INFORMATION AND CONTROL 68, 196–206 (1986)

A Superexponential Lower Bound for Gröbner Bases and Church–Rosser Commutative Thue Systems

DUNG T. HUYNH

Computer Science Department, Iowa State University, Ames, Iowa 50011

The complexity of the normal form algorithms which transform a given polynomial ideal basis into a Gröbner basis or a given commutative Thue system into a Church–Rosser system is presently unknown. In this paper we derive a double-exponential lower bound (2^{2^n}) for the production length and cardinality of Church–Rosser commutative Thue systems, and the degree and cardinality of Gröbner bases.

0. INTRODUCTION

The design and analysis of algorithms for computational problems in commutative algebra is certainly among the most active areas of research in computer algebra. In particular, computational problems for polynomial ideals have received considerable attention. The first algorithms for polynomial ideals have been provided by Hermann and improved by Seidenberg (see (Buchberger, in press)).

In Buchberger (1970), he proposes an "efficient" method for solving a variety of computational problems in the classical ideal theory. The central idea of his method is an algorithm that transforms any given basis of a polynomial ideal into an equivalent basis in normal form, which is called a Gröbner basis. When polynomial ideals are specified by Gröbner bases, many computational problems can be solved very elegantly, e.g., the membership problem (which is the problem of deciding whether a polynomial belongs to an ideal). The method of Gröbner bases has been implemented in several software packages including IBM SCRATCHPAD computer algebra system.

Another area that has a certain connection to classical ideal theory is the theory of commutative semigroups. This link is expressed by the fact that several problems for commutative semigroups can be reduced to those for polynomial ideals, e.g., the uniform word problem is reducible to the membership problem. In particular, if a commutative semigroup is given by a system of defining relations, then such a system can be transformed into

0019-9958/86 $3.00

normal form using Buchberger's method. It turns out that such a system in normal form is exactly a Church–Rosser system and in this case Buchberger's algorithm specializes to Ballantyne–Lankford's algorithm for transforming a commutative Thue system into an equivalent Church–Rosser system (Ballantyne and Lankford, 1981).

At present, the complexity of the above algorithms is not known. Despite their simplicity, there are, however, no explicit (good) lower and upper bounds. The only conclusion available from the work of Cardoza, Lipton, Mayr, and Meyer is that any algorithm that computes Gröbner bases or Church–Rosser commutative Thue systems requires exponential space (cf., (Ballantyne and Lankford, 1981; Buchberger, in press)). In particular, there is no good lower bound for the production length and cardinality of Church–Rosser commutative Thue systems or the degree and cardinality of Gröbner bases.

In this paper we show that a double-exponential lower bound holds in both cases for both parameters. Actually, we prove the lower bound for Church–Rosser commutative Thue systems. The same result holds for Gröbner bases as a corollary. The results are proved by applying a technique in (Mayr and Meyer, 1982) showing that commutative Thue systems can "count" double-exponentially large integers and by observing a connection between a Church–Rosser commutative Thue system and the minimal representatives of the classes of the congruence generated by the Thue system.

There are 4 sections. Section 1 contains general definitions, notations, and the precise statements of the results. Section 2 derives some properties of Church–Rosser commutative Thue systems and Gröbner bases. Section 3 proves the Main Lemma that establishes the main results. In Section 4 we include some concluding remarks.

1. Preliminaries and Results

In this section we review some known definitions, notations used in this work, and state the main results.

In this paper $\mathbb{N}$, $\mathbb{Q}$ denote the sets of nonnegative integers and rationals, respectively. Let $X = \{x_1,..., x_m\}$. Then $\mathbb{Q}[X]$ or $\mathbb{Q}[x_1,..., x_m]$ denotes the ring of polynomials in $x_1,..., x_m$ with rational coefficients. For a subset $F = \{f_1,..., f_s\} \subseteq \mathbb{Q}[X]$, Ideal($F$) (or Ideal($f_1,..., f_s$)) denotes the ideal generated by F, i.e.,

$$\text{Ideal}(f_1,..., f_s) = \left\{ \sum_{i=1}^{s} q_i f_i \,\middle|\, q_i \in \mathbb{Q}[X] \text{ for } i = 1,..., s \right\}.$$

In the following we introduce the concept of Gröbner bases due to Buchberger. (See (Buchberger, in press) for more details.)

