NONCOMMUTATIVE GRÖBNER BASES FOR THE COMMUTATOR IDEAL

SUSAN HERMILLER[1] AND JON MCCAMMOND[2]

Abstract. Let I denote the commutator ideal in the free associative algebra on m variables over an arbitrary field. In this article we prove there are exactly $m!$ finite Gröbner bases for I, and uncountably many infinite Gröbner bases for I with respect to total division orderings. In addition, for $m = 3$ we give a complete description of its universal Gröbner basis.

Let A be a finite set and let K be a field. We denote the free associative algebra over K with noncommuting variables in A by $K\langle A\rangle$ and the polynomial ring over K with commuting variables in A by $K[A]$. The kernel of the natural map $\gamma : K\langle A\rangle \to K[A]$ is called the *commutator ideal*. The commutator ideal in $K\langle A\rangle$, and in particular its noncommutative Gröbner bases, have been used to investigate properties of finitely generated ideals in the commutative polynomial ring $K[A]$. This has occurred, for example, in the study of free resolutions [1] and the homology of coordinate rings of Grassmannians and toric varieties [12]. In this article we establish several new results about noncommutative Gröbner bases for the commutator ideal in $K\langle A\rangle$. Our main results are as follows:

Theorem A. *There are exactly $m!$ finite reduced complete rewriting systems for the m-generated free commutative monoid and exactly $m!$ finite reduced Gröbner bases for the commutator ideal of the m-variable free associative algebra. In addition, each such rewriting system and Gröbner basis is induced by a shortlex ordering.*

Theorem B. *There are uncountably many reduced complete rewriting systems for the m-generated free commutative monoid which are compatible with a total division ordering when $m \geq 3$. As a consequence, there are uncountably many reduced noncommutative Gröbner bases with respect to total division orderings for the commutator ideal in the m-variable free associative algebra, each with a distinct set of normal forms.*

Date: June 15, 2007.

[1]Supported under NSF grant no. DMS-0071037

[2]Supported under NSF grant no. DMS-0101506

Theorem C. *The universal Gröbner basis for the commutator ideal in the free associative algebra $K\langle a, b, c\rangle$ consists of the binomials*

$$\begin{array}{ccc} ab - ba & bc - cb & ca - ac \\ ab^j c^k - b^j c^k a & bc^k a^i - c^k a^i b & ca^i b^j - a^i b^j c \\ ac^k b^j - c^k b^j a & ba^i c^k - a^i c^k b & cb^j a^i - b^j a^i c \end{array}$$

for all positive integers i, j, and k.

These theorems extend and complement several other recent results. In [5] Green, Mora, and Ufnarovski compare other properties of the Gröbner fan and universal Gröbner basis for the noncommutative and commutative cases. In [3] Eisenbud, Peeva, and Sturmfels show that for any ideal J of $K[A]$, after a generic change of coordinates, the ideal $\gamma^{-1}(J)$ must have a finite noncommutative Gröbner basis, using a specific lift of a term ordering (or total division ordering) for $K[A]$ to a total division ordering for the free associative algebra. For the more restrictive case of monoidal ideals, Diekert [2] has shown that every commutative monoid has a finite complete rewriting system. In [6], Kramer, Laubenbacher, and the first author showed that there are uncountably many distinct Gröbner bases for the commutator ideal with respect to division orderings which were not typically total division orders. Finally, we note that U. Martin [9] has independently established Theorem B.

Organization: As can be seen from the statements given above, the study of Gröbner bases for the commutator ideal can also be reformulated in terms of complete rewriting systems for the free commutative monoid. Section 1 is a brief review of rewriting systems, noncommutative Gröbner bases, and the connection between these two theories. In Section 2 we use rewriting systems to classify the finite reduced Gröbner bases for the commutator ideal (Theorem A). The proof shows that every finite Gröbner basis for this ideal which is compatible with a division ordering, is also compatible with a total division ordering. Section 3 uses geometry to classify all of the potential sets of normal forms for the 3-generator free commutative monoid. This classification is needed in the proofs of Theorems B and C which are established in Section 4. The last section, Section 5, is devoted to open questions and a few final comments.

1. Basic definitions

In this section we review the basic definitions for noncommutative Gröbner bases and rewriting systems, as well as the theorem (Theorem 1.7) connecting these two concepts. For further information about rewriting systems see [16], for a more detailed account of noncommutative Gröbner bases see [5] and [11], and for the connections between these topics see [8]. We begin with rewriting systems.

Definition 1.1 (Division ordering)**.** Let A be a finite set and let A^* be the collection of all (noncommutative) words, including the empty word, over the alphabet A. A *division ordering* on A^* is a partial ordering which is well-founded and compatible with concatenation; that is, there are no infinite descending sequences and for all $u, v, w \in A^*$ with $u > v$, we also have $wu > wv$ and $uw > vw$. A division ordering is *total* if any two elements in A^* are comparable.

