we need to show that the sets $\{a_1\}, \{a_1,a_2\}$, and $\{a_1,a_2,a_3,a_4\}$ are weak Gröbner bases in $\mathbf{Z}[x,y]$. Möller (1988) showed that $\{a_1,a_2,a_3,a_4\}$ is a weak Gröbner basis . Also, the full subsets of $\{1,2,3,4\}$ with respect to Γ are exactly $\{1\}, \{1,2\}$, and $\{1,2,3,4\}$. So, by Proposition 3.7, the sets $\{a_1\}$ and $\{a_1,a_2\}$ are also weak Gröbner bases.

4. Transitivity for Strong Gröbner Bases.

In this section we will assume that R is a unique factorization domain. Otherwise we will maintain exactly the same setup as we had in the previous section. Corresponding to Theorem 3.2 we have the following

Theorem 4.1. *F is a strong Gröbner basis in $R[\mathbf{x}]$ with respect to $\Lambda = \Gamma \times \mathbf{Z}^n$ if and only if*

1. *F is a weak Gröbner basis in $R[\mathbf{x}]$ with respect to $\{0\} \times \mathbf{Z}^n$ and*
2. *For all saturated subsets S of $\{1, ..., s\}$, G_S is a strong Gröbner basis in R with respect to Γ.*

Proof. We first assume that F is a strong Gröbner basis in $R[\mathbf{x}]$ with respect to $\Lambda = \Gamma \times \mathbf{Z}^n$. Since, by Proposition 2.4 F is a weak Gröbner basis in $R[\mathbf{x}]$ with respect to $\Lambda = \Gamma \times \mathbf{Z}^n$ as well, statement 1 follows from Theorem 3.2. It remains to prove statement 2. Let $a \in \langle G_S \rangle$ and write $a = \sum_{i \in S} b_i a_i$ where $b_i \in R$. Set

$$f = \sum_{i \in S} b_i \frac{D_S}{X_i} f_i = aD_S + \text{ lower } \mathbf{x} \text{ terms.}$$

Since $f \in \langle F \rangle$, there is a j such that $lt_\Lambda(f_j) \mid lt_\Lambda(f)$. That is

$$lt_\Gamma(lc_x(f_j))lp_x(f_j) \mid lt_\Gamma(a)D_S$$

and so $lt_\Gamma(lc_x(f_j)) \mid lt_\Gamma(a)$. Moreover, since $lp_x(f_j) \mid D_S$ and S is saturated then $lc_x(f_j) \in G_S$ and so we are done.

Conversely assume statements 1 and 2. Let $f \in \langle F \rangle$ and write, using the assumption of statement 1 and Theorem 2.7 statement 2, $f = \sum_{i=1}^s h_i f_i$ where $h_i \in R[\mathbf{x}]$ and $lp_x(f) = \max_{1 \le i \le s}\{lp_x(h_i)lp_x(f_i)\}$. Set $X = lp_x(f)$. Let S be the saturation of $S_0 = \{i | lp_x(h_i)lp_x(f_i) = X\}$. Then $f = (\sum_{i \in S_0} lc_x(h_i)lc_x(f_i))X +$ lower $\mathbf{x}$ terms. Also $\sum_{i \in S_0} lc_x(h_i)lc_x(f_i) \in \langle G_S \rangle$ and so by statement 2 there is a $j \in S$ such that $lt_\Gamma(a_j) \mid lt_\Gamma(\sum_{i \in S_0} lc_x(h_i)lc_x(f_i))$. Then we see that $lt_\Lambda(f_j) \mid lt_\Lambda(f)$, since $lp_x(f_j) \mid D_S \mid lp_x(f)$. □

We now give the analog to Corollary 3.3 for strong Gröbner bases. The proof is similar to the one for the weak case, and we do not include it.