For a finite alphabet $S = \{s_1,..., s_k\}$, $S^{\oplus}$ denotes the free commutative (or com. for short) monoid generated by S. An element of $S^{\oplus}$, called a (com.) word, is written in the form $s_1^{e_1} \cdots s_k^{e_k}$, where $e_i \in \mathbb{N}$ for $i = 1,..., k$. Notice that power products in $\mathbb{Q}\{x_1,..., x_m\}$ may be regarded as elements of $\{x_1,..., x_m\}^{\oplus}$.

We will use two orderings on $S^{\oplus}$. The partial ordering $\leqslant$ is defined as follows: For $u = s_1^{e_1} \cdots s_k^{e_k}$ and $v = s_1^{d_1} \cdots s_k^{d_k}$ in $S^{\oplus}$, $u \leqslant v$ iff $e_i \leqslant d_i$ for all $i = 1,..., k$. The second ordering, denoted by $\preccurlyeq$, is a total one and is defined as follows: For $u = s_1^{e_1},..., s_k^{e_k}$ and $v = s_1^{d_1},..., s_k^{d_k}$ in $S^{\oplus}$, $u \preccurlyeq v$ iff either $u = v$ or $\sum e_i < \sum d_i$ or $\sum e_i = \sum d_i$ and u is less than v lexicographically.

DEFINITION 1.1 (Buchberger, in press). Let $F = \{f_1,..., f_s\} \subseteq \mathbb{Q}[X]$ be an ideal basis:

(1) Let $p, q \in \mathbb{Q}[X]$. p reduces to q mod F, written $p \to_F q$, iff there is $f \in F$, $u \in X^{\oplus}$, and $\rho \in \mathbb{Q}$ such that the leading power products (w.r.t. $\preccurlyeq$) of p and $\rho \cdot u \cdot f$, and their leading coefficients are equal, and $q = p - \rho \cdot u \cdot f$.

(2) $q \in \mathbb{Q}[X]$ is in normal form mod F iff there is no q' such that $q \to_F q'$.

(3) q is a normal form of p mod F iff $p \xrightarrow{*}_F q$ and q is in normal form, where $\xrightarrow{*}_F$ denotes the reflexive, transitive closure of $\to_F$.

DEFINITION 1.2 (Buchberger, in press). (1) An ideal basis $F \subseteq \mathbb{Q}[X]$ is called a *Gröbner basis* iff for every $p \in \mathbb{Q}[X]$, if q_1 and q_2 are normal forms of p mod F, then $q_1 = q_2$.

(2) An ideal basis $F \subseteq \mathbb{Q}[X]$ is called a *reduced Gröbner basis* iff F is a Gröbner basis and for every $f \in F$, f is in normal form mod $F \setminus \{f\}$ and its leading coefficient is 1.

Notation 1.3. For $p \in \mathbb{Q}[X]$ let $\deg(p)$ denote the degree of p. For an ideal basis $F \subseteq \mathbb{Q}[X]$, the degree of F, denoted by $\deg(F)$, is Max $\{\deg(f) \mid f \in F\}$. The cardinality of a basis F, denoted by $\text{card}(F)$, is the number of its elements.

We next introduce the notion of Church–Rosser commutative Thue systems. (The reader is referred to Ballantyne and Lankford (1981); Book (1983), for more details.)

Let S be a finite alphabet. A com. semi-Thue system over S is given by a finite set of productions $R \subseteq S^{\oplus} \times S^{\oplus}$. Let $u, v \in S^{\oplus}$. u derives v in one step (written $u \Rightarrow_R v$) by application of a production in R iff there is $(l, r) \in R$ with $l \leqslant u$ such that $u = wl$ and $v = wr$. $\xRightarrow{*}_R$ denotes the reflexive, transitive

closure of $\Rightarrow_R$. A derivation is a sequence $(u_0, u_1, ..., u_n)$ of words in $S^\oplus$ such that $u_i \Rightarrow_R u_{i+1}$ for all $i = 0, ..., n-1$. A com. semi-Thue system R is said to be a com. Thue system iff $(l, r) \in R$ implies $(r, l) \in R$.