We will follow the convention that symbols from the beginning of the alphabet, such as a, b, c denote elements of A (i.e. "letters") and symbols from the end, such as u, v, w denote elements of A^* (i.e. "words").

A common example of a total division ordering is the shortlex ordering. Given a total ordering on a set A, there is a natural lexicographic, or dictionary, ordering on words in A^* which we will denote $>_{lex}$. The corresponding *shortlex ordering* $>$ on A^* is defined by setting $u > v$ if $length(u) > length(v)$, or $length(u) = length(v)$ and $u >_{lex} v$.

Definition 1.2 (Rewriting system)**.** A subset R of $A^* \times A^*$ is called a *rewriting system*. Corresponding to each ordered pair (u, v) in R there is a basic replacement rule $u \to v$. In order to be compatible with concatentation the basic rule $u \to v$ implies the replacement rules $xuy \to xvy$ for all $x, y \in A^*$. Since elements of R lead immediately to basic replacement rules, we will simply say $u \to v$ is a rule in R or $u \to v \in R$.

Every rewriting system R leads to a reflexive and transitive ordering on A^* defined by $x \geq y$ if x can be rewritten to y in a finite number of steps. A rewriting system R is *terminating* if the induced ordering of A^* is a division ordering, it is *confluent* if $x \geq y$ and $x \geq z$ implies there is a $w \in A^*$ such that $y \geq w$ and $z \geq w$, and it is *complete* if it is both terminating and confluent.

Definition 1.3 (Normal forms)**.** The words in A^* which cannot be rewritten by a rewriting system R are called *irreducible words*. If every proper subword of w is irreducible we say that w is *nearly irreducible*. If R is terminating, then every word in A^* can be rewritten to an irreducible word. If R is also confluent then this irreducible word is unique. Thus, in a complete rewriting system, every word can be reduced to a unique irreducible word called its *normal form*. Since any subword of an irreducible word is also irreducible, the set of normal forms is closed under the taking of subwords.

A complete rewriting system R is *reduced* if for every rule $u \to v$ in R, v is irreducible and u is nearly irreducible.

Definition 1.4 (Monoid presentation)**.** Every rewriting system R determines a monoid presentation $M = \langle A \mid \{u = v \mid (u, v) \in R\}\rangle$. Moreover, the ordering on A^* induced by R is *compatible* with this monoid in the sense that $x \geq y$ implies that x and y are words representing the same element of M. If R is also complete, then the normal forms are in one-to-one correspondence with the elements of M.

For each element $m \in M$, the *congruence class* of m is the set of all words in A^* that represent the element m. For a complete rewriting system, the ordering on A^* restricted to a congruence class of M is a partially ordered set with a minimum element. Conversely, let M be a monoid generated by A and let $>$ be a division ordering on A^* which is compatible with M. If $>$ restricted to each congruence class is a partially ordered set with a minimum element then there is a unique reduced complete rewriting system R over the alphabet A which presents M and such that for every rule $u \to v \in R$, $u > v$. Note that each irreducible word is precisely the minimum element of its congruence class with respect to $>$.

Eschenbach [4] has given an example of a finite reduced complete rewriting system for a monoid which is compatible with a division ordering, but not with any total division ordering, so allowing division orderings which are not total results in a more general construction.

We now turn to noncommutative Gröbner bases.

Definition 1.5 (Leading term)**.** Let K be a field and let A be a set of size m. The monoid ring of A^* over K is known as the *m-variable free associative algebra over K*, which we will denote by $K\langle A\rangle$. If $>$ is a total division ordering on A^* and $f = k_1m_1 + \cdots k_jm_j$ is an element of $K\langle A\rangle$ (with $k_i \in K$ and $m_i \in A^*$ for each i), then the *leading term* of f is the term k_im_i such that $m_i > m_j$ for all $j \neq i$. If $>$ is merely a division ordering then the leading term of f is defined as above, but not every f in $K\langle A\rangle$ will have a leading term. If f is an element of $K\langle A\rangle$ with leading term k_im_i, then the replacement rule corresponding to f is

$$m_i \to \frac{-1}{k_i}\sum_{j\neq i} m_jk_j$$

The definitions for rewriting systems can readily be extended to this context.

Definition 1.6 (Noncommutative Gröbner basis)**.** Let I be an ideal in the m-variable free associative algebra $K\langle A\rangle$. A *noncommutative Gröbner basis* for I with respect to a division ordering $>$ is a set G of generators for I such that (1) every element of G has a leading term and (2) the corresponding system of replacement rules is confluent. When the ordering $>$ is total, the first condition is immediate and the second is equivalent to the statement that the leading terms of G generate the same ideal as the leading terms of I. We will always use the weaker definition which does not require a total ordering unless otherwise specified.

