On the Complexity of Gröbner Bases Conversion

MICHAEL KALKBRENER

Group Market Risk Management, Deutsche Bank AG London

In this paper the complexity of the conversion problem for Gröbner bases is investigated. It is shown that for adjacent Gröbner bases F and G the maximal degree of the polynomials in G, denoted by $deg(G)$, is bounded by a quadratic polynomial in $deg(F)$. For non-adjacent Gröbner bases, however, the growth of degrees can be doubly exponential.

1. Introduction

In recent years several algorithms for converting a Gröbner basis (Buchberger 1965, 1970) for one term order to a Gröbner basis for a different term order have been developed; see for instance Faugère et al. (1993), Faugère (1994), Traverso (1996), Noro and Yokoyama (1995) and Collart et al. (1997). The main reason is the obvious demand for fast conversion algorithms. For instance, if for some polynomial ideal a Gröbner basis with respect to a lexicographic term order is sought, it may well be more efficient to compute first a Gröbner basis with respect to a total degree order, and then to convert, since the former bases are generally much faster to compute than the latter. More specialised applications which by nature involve basis conversions might for instance be the implicitisation of varieties (Hoffmann, 1989; Licciardi and Mora, 1994; Kalkbrener, 1996) and the inversion of polynomial isomorphisms.

Practical experiments with conversion algorithms have been very successful. In this paper we will investigate the theoretical complexity of the conversion problem. We will deal with the following question: let F and G be two reduced Gröbner bases of a polynomial ideal. How much can the maximal degree of the polynomials in F and the maximal degree of the polynomials in G differ? We will prove that for every natural number m there is a prime ideal P and two reduced Gröbner bases F and G of P such that F has bounded degree and $O(m)$ cardinality and G has degree and cardinality at least 2^{2^m}. We will easily derive this doubly exponential lower bound from a theorem in Huynh (1986).

The following doubly exponential upper bound is an immediate consequence of results in Bayer (1982), Möller and Mora (1984) and Giusti (1988): let I be a homogeneous ideal in the polynomial ring $K[x_0, \ldots, x_n]$ over the field K and F and G two reduced Gröbner bases of I and define the degree of F by $deg(F) := \max(\{deg(f) \mid f \in F\})$. Then

$$deg(G) < ((n+1)(deg(F)+1)+1)^{(n+1)2^{dim(I)+1}},$$

where $dim(I)$ denotes the projective dimension of I.

Now the question arises of whether this doubly exponential behaviour can be improved if, instead of two arbitrary Gröbner bases, two adjacent Gröbner bases F and G are considered. The notion of adjacent Gröbner bases can be formulated using the concept of the Gröbner fan (Mora and Robbiano, 1988): F and G are called adjacent if their cones C_1 and C_2 in the Gröbner fan of I are adjacent, i.e. if the intersection of C_1 and C_2 generates an n-dimensional subspace in $\mathbf{Q}^{n+1}$. We will show that for adjacent Gröbner bases F and G the quadratic bound

$$deg(G) < 2 \cdot deg(F)^2 + (n+1) \cdot deg(F) \tag{1.1}$$

holds.

Bound (1.1) can be used for a local complexity analysis of the Gröbner walk (Collart et al., 1997; Amrhein et al., 1996). In this algorithm the Gröbner bases conversion is done in several steps following a path in the Gröbner fan of I. Bound (1.1) shows that the path can always be chosen in such a way that the growth of the degrees in each conversion step is at most quadratic.

2. A Doubly Exponential Lower Bound

In this section we derive a doubly exponential lower bound on Gröbner bases conversion from a result in Huynh (1986).

The natural numbers are denoted by $\mathbf{N}$, the non-negative integers by $\mathbf{N}_0$ and the rational numbers by $\mathbf{Q}$. The set of terms in the variables $x_0, \ldots, x_n$ is denoted by $T(x_0, \ldots, x_n)$. Let f be an element of the polynomial ring $K[x_0, \ldots, x_n]$, where K is an arbitrary field, and I an ideal in $K[x_0, \ldots, x_n]$. For an admissible term order $\prec$ on $T(x_0, \ldots, x_n)$ the initial term of f is denoted by $in_\prec(f)$ and the ideal generated by $\{in_\prec(f) \mid f \in I\}$ by $in_\prec(I)$.