Corollary 4.2. *Let R be a Γ-graded UFD, and $F = \{f_1, \dots, f_s\}$ be a weak Gröbner basis in $R[\mathbf{x}]$ with respect to $\{0\} \times \mathbf{Z}^n$. For each saturated subset S of $\{1, \dots, s\}$ let $\{a^*_{S,1}, \dots, a^*_{S,t_S}\}$ be a strong Gröbner basis of G_S in R with respect to Γ. Write*

$$a^*_{S,i} = \sum_{j \in S} b_{S,i,j} a_j$$

and define

$$f^*_{S,i} = \sum_{j \in S} b_{S,i,j} \frac{D_S}{X_j} f_j$$

for all $i = 1, \ldots, t_S$. *Then*

$$F^* = \bigcup_{S \text{ saturated}} \{f^*_{S,1}, \ldots, f^*_{S,t_S}\} \cup F$$

is a strong Gröbner basis with respect to Λ.

The above Corollary is a generalization of a result of Möller (1988). There $\Gamma = 0$, and R is a PID and the polynomials $f_{S,i}$'s are called T-polynomials. The next corollary essentially states that result.

Corollary 4.3. *Let* R *be a PID with a trivial grading and let* $F = \{f_1, \ldots, f_s\}$ *be a weak Gröbner basis in* $R[\mathbf{x}]$. *For each saturated subset* S *of* $\{1, ..., s\}$, *let*

$$a^*_S = gcd(a_i \mid i \in S) \textit{ and write } a^*_S = \textstyle\sum_{i \in S} l_i a_i.$$

Define

$$f^*_S = \sum_{i \in S} l_i \frac{D_S}{X_i} f_i.$$

Then

$$F^* = \{f^*_S \mid S \textit{ is a saturated subset of } \{1, ..., s\}\} \cup F$$

is a strong Gröbner basis in $R[\mathbf{x}]$.

Corollary 4.4. *If* R *is a PID with the trivial grading, then every ideal in* $R[\mathbf{x}]$ *has a strong Gröbner basis.*

Proof. By Proposition 2.6 $R[\mathbf{x}]$ has a weak Gröbner basis so by the last corollary $R[\mathbf{x}]$ has a strong Gröbner basis. □

As we did in Corollary 3.4 for Theorem 3.2, we restate Theorem 4.1 in the case $R = k[\mathbf{y}]$, where k is an integral domain, $\mathbf{y} = \{y_1, ..., y_m\}$ are variables with a term order, and we have an elimination order between the $\mathbf{y}$ variables and the $\mathbf{x}$ variables with the $\mathbf{x}$ variables bigger than the $\mathbf{y}$ variables.

Corollary 4.5. *A subset* F *of* $k[\mathbf{y}, \mathbf{x}]$ *is a strong Gröbner basis in* $k[\mathbf{y}, \mathbf{x}]$ *over* k *if and only if*

1. F *is a weak Gröbner basis in* $(k[\mathbf{y}])[\mathbf{x}]$ *over* $k[\mathbf{y}]$ *and*
2. *For all saturated subsets* S *of* $\{1, ..., s\}$, G_S *is a strong Gröbner basis in* $k[\mathbf{y}]$ *over* k.

In the next corollary we specialize to the case where the variables $\mathbf{y}$ are a single variable y. We also assume that k is a field.

Corollary 4.6. *Let* F *be a finite subset of* $k[y, \mathbf{x}]$. *Then* F *is a strong Gröbner basis in* $(k[y])[\mathbf{x}]$ *if and only if* F *is a weak (and hence strong) Gröbner basis in* $k[y, \mathbf{x}]$.