Let R be a com. Thue system over a finite alphabet S. Then $\overset{*}{\Rightarrow}_R$ defines a congruence on $S^\oplus$ which is denoted by $\sim R$ and we write $u \sim v \bmod R$ iff u, v belong to the same class. (S, R) is called a presentation of the quotient semigroup $S^\oplus / \sim R$, and R is called a set of defining relations.

DEFINITION 1.4. Let R be a com. Thue system over S:

(1) Let $u, v \in S^\oplus$ with $u \Rightarrow_R v$. $u \Rightarrow_R v$ is called a *reduction* w.r.t. R, written $u \to_R v$, iff u derives v in one step using a production $(l, r) \in R$ that satisfies $l \succ r$.

(2) A word $u \in S^\oplus$ is *irreducible* w.r.t. R iff there is no $v \in S^\oplus$ with $u \to_R v$.

(3) R is said to be *Church–Rosser* iff for all $u, v \in S^\oplus$, $u \sim v \bmod R$ implies that if $u \overset{*}{\to}_R u'$, $v \overset{*}{\to}_R v'$, and u', v' are irreducible w.r.t. R, then $u' = v'$.

(4) R is said to be a *reduced Church–Rosser* com. Thue system iff R is Church–Rosser and for every production $(l, r) \in R$, l and r are irreducible w.r.t. $R \setminus \{(l, r)\}$.

Notation 1.5. For $u \in S^\oplus$, length (u) denotes the length of u. For $(u, v) \in S$ the height of (u, v), denoted by height (u, v), is $\mathrm{Max}\{\mathrm{length}(u), \mathrm{length}(v)\}$. For a finite subset $R \subseteq S^\oplus \times S^\oplus$, the height of R, denoted by height (R), is $\max\{\mathrm{height}(u, v) \mid (u, v) \in R\}$. The cardinality of R is denoted by $\mathrm{card}(R)$.

The main results of this paper are the following theorems:

THEOREM I. *For every $n \in \mathbb{N}$, $n > 0$, there is a com. Thue system R with bounded height and $O(n)$ cardinality such that any Church–Rosser com. Thue system equivalent to R has height and cardinality at least 2^{2^n}.*

THEOREM II. *For every $n \in \mathbb{N}$, $n > 0$, there is an ideal basis F with bounded degree and $O(n)$ cardinality such that any Gröbner basis equivalent to F has degree and cardinality at least 2^{2^n}.*

Remarks. (1) We see later that the reduced Church–Rosser com. Thue system (reduced Gröbner basis) equivalent to a given one is unique. (This is known for Gröbner bases (Buchberger, in press).)

(2) Theorem II will be obtained as a corollary from Theorem I. We will see that a com. Thue system is reduced Church–Rosser iff it is reduced Gröbner when regarded as a polynomial ideal basis.

2. Some Properties of Church–Rosser Commutative Thue Systems and Gröbner Bases

In this section we want to derive several properties of Church–Rosser commutative Thue systems and Gröbner bases. We first introduce some notions and notations.

Let $\leqslant$ and $\preccurlyeq$ be the partial and total orderings on $S^{\oplus}$ as defined in Section 1. Then $\preccurlyeq$ satisfies the following properties: (1) $\varepsilon \preccurlyeq u$ for all $u \in S^{\oplus}$, where ε is the empty word, (2) $u \preccurlyeq v$ iff[1] $u+w \preccurlyeq v+w$ for all $u, v, w \in S^{\oplus}$. Concerning $\leqslant$ there is the well-known theorem by Dickson which states that any subset $I \subseteq S^{\oplus}$ has finitely many minimal elements. The set of minimal elements of I is denoted by $\operatorname{Min} I$.

A subset $I \subseteq S^{\oplus}$ is called an ideal iff[2] $I + S^{\oplus} \subseteq I$. If I is an ideal in $S^{\oplus}$, then $I = \operatorname{Min} I + S^{\oplus}$.