Let $f_1, \ldots, f_r$ be homogeneous polynomials in $K[x_0, \ldots, x_n] \setminus K$ and define

$$g_i := f_i - y_i \quad \text{for } i \in \{1, \ldots, r\}. \tag{2.1}$$

Denote the ideal generated by $f_1, \ldots, f_r$ in $K[x_0, \ldots, x_n]$ by I and the prime ideal generated by $g_1, \ldots, g_r$ in $K[x_0, \ldots, x_n, y_1, \ldots, y_r]$ by P. Let $\prec_x$ be a graded order on $T(x_0, \ldots, x_n)$, $\prec_y$ an order on $T(y_1, \ldots, y_r)$ and $\prec$ the order on $T(x_0, \ldots, x_n, y_1, \ldots, y_r)$ defined by

$$u_1 v_1 \prec u_2 v_2 \qquad \text{if } u_1 \prec_x u_2 \text{ or } (u_1 = u_2 \text{ and } v_1 \prec_y v_2)$$

for $u_1, u_2 \in T(x_0, \ldots, x_n)$ and $v_1, v_2 \in T(y_1, \ldots, y_r)$.

Lemma 2.1. *For* $u \in T(x_0, \ldots, x_n)$

$$u \in in_{\prec_x}(I) \quad \textit{iff} \quad u \in in_\prec(P).$$

Proof. If $u = in_\prec(f)$ for some $f(x_0, \ldots, x_n, y_1, \ldots, y_r) \in P$ then

$$u = in_{\prec_x}(f(x_0, \ldots, x_n, 0, \ldots, 0)) \quad \text{and} \quad f(x_0, \ldots, x_n, 0, \ldots, 0) \in I.$$

On the other hand, let $u \in in_{\prec_x}(I)$. Then there exists a homogeneous $f \in I$ with $in_{\prec_x}(f) = u$. Write f in the form

$$f = \sum h_i f_i,$$

where every h_i is either homogeneous of degree $deg(f) - deg(f_i)$ or 0. Define

$$g = \sum h_i g_i = \sum h_i f_i - \sum h_i y_i \in P.$$

Since the degree of $f = \sum h_i f_i$ in $x_0, \ldots, x_n$ is greater than the degree of $\sum h_i y_i$ in $x_0, \ldots, x_n$ we obtain

$$u = in_{\prec_x}(f) = in_{\prec}(g).$$

$\square$

Based on the construction in Mayr and Meyer (1982) the following result was shown in Huynh (1986).

Theorem 2.1. *For every $m \in \mathbf{N}$ there is an ideal basis F with bounded degree and $O(m)$ cardinality such that any Gröbner basis equivalent to F has degree and cardinality at least 2^{2^m}.*

Together with the above lemma we immediately obtain the following corollary.

Corollary 2.1. *For every $m \in \mathbf{N}$ there is a prime ideal P and two reduced Gröbner bases F and G of P such that F has bounded degree and $O(m)$ cardinality and G has degree and cardinality at least 2^{2^m}.*

Obviously Lemma 2.1 remains true if we replace definition (2.1) by

$$g_i := f_i - y_i^{deg(f_i)} \quad \text{for } i \in \{1, \ldots, r\}. \tag{2.2}$$

In this case we obtain from Theorem 2.1 that for every $m \in \mathbf{N}$ there is a homogeneous ideal P and two reduced Gröbner bases F and G of P such that F has bounded degree and $O(m)$ cardinality and G has degree and cardinality at least 2^{2^m}.

We want to mention that the constructions (2.1) resp. (2.2) are standard tools in Gröbner basis theory.

3. A Quadratic Upper Bound

In this section we construct a quadratic upper bound for the conversion of adjacent Gröbner bases. Before we give the details of the construction we outline the basic steps.