Proof. Applying Theorem 4.1 we have that F is a strong Gröbner basis in $(k[y])[\mathbf{x}]$ if and only if F is a weak Gröbner basis in $(k[y])[\mathbf{x}]$ and G_S is a strong Gröbner basis in $k[y]$ with respect to the trivial grading. The last statement is equivalent to G_S containing the gcd of its elements, which is equivalent to G_S being a weak

Gröbner basis with respect to the canonical $\mathbf{Z}$ grading. So finally using Corollary 3.4 we get the result. □

As mentioned in Section 3, Möller (1988) gives an algorithm for computing a weak Gröbner basis of an ideal I in $(k[y])[\mathbf{x}]$ with respect to the grading $\{0\} \times \mathbf{Z}^n$. Corollaries 4.3 and 4.6 then indicate a method for computing a Gröbner basis of an ideal I in $k[y, \mathbf{x}]$: first compute a weak Gröbner basis of I with respect to the grading $\{0\} \times \mathbf{Z}^n$ using Möller's algorithm, then use Corollary 4.3 to obtain a strong Gröbner basis of I with respect to $\{0\} \times \mathbf{Z}^n$; by Corollary 4.6, this is a weak Gröbner basis in $k[y, \mathbf{x}]$.

We now go back to the general situation. We observed in the Example directly above Proposition 3.7, that even though F is a weak Gröbner basis, it need not be true that each of the sets F_S, for saturated sets S, is a weak Gröbner basis. The same situation occurs for strong Gröbner bases. Indeed, in the same example we note that the grading on $R[x_1, x_2] = k[y, x_1, x_2]$ is just a term order over a field and so weak Gröbner basis and strong Gröbner basis are equivalent. Thus F being a strong Gröbner basis does not even imply that F_S is a weak Gröbner basis, let alone a strong Gröbner basis. Again for full subsets this problem does not occur, i.e. analogously to Proposition 3.7 we have

Proposition 4.7. *If F is a strong Gröbner basis in $R[\mathbf{x}]$ with respect to Λ, then F_S is also a strong Gröbner basis in $R[\mathbf{x}]$ with respect to Λ for all full subsets S of $\{1, \ldots, s\}$.*

Proof. Let $f \in \langle F_S \rangle$ and write $f = aX+$ lower $\mathbf{x}$ terms, where $a \in R$ and X is a power product in $\mathbf{x}$. We need to find a $j \in S$ such that $lt_\Lambda(f_j) \mid lt_\Lambda(f)$, that is, $lt_\Gamma(a_j) \mid lt_\Gamma(a)$ and $X_j \mid X$. We first note that by Proposition 2.4, F is a weak Gröbner basis with respect to Λ, and so by Proposition 3.7, F_S is a weak Gröbner basis with respect to Λ. Thus by Theorem 3.2, F_S is a weak Gröbner basis with respect to $\{0\} \times \mathbf{Z}^n$. Hence, using Proposition 3.5, there is a saturated subset T of S such that $D_T \mid X$ and $a \in \langle G_T \rangle$. Now T is also a saturated subset of $\{1, \ldots, s\}$ since if $i \in \{1, \ldots, s\}$, then $X_i \mid D_T$ implies $X_i \mid D_S$ which in turn implies that $i \in S$, since S is saturated in $\{1, \ldots, s\}$, and so finally $i \in T$ since T is saturated in S. Thus by Theorem 4.1, G_T is a strong Gröbner basis with respect to Γ. Hence there is a $j \in T$ such that $lt_\Gamma(a_j) \mid lt_\Gamma(a)$. Since $j \in T$ we have $X_j \mid D_T$ and so $X_j \mid X$. □

Example. We will continue the Example given at the end of the last section. We add to the weak Gröbner basis F the polynomial $f_5 = (x^2y^2 - 51y^2 + 3x^2)z^2$. One can show that this is the polynomial that we need to add to F using Corollary 4.2 to see that $\{f_1, \ldots, f_5\}$ is a strong Gröbner basis in $\mathbf{Z}[x, y, z]$ (see the corresponding example in Möller (1988)). Alternatively, since in Möller (1988) it is shown that $\{a_1, \ldots, a_5\}$ is a strong Gröbner basis we can apply Proposition 4.7 as we did in the previous example to show that $\{f_1, \ldots, f_5\}$ is a strong Gröbner basis.