In the following let R be a com. Thue system over S. For any $u \in S^{\oplus}$ let $\sigma(u)$ denote the minimal element w.r.t. $\preccurlyeq$ which is congruent to u mod R. The set of these elements is denoted by U_R, i.e.,

$$U_R = \{u \in S^{\oplus} \mid u = \sigma(u)\}.$$

Further, if R is Church–Rosser, we may assume that R is given by productions of the form (l, r) with $l \succ r$.

It is not hard to show the following.

Proposition 2.1. *Let R be a com. Thue system over S. Then $S^{\oplus} \setminus U_R$ is an ideal in $S^{\oplus}$.*

Proof. See Eilenberg and Schützenberger (1969), Proposition 6.1. ∎

Proposition 2.2. *Let R be a com. Thue system over S. If R is Church–Rosser, then $u \xrightarrow{*}_R \sigma(u)$ for every $u \in S^{\oplus}$.*

Proof. Obvious. ∎

Proposition 2.3. *Let R be a com. Thue system over S. Further let $A_R := S^{\oplus} \setminus U_R$. If R is Church–Rosser, then for every $u \in \operatorname{Min} A_R$ there is some $v \in S^{\oplus}$ such that $(u, v) \in R$.*

Proof. We show that for every $u \in \operatorname{Min} A_R$ there is a production of the form (u, v) in R. To this end, observe that $u \in A_R$ implies $u \neq \sigma(u)$. Therefore, $u \to_R^+ \sigma(u)$. This implies that there is a production (w, v) applicable at u. Hence $w \leqslant u$. We claim that $w = u$. Assume otherwise that

[1] The operation in $S^{\oplus}$ is also written as $+$.

[2] For $A, B \subseteq S^{\oplus}$, $A + B = \{u + v \mid u \in A \text{ and } v \in B\}$.

$w < u$. Then $w \in U_R$ which implies that $w = \sigma(w)$. On the other hand, $w \to_R v$ implies that $w \succ \sigma(w)$, a contradiction! ∎

COROLLARY 2.4. *Let R be a com. Thue system over S. Again let $A_R := S^{\oplus} \setminus U_R$. If R is reduced Church–Rosser, then*

$$\text{Min } A_R = \{l \mid (l, r) \in R\}.$$

Proof. From the proof of Proposition 2.3 it remains to show that there is no production $(u, v) \in R$ with $u > w$ for some $w \in \text{Min } A_R$. Assume otherwise that such a production exists. Let $w \in \text{Min } A_R$ with $w < u$. Since R is Church–Rosser, there is, by Proposition 2.3, a production of the form (w, v) in R. Now, $u > w$ implies that u is not irreducible w.r.t. $R \setminus \{(u, v)\}$ and hence R is not reduced, a contradiction! ∎

THEOREM 2.5. *Let R be a com. Thue system over S and $A_R := S^{\oplus} \setminus U_R$. If R is reduced Church–Rosser, then it holds that*

$$\{l \mid (l, r) \in R\} = \text{Min } A_R$$

and[3]

$$\{r \mid (l, r) \in R\} \subseteq U_R.$$

Proof. The equality is from Corollary 2.4. It remains to show the inclusion. Assume otherwise that there is a production (u, v) in R so that $v \in A_R$. Let w be some element of Min A_R with $w \leqslant v$. Since R is Church–Rosser, there is, by Proposition 2.3, a production of the form $(w, \bar{v})$. Thus v is not irreducible w.r.t. $R \setminus \{(u, v)\}$ and hence R is not reduced, a contradiction. ∎

COROLLARY 2.6. *To every com. Thue system there is a unique equivalent reduced Church–Rosser com. Thue system.*

Proof. Follows immediately from Theorem 2.5. ∎

In the remainder of this section we make some observations about the connection between (reduced) Church–Rosser com. Thue systems and (reduced) Gröbner bases.

For a given com. Thue system R over S let Ideal(R) denote Ideal$(l - r \mid (l, r) \in R) \subseteq \mathbb{Q}[S]$.