Let F and G be two adjacent Gröbner bases of a homogeneous ideal I in $K[x_0, \ldots, x_n]$ with respect to term orders $\prec_1$ and $\prec_2$ respectively. It follows from basic properties of the Gröbner fan that there exists a homogeneous ideal J in $K[x_0, \ldots, x_n]$ with the following properties:

$$in_{\prec_1}(I) = in_{\prec_1}(J), \quad in_{\prec_2}(I) = in_{\prec_2}(J)$$

and Ψ generates an n-dimensional subspace in $\mathbf{Q}^{n+1}$, where Ψ is the set of those weight vectors ω such that J is ω-homogeneous. Now we define an equivalence relation $\sim$ on $T(x_0, \ldots, x_n)$ by $u \sim v$ if and only if u and v have the same ω-degree for every $\omega \in \Psi$. This equivalence relation has the following important property (see Corollary 3.1): for every equivalence class E in $T(x_0, \ldots, x_n)$

$$|E \cap \langle\{in_{\prec_1}(f) \mid f \in F\}\rangle| = |E \cap \langle\{in_{\prec_2}(g) \mid g \in G\}\rangle|,$$

where $\langle\{in_{\prec_1}(f) \mid f \in F\}\rangle$ denotes the set of terms which are divisible by an element of $\{in_{\prec_1}(f) \mid f \in F\}$. Note that this property is a generalization of the well known fact that $in_{\prec_1}(I)$ and $in_{\prec_2}(I)$ have the same Hilbert function. In the next step we construct a partition $(E_r)_{r\in R}$ of $T(x_0,\ldots,x_n)$ such that each element E_r of this partition is order-isomorphic to $T(x_0,x_1)$ and for every $i\in\mathbf{N}_0$ the set $\{u\in E_r \mid deg(u)=i\}$ is an equivalence class with respect to $\sim$ (see Lemma 3.2). In this way we are able to reduce the original problem in $T(x_0,\ldots,x_n)$ to the case of two variables. It is easy to show that for $T(x_0,x_1)$ a linear bound exists (Lemma 3.3). From this linear bound which holds in each of the E_r we construct the quadratic bound for $T(x_0,\ldots,x_n)$ in the proof of Proposition 3.1.

The whole proof only uses rather elementary and purely combinatorial arguments. In the following subsection the theorem we want to prove is translated into the language of combinatorics.

3.1. From commutative algebra to combinatorics

Let $I\neq\{0\}$ be a proper homogeneous ideal in the polynomial ring $K[x_0,\ldots,x_n]$. We first recall the definition of the Gröbner fan of I.

The set $\Omega:=\{(\psi_0,\ldots,\psi_n)\in\mathbf{Q}^{n+1} \mid \psi_i\geq 0 \text{ for every } i\in\{0,\ldots,n\}\}$ is called the set of weight vectors. Let $\omega=(\omega_0,\ldots,\omega_n)\in\Omega$. For a term $u=x_0^{i_0}\cdots x_n^{i_n}$ we denote its ω-degree by

$$deg_\omega(u):=\sum_{j=0}^{n} i_j\omega_j.$$

The ω-degree of a non-zero polynomial f, abbreviated $deg_\omega(f)$, is the maximum of the ω-degrees of the terms which occur in f with non-zero coefficients. The initial form of f with respect to ω, abbreviated $in_\omega(f)$, is the sum of all those monomials in f with maximal ω-degree. Furthermore, $deg_\omega(0):=-1$ and $in_\omega(0):=0$. The ideal generated by $\{in_\omega(g) \mid g\in I\}$ is denoted by $in_\omega(I)$. A polynomial f is called ω-homogeneous if $f=in_\omega(f)$. An ideal in $K[x_0,\ldots,x_n]$ is called ω-homogeneous if it has a basis consisting of ω-homogeneous polynomials.