5. Structure Theorem for Graded Rings with Strong Gröbner Bases

Möller (1988) states that all ideals in $R = k[x_1, \ldots, x_n]$ for a UFD k can have a strong Gröbner basis only when k is a PID. Here, in our terminology, R has the grading associated to a term order on $\mathbf{x}$ and k has the trivial grading. In this section we show that any Γ-graded ring R with strong Gröbner bases is of the form $R = k[x_1, \ldots, x_n]$, where k is a PID and Γ is $\mathbf{Z}^n$ with a term order (see Theorem

5.4). The statement that the gradings are all basically $\mathbf{Z}^n$ gradings was already noted by Robbiano in Robbiano (1986). We will continue our assumptions made in section 2 concerning the group Γ. Namely, Γ is generated by Γ_0 and Γ_0 is well ordered.

Theorem 5.1. *Assume that R is a Γ-graded UFD and that there are only finitely many homogeneous irreducibles of positive value. Then R is isomorphic to $R_0[x_1, \dots, x_n]$ where R_0 is a UFD, $\{x_1, \dots, x_n\}$ are indeterminates. Furthermore Γ is isomorphic to $\mathbf{Z}^n$, the ordering on Γ is a term ordering and the grading on R is the usual one associated to a term ordering.*

Proof. Since R is a Noetherian UFD, we know that R_0 is also a Noetherian UFD. Let $p_1, \dots, p_s$ be all the homogeneous irreducibles of positive value. Then since every homogeneous element must factor as a product of homogeneous irreducibles we see that $R = R_0[p_1, \dots, p_s]$. Also we see that Γ_0 is generated by $v_\Gamma(p_1), \dots, v_\Gamma(p_s)$. Moreover Γ is torsion free since if $\gamma \in \Gamma$ and $\gamma > 0$ then $\gamma < 2\gamma < 3\gamma < \cdots$ (and similarly if $\gamma < 0$). Hence Γ is isomorphic to $\mathbf{Z}^n$ for some positive integer n. From now on we will assume that $\Gamma = \mathbf{Z}^n$. Let $v_\Gamma(p_i) = \gamma_i \in \mathbf{Z}^n$.

Let $A = (\gamma_i)$ denote the matrix of these vectors. We now show that $s = rank(A)$. It suffices to show that $s \leq rank(A)$ so assume to the contrary that $s > rank(A)$. Then there exists a non empty subset K of $\{1, \dots, s\}$ and non-zero integers a_i for $i \in K$ satisfying $\sum_{i \in K} a_i\gamma_i = 0$. Let $K_1 = \{i \in K \mid a_i > 0\}$ and let $K_2 = K - K_1$. Set $\gamma = \sum_{i \in K_1} a_i\gamma_i = \sum_{i \in K_2}(-a_i)\gamma_i$. Let $b_1 = \prod_{i \in K_1} p_i^{a_i}$ and $b_2 = \prod_{i \in K_2} p_i^{-a_i}$. Then $b_3 = b_1 + b_2$ is in R_γ and none of its irreducible homogeneous divisors can be a p_i with $i \in K_1 \cup K_2$. Set $K_3 = \{i \mid p_i \text{ divides } b_3\}$ and note that $K_3 \neq \emptyset$. Write $b_3 = r_3 \prod_{i \in K_3} p_i^{a_i}$ where $r_3 \in R_0$, and $a_i > 0$ for all $i \in K_3$. Now let $b_4 = b_1b_2 + b_1b_3 + b_2b_3 \in R_{2\gamma}$. Again b_4 can have none of its irreducible homogeneous divisors among the p_i with $i \in K_1 \cup K_2 \cup K_3$. So continue by defining K_4 for b_4 analogously to the above and set $b_5 = b_1b_2b_3 + b_1b_2b_4 + b_1b_3b_4 + b_2b_3b_4$. We continue the argument until we have an element of an R_δ for some $\delta > 0$ with no irreducible homogeneous divisors. This is impossible and so $s = rank(A)$, as desired.