THEOREM 2.7. *Let R be a com. Thue system over S. Let G be the reduced Gröbner basis for* Ideal(R). *Then the following holds*:

[3] Actually A_R is the set of M-terms in the case of Gröbner bases (Buchberger, 1976).

(1) *The elements of G are of the form* $u - v$, $u, v \in S^{\oplus}$.

(2) *The set* $\{(u, v) \mid u - v \in G\}$ *is the reduced Church–Rosser system equivalent to R.*

Proof. Observe that Buchberger's algorithm for reduced Gröbner bases with bases obtained from com. Thue systems on the input behaves exactly as Ballantyne–Lankford's algorithm for reduced Church–Rosser com. Thue systems does (Buchberger, in press). From the uniqueness of reduced Gröbner bases (op. cit.) Theorem 2.7 follows. ▮

Remark. From Theorem 2.7 we see that uniqueness of reduced Church–Rosser com. Thue systems follows from uniqueness of reduced Gröbner bases. However, Corollary 2.6 is obtained in a simpler way.

For the proof of Theorem II as a corollary of Theorem I we need the following lemma.

LEMMA 2.8. *Let R be a com. Thue system over S and G be any Gröbner basis for* Ideal(R). *Further let* $A_R := S^{\oplus} \setminus U_R$. *Then* Min A_R *is contained in the set of leading power products of the elements of G.*

Proof. The lemma is proven via a property of Gröbner bases shown in Buchberger (1976), which states that the sets of M-terms[4] of two Gröbner bases of a given ideal are the same (cf. Buchberger, 1976, Lemma 1.8).

Now consider the reduced Gröbner basis of Ideal(R). By Theorems 2.5 and 2.7, it follows that the set of M-terms of the reduced Gröbner basis for Ideal(R) is exactly A_R. This proves Lemma 2.8. ▮

From the results we prove in this section it is obvious that Theorem I and Theorem II can be obtained from the following.

MAIN LEMMA. *For every* $n \in \mathbb{N}$, $n > 0$, *there is a com. Thue system R over a finite alphabet S such that the following holds*:

(1) *There is some* $u \in$ Min A_R *with length*$(u) \geqslant 2^{2^n}$,

(2) *Card*(Min A_R) $\geqslant 2^{2^n}$,

(3) *R has bounded height and* $O(n)$ *productions,*

where $A_R = S^{\oplus} \setminus U_R$ *and* U_R *is the set of the least representatives of classes of the congruence defined by R.*

The main lemma proof will be shown in the next section.

[4] A power product is an M-term iff it is $\geqslant$ the leading power product of some basis element.

3. Proof of Main Lemma

This section provides a proof for the Main Lemma which establishes Theorems I and II. The proof is based on a technique of reducing counter machine computation to the word problem for com. semigroup, which is the problem of deciding for a com. Thue system R over S and two words $u, v \in S^{\oplus}$ whether $u \sim v \bmod R$ (cf. Mayr and Meyer, 1982, Sect. 6). The basic idea is that com. Thue systems can "count" double-exponentially large integers.

The idea of our proof is as follows. Let x, y, t, c be symbols of some finite alphabet S, which will be specified later. Let $n \in \mathbb{N}$ and $ex_n := 2^{2^n}$. We will construct a com. Thue system R with the following properties: Let $w := tcx^e y^f$, $e + f = ex_n$:

(a) If $u \geqslant w$, then $\sigma(u) \neq u$, i.e., u is not the least representative of its class.

(b) If $u < w$, then $\sigma(u) = u$.

(a) and (b) imply that $\{w \mid w = tcx^e y^f \text{ and } e + f = ex_n\}$ is a subset of $\operatorname{Min} A_R$, where $A_R = S^{\oplus} \setminus U_R$ and U_R is the set of the least representatives w.r.t. the congruence generated by R.

The following lemma is shown in Mayr and Meyer, (1982).

Lemma 3.1. *Let $n \in \mathbb{N}$ and $ex_n := 2^{2^n}$. There is a finite alphabet X containing s', c', t', b' and a com. Thue system P over X with bounded height and $O(n)$ productions such that*

$$s'c' \sim t'c'b'^{ex_n} \bmod P.$$

Furthermore, if $s'c' \sim w \bmod P$ and w contains an occurrence of s' or t', then either $w = s'c'$ or $w = t'c'b'^{ex_n}$.