For a term order $\prec$ let $C_\prec(I)$ be the topological closure in $\mathbf{Q}^{n+1}$ of

$$\{\omega\in\Omega \mid in_\prec(I)=in_\omega(I)\}.$$

This is a convex polyhedral cone in $\mathbf{Q}^{n+1}$ with a non-empty interior called the Gröbner cone of I with respect to the term order $\prec$. The Gröbner fan of I is the *finite* set $\{C_\prec(I) \mid \prec \text{ a term order}\}$ (see Mora and Robbiano, 1988). Let $\prec_1$ and $\prec_2$ be term orders and F and G the reduced Gröbner bases of I with respect to $\prec_1$ resp. $\prec_2$. It can be easily shown that $C_{\prec_1}(I)=C_{\prec_2}(I)$ if and only if $F=G$.

We call the term orders $\prec_1$ and $\prec_2$ (resp. the Gröbner bases F and G) adjacent if $C_{\prec_1}(I)\cap C_{\prec_2}(I)$ generates an n-dimensional subspace in $\mathbf{Q}^{n+1}$.

We will prove the following bound.

Theorem 3.1. *Let F and G be reduced Gröbner bases of I. If F and G are adjacent then*

$$deg(G)<2\cdot deg(F)^2+(n+1)\cdot deg(F),$$

where $deg(F):=\max(\{deg(f) \mid f\in F\})$.

For proving this bound we will first transform Theorem 3.1 into a purely combinatorial statement (see Proposition 3.1).

Let $\prec_1$ and $\prec_2$ be adjacent term orders. It follows from basic properties of the Gröbner fan (see, for instance, Collart and Mall, 1997) that we can choose an appropriate $\psi \in C_{\prec_1}(I) \cap C_{\prec_2}(I)$ such that the ideal $J := in_\psi(I)$ in $K[x_0, \ldots, x_n]$ has the following three properties:

(a) $in_{\prec_1}(I) = in_{\prec_1}(J)$ and $in_{\prec_2}(I) = in_{\prec_2}(J)$,
(b) $(1, 1, \ldots, 1) \in \Psi$, where $\Psi := \{\omega \in \Omega \mid J \text{ is } \omega\text{-homogeneous}\}$,
(c) Ψ generates an n-dimensional subspace H in $\mathbf{Q}^{n+1}$.

We define the following equivalence relation $\sim$ on $T(x_0, \ldots, x_n)$: $u \sim v$ for $u, v \in T(x_0, \ldots, x_n)$ if

$$deg_\omega(u) = deg_\omega(v) \quad \text{for every } \omega \in \Psi.$$

Let A be a non-empty subset of $T(x_0, \ldots, x_n)$. We denote the linear hull of A in the K-vector space $K[x_0, \ldots, x_n]$ by $K(A)$, i.e.

$$K(A) := \{\sum_{i=1}^{r} h_i a_i \mid r \in \mathbf{N},\ a_1, \ldots, a_r \in A,\ h_1, \ldots, h_r \in K\}.$$

It is well known that the ideals $in_{\prec_1}(I)$ and $in_{\prec_2}(I)$ have the same Hilbert function. Since they can be regarded as initial ideals of J it follows from Lemma 3.1 that these ideals even satisfy the stronger condition

$$dim(in_{\prec_1}(I) \cap K(E)) = dim(in_{\prec_2}(I) \cap K(E)) \quad \text{for every equivalence class } E. \qquad (3.1)$$

Lemma 3.1. *Let $\prec$ be a term order and $E \subseteq T(x_0, \ldots, x_n)$ an equivalence class with respect to $\sim$. Then the subvector spaces $J \cap K(E)$ and $in_\prec(J) \cap K(E)$ in $K(E)$ have the same dimension.*