Now set $\mathcal{L} = \{\sum_{i=1}^s a_i\gamma_i \mid a_i \in \mathbf{N}\}$. We show that for all $\gamma \in \mathbf{Z}^n$ we have

$$R_\gamma = \begin{cases} 0 & \text{if } \gamma \notin \mathcal{L} \\ \displaystyle\prod_{i=1}^s p_i^{a_i} R_0 & \text{if } \gamma = \displaystyle\sum_{i=1}^s a_i\gamma_i \in \mathcal{L}. \end{cases}$$

Since $rank(A) = s$, we have for all $\gamma \in \mathcal{L}$ there is a unique decomposition $\gamma = \sum_{i=1}^s a_i\gamma_i$. First assume $\gamma \notin \mathcal{L}$ and let $c \in R_\gamma$ be non-zero. Then $c = r_0 \prod_{i=1}^s p_i^{b_i}$, where $r_0 \in R_0$, and $b_i \in \mathbf{N}$. But then $\gamma = \sum_{i=1}^s b_i\gamma_i \in \mathcal{L}$. This is a contradiction. Now let $\gamma = \sum_{i=1}^s a_i\gamma_i \in \mathcal{L}$ and $c \in R_\gamma$. Then $c = r_0 \prod_{i=1}^s p_i^{b_i}$, where $r_0 \in R_0$, and $b_i \in \mathbf{N}$. Therefore $\gamma = \sum_{i=1}^s b_i\gamma_i = \sum_{i=1}^s a_i\gamma_i$ which implies that $a_i = b_i$ for each i, since $rank(A) = s$. Hence c is in $\prod_{i=1}^s p_i^{a_i} R_0$.

Finally, $s = n$, since $\mathcal{L} = \Gamma_0$, and Γ_0 generates $\mathbf{Z^n}$. Also $\mathcal{L}$ is isomorphic to $\mathbf{N}^n$ since every element of Γ is written uniquely as $\sum_{i=1}^s a_i\gamma_i$. Also $p_1, \dots, p_n$ are algebraically independent because of the direct sum decomposition of R. $\square$

Corollary 5.2. *Assume that R is a Γ-graded UFD and let I be the so-called irrelevant ideal, $I = \sum_{\gamma > 0} R_\gamma$. Assume that I has a strong Gröbner basis. Then R is* *isomorphic to $R_0[x_1, \ldots, x_n]$ where R_0 is a UFD and $\{x_1, \ldots, x_n\}$ are indeterminates. Furthermore Γ is isomorphic to $\mathbf{Z}^n$, the ordering on Γ is a term ordering and the grading on R is the usual one associated to a term ordering.*

Proof. By the previous Theorem, it suffices to show that there are only finitely many homogeneous irreducibles of positive value in R. If $I = 0$ then $R = R_0$ and we are done. Otherwise $I \neq 0$. Let $\{b_1, \ldots, b_t\}$ be a strong Gröbner basis for I. Since I is a homogeneous ideal we may assume that each of the b_i is homogeneous. Then if c is any homogeneous irreducible, there is an i such that $b_i = lt_\Gamma(b_i) \mid c = lt_\Gamma(c)$. Since c is irreducible and b_i is not a unit (one readily sees that $I \cap R_0 = \{0\}$) we see that c is an associate of b_i and so $\{b_1, \ldots, b_t\}$ contains all the homogeneous irreducibles of positive value. □

Proposition 5.3. *Assume that R is a Γ-graded UFD and every ideal in R generated by elements of R_0 has a strong Gröbner basis. Then R_0 is a PID.*