Proof. See Mayr and Meyer (1982), Lemma 6, and Lemma 8. (Note that s' is used to start computation, whereas t' means that computation stops; c' is a control symbol.) ▮

With the notations of Lemma 3.1 the following facts hold.

Fact 3.2. *There is a unique repetition-free derivation in P leading from $s'c'$ to $t'c'b'^{ex_n}$. Furthermore, this derivation contains at every step at least three symbols different from b'.*

Proof. This unique repetition-free derivation is given in the proof of Lemma 6 in (Mayr and Meyer, 1982). ▮

Concerning words of the form $t'c'b'^e$, $e < ex_n$, we have

FACT 3.3. *Let u and v be two words of the form $t'c'b'^e$, $e < ex_n$. If there is a word w such that $w \sim u \bmod P$ and $w \sim v \bmod P$, then the repetition-free derivations from w to u and from w to v are identical and $u = v$.*

Proof. Otherwise Lemma 3.1 and Fact 3.2 would be violated. ∎

We now construct the com. Thue system R. Let a, x, $\bar{x}$, y, $\bar{y}$, z, $\bar{z}$, s, t_1, t_2, $d_1,\ldots, d_3$, $s_1,\ldots, s_5$, $c_1,\ldots, c_5$ be symbols.

Construct the production $(s_1c_1, s_1d_1d_2d_3)$ and a set of productions for the equivalence

$$s_1d_1 \sim t_1d_1a^{ex_n}. \tag{3.1}$$

Construct a set of productions for the equivalence

$$t_1d_2 \sim t_2d_2x^{ex_n}. \tag{3.2}$$

Construct a set of productions for the equivalence

$$t_2d_3a^{ex_n} \sim s_2d_3 \tag{3.3}$$

together with the production $(s_2d_1d_2d_3, s_2c_2)$.

(*Comment.* d_1, d_2, d_3 are control symbols in (3.1), (3.2), (3.3). The productions in (3.1), (3.2), and (3.3) have the effect that any derivation starting at $s_2c_2x^e$ must apply first productions in (3.3), then productions in (3.2). Productions in (3.1) can be applied only when $e \geqslant ex_n$. Thus, if $e < ex_n$, then such a derivation leads to some other word of greater length.)

Add the production

$$(s_2c_2, s_3c_3s). \tag{3.4}$$

Construct a set of productions for the equivalence

$$s_3c_3 \sim s_4c_4\bar{z}^{ex_n}. \tag{3.5}$$

Add the productions

$$(sx, s\bar{x}z), \qquad (sy, s\bar{y}z). \tag{3.6}$$

(*Comment.* (3.6) converts x to $\bar{x}$, y to $\bar{y}$, where the total number of converted x's and y's is the number of z's.)

Construct a set of productions for the equivalence

$$s_4c_4\bar{z}^{ex_n}z^{ex_n} \sim s_5c_5. \tag{3.7}$$

(*Comment.* (3.7) is used to test whether the total number of converted x's and y's is ex_n.)

Add the production

$$(s_5c_5x,\ s_5c_5y). \tag{3.8}$$

(*Comment.* (3.8) is used to convert one x of a word $s_5c_5x^ey^f$ to y.)
Add the productions

$$(s_5c_5\bar{x},\ s_5c_5x),\ (s_5c_5\bar{y},\ s_5c_5y). \tag{3.9}$$

(*Comment.* (3.9) converts $\bar{x}$'s and $\bar{y}$'s back to x's and y's, respectively.)
Let R be the set of productions in (3.1)–(3.9), where the auxiliary symbols in the subconstructions are distinct, and let S be the set of all symbols.