Proof. For $f \in K(E)$ we denote the equivalence class of f in the factor space $K(E)/(J \cap K(E))$ by $[f]$. We want to show that the set $C := \{[u] \mid u \in E,\ u \notin in_\prec(J)\}$ is a basis of the vector space $K(E)/(J \cap K(E))$. Denote the elements of C by $[u_1], \ldots, [u_r]$ and choose $h_1, \ldots, h_r \in K$ such that $\sum_{i=1}^r h_i[u_i] = [0]$. Then $\sum_{i=1}^r h_i u_i \in J$ and therefore reducible to 0 modulo the reduced Gröbner basis $G_\prec$ of J with respect to $\prec$. By definition of C, $h_1 = \ldots = h_r = 0$. Hence, C is linearly independent. Let $f \in K(E)$ and f' the normal form of f modulo $G_\prec$. Since every polynomial in $G_\prec$ is ω-homogeneous for every $\omega \in \Psi$, $f' \in K(E)$ and $[f] = [f']$. Hence, C is a basis of $K(E)/(J \cap K(E))$ and

$$dim(J \cap K(E)) = |E| - dim(K(E)/(J \cap K(E))) = |E| - |C| = dim(in_\prec(J) \cap K(E)).$$

□

We define a partial order $\ll$ on $T(x_0, \ldots, x_n)$ by $u \ll v$ if u divides v. Let A be a subset of $T(x_0, \ldots, x_n)$. A is called an upset or order filter if $a \ll u$ implies $u \in A$ for every $a \in A$ and $u \in T(x_0, \ldots, x_n)$. A is called an antichain if any two distinct elements of A are incomparable w.r.t. $\ll$. Let $\langle A \rangle$ be the smallest upset which contains A, i.e.

$$\langle A \rangle := \{u \in T(x_0, \ldots, x_n) \mid a \ll u \text{ for some } a \in A\}.$$

We say that A generates $\langle A \rangle$. Obviously every upset in $T(x_0, \ldots, x_n)$ is generated by a uniquely defined antichain. Furthermore, a subset A of $T(x_0, \ldots, x_n)$ is a minimal basis of a monomial ideal in $K[x_0, \ldots, x_n]$ if and only if A is an antichain in $T(x_0, \ldots, x_n)$.

Corollary 3.1. *Let F and G be reduced Gröbner bases of I w.r.t. the adjacent term orders $\prec_1$ and $\prec_2$. Then for every equivalence class E in $T(x_0,\ldots,x_n)$*

$$|E \cap \langle \{in_{\prec_1}(f) \mid f \in F\} \rangle| = |E \cap \langle \{in_{\prec_2}(g) \mid g \in G\} \rangle|.$$

Proof. Since $E \cap \langle \{in_{\prec_1}(f) \mid f \in F\} \rangle$ is a basis of $in_{\prec_1}(I) \cap K(E)$, the corollary immediately follows from (3.1). □

Hence, for proving Theorem 3.1 it suffices to show the following result:

Proposition 3.1. *Let A and B be antichains in $T(x_0,\ldots,x_n)$ with $|E \cap \langle A \rangle| = |E \cap \langle B \rangle|$ for every equivalence class E in $T(x_0,\ldots,x_n)$. If $A \neq \{1\}$ then*

$$deg(B) < 2 \cdot deg(A)^2 + (n+1) \cdot deg(A). \tag{3.2}$$

3.2. Proof of the bound

Before we are able to prove this proposition we need more information about the equivalence relation $\sim$.

The subspace $H \subseteq \mathbf{Q}^{n+1}$ is the variety of a linear form $f = m_0x_0 + \ldots + m_nx_n$, where

(1) $m_0,\ldots,m_n$ are integers,
(2) $\gcd(m_0,\ldots,m_n) = 1$,
(3) at least one of the m_i is positive,
(4) at least one of the m_i is negative.

Without loss of generality we assume that the variables are ordered in such a way that there exists an $l \in \{0,\ldots,n-1\}$ with

$$m_i > 0 \text{ for } i \in \{0,\ldots,l\} \quad \text{and} \quad m_j \leq 0 \text{ for } j \in \{l+1,\ldots,n\}.$$

We define $s := \prod_{i=0}^{l} x_i^{m_i}$ and $t := \prod_{j=l+1}^{n} x_j^{-m_j}$. Let $R \subseteq T(x_0,\ldots,x_n)$ be the set of terms which are neither divisible by s nor by t. For every $r \in R$ and $k \in \mathbf{N}_0$ define

$$E_{r,k} := \{rs^it^{k-i} \mid i \in \{0,\ldots,k\}\} \text{ and } E_r := \bigcup_{k \in \mathbf{N}_0} E_{r,k}.$$