Proof. It suffices to show that for any $c_1, c_2 \in R_0$ with $\gcd(c_1, c_2) = 1$, the ideal $I = \langle c_1, c_2 \rangle$ in R_0 is the unit ideal R_0. Let $J = IR$. Since any divisor of an element of R_0 is in R_0 (Lemma 2.1) and by hypothesis, J has a strong Gröbner basis, we see that there exist $b_1, \ldots, b_t$ in R_0 such that for all $r \in I$ there is an i such that $b_i \mid r$. Thus there exist integers $\nu < \mu$ such that for some i, b_i divides both $c_1^\nu + c_2$ and $c_1^\mu + c_2$ (this follows since there are infinitely many such $c_1^\nu + c_2$ and only finitely many b_i). Then b_i divides the difference $c_1^\mu - c_1^\nu = c_1^\nu(c_1^{\mu-\nu} - 1)$. Note that $d = \gcd(b_i, c_1) = 1$, for otherwise d divides both c_1 and c_2 which is a contradiction to $\gcd(c_1, c_2) = 1$. Thus b_i divides $c_1^{\mu-\nu} - 1$, say $c_1^{\mu-\nu} - 1 = ab_i$ and hence $1 \in I$. □

Theorem 5.4. *Assume that R is a Γ-graded UFD and every ideal in R has a strong Gröbner basis. Then R is isomorphic to $k[x_1, \ldots, x_n]$ where k is a PID and $\{x_1, \ldots, x_n\}$ are indeterminates. Furthermore Γ is isomorphic to $\mathbf{Z}^n$, the ordering on Γ is a term ordering and the grading on R is the usual one associated to a term ordering.*

Proof. This is immediate from the previous three results. □

Corollary 5.5. *Let R be a Γ-graded PID and suppose that every ideal in R has a strong Gröbner basis with respect to Γ. If $\Gamma \neq 0$, then Γ is isomorphic to $\mathbf{Z}$ and R is isomorphic to $k[x]$ where k is a field, x is a single variable and the grading is the canonical grading.*

We note that Corollary 4.4 may be viewed as a converse to Theorem 5.4.

References

[1] Adams, W.W., Boyle, A.K. (1992). Some Results on Gröbner basis over Commutative Rings. *J. Symb. Comp.* **13**, 473–484.

[2] Bayer, D., Stillman, M. (1987). A Theorem on Refining Division Orders by the Reverse Lexicographic Order. *Duke Math. J.* **55**, 321–328.

[3] Buchberger, B. (1985). Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory. *Multidimensional Systems Theory* (N.K.Bose, ed.), D. Reidel Publishing Co., 184–232.

[4] Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner basis and Primary Decomposition of Polynomial Ideals. *J. Symb. Comp.* **6**, 148–168.

[5] Miola, A., Mora, T. (1988). Constructive Lifting in Graded Structures: A Unified View of Buchberger and Hensel Methods. *J. Symb. Comp.* **6**, 306–323.

[6] Möller, H. (1988). On the Construction of Gröbner basis Using Syzygies. *J. Symb. Comp.* **6**, 345–360.

[7] Robbiano, L. (1986). On the Theory of Graded Structures. *J. Symb. Comp.* **2**, 139–170.

[8] Robbiano, L. (1989). Gröbner Bases: A Foundation for Commutative Algebra. Preprint.

[9] Spear, D. (1977). A Constructive Approach to Commutative Ring Theory. *Proceedings 1977 MACSYMA User's Conference*, 369–376.

[10] Shtokhamer, R. (1988). Lifting canonical algorithms from a ring R to the ring $R[x]$. *J. Symb. Comp.* **6**, 169–179.

[11] Zacharias, G. (1978). Generalized Gröbner Bases in Commutative Polynomial Rings. *Thesis at MIT, dept. of Computer Science.*

University of Maryland, College Park, MD

National Science Foundation, Washington D.C.

George Mason University, Fairfax, VA