LEMMA 3.4. *Every word w of the form $s_2c_2x^ey^f$ with $e+f=ex_n$ is congruent to s_1c_1 mod R, i.e., $\sigma(w)\neq w$.*

Proof. By (3.1)–(3.3) we have

$$s_1c_1 \sim s_2c_2x^{ex_n} \bmod R.$$

Further, any word $w=s_2c_2x^ey^f$ with $e+f=ex_n$ is congruent to $ss_5c_5y^{ex_n}$ mod R by (3.4)–(3.9). Therefore, $w\sim s_2c_2x^{ex_n}$ mod R. ∎

LEMMA 3.5. *Let $w=s_2c_2x^ey^f$ with $e+f=ex_n$. Then for every word u, if $u<w$, then $\sigma(u)=u$.*

Proof. If u does not contain s_2 or c_2, then no production is applicable and hence $\sigma(u)=u$. Therefore, we may assume that $u=s_2c_2x^{e'}y^{f'}$ and $e'+f'<ex_n$.

We claim that if there is a derivation in R leading from u to another word $v\neq u$, then length$(v)>$length(u) and hence $\sigma(u)=u$.

First, observe that in a derivation starting at u, which applies productions in (3.3), (3.2) only, a word containing t_1d_1 can never be reached. Further, if such a derivation reaches a word containing s_2c_2, then by Fact 3.3 it must be u itself.

Second observe that a derivation starting at u, which applies productions in (3.4)–(3.7), can never apply any productions in (3.8), (3.9), since the number of z's is not sufficient so that s_5c_5 can be obtained by (3.7).

From the above observations, it follows that we need only to consider those words v which u may reach by applying either only productions in (3.3), (3.2), or only productions in (3.4)–(3.7). It is not hard to see that in each case, either $v=u$ or length$(v)>$length(u). Thus, $\sigma(u)=u$, and this completes the proof of Lemma 3.5. ∎

From Lemma 3.4 and 3.5, the Main Lemma follows, since it can easily be seen that height(R) is bounded and R has $O(n)$ productions.

4. Concluding Remarks

The results we obtain in this paper show that any normal form algorithm for Gröbner bases or Church–Rosser commutative Thue systems requires double-exponential time, since the size of the output is double-exponential in the worst-case. Our proof technique, based on the power of commutative Thue systems of "counting" double-exponentially large integers, cannot be extended to obtain better lower bounds, since otherwise it would also provide a lower bound sharper than the exponential lower bound for the space complexity of the uniform word problem for commutative semigroups, which is known to be exponential-space complete.

As a by-product, the results in Section 2 give a clear answer to the question whether Ballantyne–Lankford's algorithm is different from Biryukov's algorithm for the equivalence problem for commutative semigroups (cf. Cardoza, Lipton, and Meyer, 1976) as remarked in (Ballantyne and Lankford, 1981). In particular, Theorem 2.5 and Corollary 2.6 seem to be interesting in their own right.

Received: September 12, 1984; accepted: October 28, 1985

References

Ballantyne, A., and Lankford, D. (1981), New decision algorithms for finitely presented commutative semigroups, *Comput. Math. Appl.* **7**, 159–165.

Book, R. (1983), Thue systems and the Church–Rosser property: Replacement systems, specification of formal languages, and presentations of monoids, *in* "Combinatorics on Words: Progress and Perspectives" (L. Cummings, Ed.), pp. 1–38, Academic Press, New York/London.

Buchberger, B. (1970), Ein Algorithmisches Kriterium fur die Lösbarkeit eines Algebraischen Gleichungssystems, *Aequationes Math.* **4**, 374–383.

Buchberger, B. (1976), Some properties of Gröbner bases for polynomial ideals, *ACM SIGSAM Bull.* **10**, 19–24.

Buchberger, B. (in press), Gröbner bases: An algorithmic method in polynomial ideal theory, *in* "Recent Trends in Multidimensional Systems Theory," (N. K. Bose, Ed.).

Cardoza, E. (1975), "Computational Complexity of the Word Problem for Commutative Semigroups," tech. memo. 67, MIT, Cambridge, Mass.

Cardoza, E., Lipton, R., and Meyer, A. (1976), Exponential space complete problems for petri nets and commutative semigroups, *in* "Proceedings of the 8th Annu. ACM Sympos. Theory of Comput. Conference," pp. 50–54.

Eilenberg, S., and Schützenberger, M. (1969), Rational sets in commutative monoids, *J. Algebra* **13**, 173–191.

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