Obviously, for every $u \in T(x_0,\ldots,x_n)$ there exist uniquely determined $i,j \in \mathbf{N}_0$ and $r \in R$ with $u = rs^it^j$. Hence,

(1) $\bigcup_{r \in R} E_r = T(x_0,\ldots,x_n)$,
(2) $E_{r_1} \cap E_{r_2} = \emptyset$ for $r_1, r_2 \in R$ with $r_1 \neq r_2$,
(3) for every $r \in R$ the function o, defined by $o(rs^it^j) := x_0^ix_1^j$, is an order isomorphism between the posets E_r and $T(x_0,x_1)$.

Hence $(E_r)_{r \in R}$ is a partition of $T(x_0,\ldots,x_n)$ and each of the E_r is isomorphic to the poset $T(x_0,x_1)$. We will show in Lemma 3.2 that for every $r \in R$ and every $k \in \mathbf{N}_0$ the set $E_{r,k}$ which is the set of elements of rank k in the poset E_r is an equivalence class. By means of this result we will reduce the problem of proving bound (3.2) to the construction of a bound for antichains in $T(x_0,x_1)$. This bound will be given in Lemma 3.3.

Lemma 3.2. *For every $r \in R$ and $k \in \mathbf{N}_0$ the set $E_{r,k}$ is an equivalence class.*

PROOF. By definition, $deg_\omega(s) = deg_\omega(t)$ for every $\omega \in \Psi$. Let $u = rs^i t^{k-i}$ and $v = rs^j t^{k-j}$ be elements of $E_{r,k}$. Then $deg_\omega(u) = deg_\omega(r) + k \cdot deg_\omega(s) = deg_\omega(v)$ for every $\omega \in \Psi$ and therefore $u \sim v$.

On the other hand, assume that $u = x_0^{i_0} \cdots x_n^{i_n}$ and $v = x_0^{j_0} \cdots x_n^{j_n}$ are elements of $T(x_0, \ldots, x_n)$ with $i_0 \geq j_0$ and $u \sim v$. Then there exists an $l \in \mathbf{N}_0$ with

$$(l \cdot m_0, \ldots, l \cdot m_n) = (i_0 - j_0, \ldots, i_n - j_n).$$

Hence, $ut^l = vs^l$ and therefore $u, v \in E_{r,k}$ for some $r \in T(x_0, \ldots, x_n)$ and $k \in \mathbf{N}_0$. □

The degree of $f \in K[x_0, \ldots, x_n]$ in the variable x_i is denoted by $deg_i(f)$.

LEMMA 3.3. *Let A, B be antichains in $T(x_0, x_1)$ such that $|\{u \in \langle A \rangle \mid deg(u) = k\}| = |\{u \in \langle B \rangle \mid deg(u) = k\}|$ for every $k \in \mathbf{N}_0$. If $A \neq \{1\}$ then*

$$deg(B) < 2 \cdot deg(A).$$

PROOF. For $C \subseteq T(x_0, x_1)$ and $k \in \mathbf{N}_0$ define $\nabla_k(C) := \{u \in \langle C \rangle \mid deg(u) = k\}$. Note that for every $i \geq 2 \cdot deg(A) - 1$ the set

$$\{deg_0(a) \mid a \in \nabla_i(A)\}$$

is an interval in $\mathbf{N}_0$. Therefore,

$$|\nabla_{i+1}(B)| = |\nabla_{i+1}(A)| = |\nabla_i(A)| + 1 \leq |\nabla_{i+1}(\nabla_i(B))| \leq |\nabla_{i+1}(B)|.$$

Thus, $deg(B) \leq i$ and the lemma is proved. □

By proving Proposition 3.1 we will now complete the proof of Theorem 3.1.

PROOF OF PROPOSITION 3.1. Let A and B be antichains in $T(x_0, \ldots, x_n)$ with $|E \cap \langle A \rangle| = |E \cap \langle B \rangle|$ for every equivalence class E in $T(x_0, \ldots, x_n)$ and assume that $A \neq \{1\}$. Let $b \in B$ and write it in the form $b = rs^i t^{k-i}$ for some $r \in R$ and $i, k \in \mathbf{N}_0$. We will prove this proposition by giving bounds for $deg(r)$, k and $deg(s)$ and $deg(t)$ (see (3.3), (3.5) and (3.6)).

Denote $deg(A)$ by α and $\max(\{deg_i(a) \mid a \in A\})$ by α_i for every $i \in \{0, \ldots, n\}$. First we show that for every $r = (r_0, \ldots, r_n) \in R$

$$E_r \cap B \neq \emptyset \text{ implies } r_i \leq \alpha_i \text{ for every } i \in \{0, \ldots, n\}. \tag{3.3}$$

Let $r = (r_0, \ldots, r_n) \in R$, $k \in \mathbf{N}_0$ with $E_{r,k} \cap B \neq \emptyset$ and $i \in \{0, \ldots, n\}$. If $r_i = 0$ then (3.3) obviously holds. Therefore assume $r_i > 0$ and let $e_i \in \mathbf{N}_0^{n+1}$ be the vector which is 1 on the i-th position and 0 everywhere else. Obviously,

$$E_{r,k} \cap \langle B \rangle \neq \{u + e_i \mid u \in E_{r-e_i,k} \cap \langle B \rangle\}$$

and therefore

$$|E_{r,k} \cap \langle A \rangle| = |E_{r,k} \cap \langle B \rangle| > |E_{r-e_i,k} \cap \langle B \rangle| = |E_{r-e_i,k} \cap \langle A \rangle|.$$

Hence there exist $v \in E_r \cap \langle A \rangle$ and $a \in A$ such that a divides v but does not divide $v - e_i$. Thus,

$$deg_i(a) = deg_i(v) \geq r_i$$

and (3.3) is proved.

Let $r \in R$. Obviously, $E_r \cap \langle A \rangle$ is an upset in the poset E_r. Let C be the antichain which generates this upset in E_r. We will show that

$$E_{r,k} \cap C = \emptyset \qquad \text{for } k > \alpha. \tag{3.4}$$

Let $k > \alpha$ and $u \in E_{r,k} \cap \langle A \rangle$. Then there exists an $a = r_1 s^{i_1} t^{j_1} \in A$ which divides u. Let $v = r_2 s^{i_2} t^{j_2}$ such that $u = av$. From $av \in E_r$ we obtain $r_1 r_2 \in E_r$. Write $r_1 r_2$ in the form $rs^l t^{l'}$. Since s and t do not divide r_2 we have $l + l' \leq \mathit{deg}(r_1)$. Hence, $a' := ar_2$ is an element of $E_{r,l+l'+i_1+j_1} \cap \langle A \rangle$ and

$$l + l' + i_1 + j_1 \leq \mathit{deg}(a) \leq \alpha.$$

Since a' divides u, $u \notin C$ and (3.4) is proved.

Let $C' \subseteq E_r$ be the antichain which generates the upset $E_r \cap \langle B \rangle$ in E_r. Since E_r is isomorphic to $T(x_0, x_1)$ and

$$|E_{r,k} \cap \langle C \rangle| = |E_{r,k} \cap \langle C' \rangle|$$

we obtain from Lemma 3.3 and (3.4)

$$E_{r,k} \cap C' = \emptyset \qquad \text{for } k \geq 2\alpha. \tag{3.5}$$

If $A \neq B$ there exist $a \in A \setminus B$, $b \in B \setminus A$, $r \in R$ and $i, j, k \in \mathbf{N}_0$ with $k > 0$ and $a = rs^i t^{k-i}$ and $b = rs^j t^{k-j}$. In particular,

$$\mathit{deg}(s) = \mathit{deg}(t) \leq \alpha. \tag{3.6}$$

Let $b \in B$ and write it in the form $b = rs^i t^{k-i}$ for some $r \in R$ and $i, k \in \mathbf{N}_0$. By (3.3) and (3.5), $\mathit{deg}(r) \leq (n+1)\alpha$ and $k < 2\alpha$. Together with (3.6),

$$\mathit{deg}(b) < 2\alpha^2 + (n+1)\alpha.$$

□

We finish this paper by presenting for every $d \in \mathbf{N}$ adjacent Gröbner bases A_d and B_d with $\mathit{deg}(A_d) = d$ and $\mathit{deg}(B_d) = d^2$.

In Möller and Mora (1984) a class of homogeneous ideals $(I_{dn})_{d,n \in \mathbf{N}}$ in $n+1$ variables is given. Each of these ideals has reduced Gröbner bases A_{dn} and B_{dn} with $\mathit{deg}(A_{dn}) = d$ and $\mathit{deg}(B_{dn}) = d^n$. If $n = 2$ the Gröbner bases

$$A_{d2} = \{x_0^d - x_1 x_2^{d-1},\ x_1^d\}, \qquad B_{d2} = \{x_0^d - x_1 x_2^{d-1},\ x_1^d,\ x_0^d x_1^{d-1},\ x_0^{2d} x_1^{d-2}, \ldots,\ x_0^{d^2}\}$$

are adjacent.

Acknowledgements

I am grateful to Peter Bürgisser and Daniel Mall for many interesting discussions.

References

Amrhein, B., Gloor, O., Küchlin, W. (1996). Walking faster. In *Proc. DISCO'96, Springer LNCS 1128*, pp. 150–161, Karlsruhe, Germany.

Bayer, D. (1982). *The division algorithm and the Hilbert scheme.* PhD thesis, Harvard Univ., Dept. of Math., Cambridge, Massachusetts, USA.

Buchberger, B. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Univ. Innsbruck, Dept. of Math., Innsbruck, Austria.

Buchberger, B. (1970). Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Mathematicae* **4**, 374–383.

Collart, S., Kalkbrener, M., Mall, D. (1997). Converting bases with the Gröbner walk. *J. Symb. Comp.* **24**, 465–470.

Collart, S., Mall, D. (1997). Toric degenerations of polynomial ideals and geometric localisation of fans. *J. Symb. Comp.* **24**, 443–464.

Faugère, J.C. (1994). *Résolution des systèmes d'équations algébriques.* PhD thesis, Univ. Paris VI, Dept. of Math., Paris, France.

Faugère, J.C., Gianni, P., Lazard, D., Mora, T. (1993). Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comp.* **16**, 329–344.

Giusti, M. (1988). Combinatorial dimension theory of algebraic varieties. *J. Symb. Comp.* **6**, 249–265.

Hoffmann, C.M. (1989). *Geometric and Solid Modeling: An Introduction.* Morgan Kaufmann Publishers Inc., San Mateo, California, USA.

Huynh, D.T. (1986). A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems. *Information and Control* **68**, 196–206.

Kalkbrener, M. (1996). Implicitization by Gröbner basis conversion. *Euromath Bull.* **2**, 197–204.

Licciardi, S., Mora, T. (1994). Implicitization of hypersurfaces and curves by the Primbasissatz and basis conversion. In *Proc. ISSAC'94*, pp. 191–196, Oxford, UK.

Mayr, E.W., Meyer, A.R. (1982). The complexity of the word problem for commutative semigroups and polynomial ideals. *Advances in Math.* **46**, 305–329.

Möller, H.M., Mora, T. (1984). Upper and lower bounds for the degree of Gröbner bases. In *Proc. EUROCAL'84, Springer LNCS 174*, pp. 172–183, Cambridge, UK.

Mora, T., Robbiano, L. (1988). The Gröbner fan of an ideal. *J. Symb. Comp.* **6**, 183–208.

Noro, M., Yokoyama, K. (1995). New methods for the change-of-ordering in Gröbner basis computation. Research report ISIS-RR-95-8E, Institute for Social Information Science, FUJITSU, Numazu, Japan.

Traverso, C. (1996). Hilbert functions and Buchberger algorithm. *J. Symb. Comp.* **22**, 355–376.