A Gröbner basis G is *reduced* if no term of any polynomial in G is divisible by the leading term of another polynomial in G. The *universal Gröbner basis* for I is the union of all of the reduced Gröbner bases with respect to all (total) division orderings for this ideal. Theoretically, restricting to total division orderings could change the universal Gröbner basis of an ideal. For the universal Gröbner basis for the commutator ideal described in Theorem C, however, either definition yields the same result.

The following theorem outlines the connection between rewriting systems and Gröbner bases in the specific case we will need to use in later sections. Its proof is straightforward from the definitions and will be omitted.

Theorem 1.7. *If $\mathbb{N}^m$ denotes the m-generated free commutative monoid on A and I denotes the commutator ideal in the m-variable free associative algebra, then there is a bijective correspondence between the reduced complete rewriting systems on A for $\mathbb{N}^m$ and the reduced Gröbner bases for I. More specifically, if R is a reduced complete rewriting system for $\mathbb{N}^m$ compatible with a (total) division ordering $>$ on A^*, then $\{u - v \mid u \to v \in R\}$ is a reduced Gröbner basis for I with respect to $>$, and conversely, if G is a reduced Gröbner basis for I with respect to a (total) division ordering $>$, then the elements of G must be of the form $u - v$ where u and v are monomials and the set $\{u \to v \mid u - v \in G, u > v\}$ is a reduced complete rewriting system for $\mathbb{N}^m$ compatible with $>$.*

Note that Eschenbach's result mentioned earlier shows that weakening statements such as this to allow non-total division orderings tends to include additional rewriting systems and additional Gröbner bases. In particular, a consequence of Eschenbach's example is that there exists a finitely generated ideal in an associative algebra which has a Gröbner basis with respect to a division ordering, but does not contain a Gröbner basis with respect to any total division ordering.

2. Finite Gröbner bases

Let $\mathbb{N}^m$ denote the free commutative monoid generated by $A = \{a_1, \ldots, a_m\}$ and let $K\langle A\rangle$ denote the free associative algebra with variables A. In this section we classify the finite Gröbner bases for the commutator ideal in $K\langle A\rangle$ by classifying the finite reduced complete rewriting systems for $\mathbb{N}^m$. These tasks are equivalent by Theorem 1.7. We begin by analyzing the simplest rules in such a rewriting system.

Lemma 2.1. *If R is a complete rewriting system for $\mathbb{N}^m$, then for every $i \neq j$ between 1 and m, R contains either the rule $a_i a_j \to a_j a_i$ or the rule $a_j a_i \to a_i a_j$. If R is reduced, then these are the only rules which involve at most two elements of A.*

Proof. Since a word of length 1 is the unique representative of a monoid generator it must be its normal form. Similarly, the product of two distinct monoid generators a_i and a_j has only two representatives (namely $a_i a_j$ and $a_j a_i$), so one of these is the normal form and the other must be reducible to it. Since every proper subword of both words is already in normal form, there must be an explicit rule in R which rewrites $a_i a_j \to a_j a_i$ or $a_j a_i \to a_i a_j$ (but not both). The final assertion follows from the fact that every word in

A^* which involves only two letters can be reduced to a unique normal form using only the rules already described. □

The 2-variable rules can be encoded in a graph to make them easier to describe.

Definition 2.2 (2-variable graph)**.** Let R be a complete rewriting system for $\mathbb{N}^m$. The 2-*variable graph* associated to R is a directed graph Γ with vertex set A and a directed edge from a_i to a_j if and only if $a_j a_i \to a_i a_j$ is a rule in R.

By Lemma 2.1, every pair of vertices in Γ is connected by an edge in one direction or the other. In other words, Γ is what graph theorists call a *tournament*. In Lemma 2.4 we will show how 2-variable graphs restrict the set of possible normal forms for a complete rewriting system.

Lemma 2.3. *Let R be a complete rewriting system for $\mathbb{N}^m$. If w is a nearly irreducible word and a is a variable, then all occurrences of a in w occur consecutively.*

Proof. Suppose not and let w be a shortest nearly irreducible word which fails to have this property. Since nearly irreducible words are closed under the taking of subwords we can assume that $w = aua$ where u is a non-trivial word which does not contain a. Then the distinct words au and ua are irreducible words which represent the same element of $\mathbb{N}^m$, giving a contradiction. □

Lemma 2.4. *If R is a complete rewriting system for $\mathbb{N}^m$ and w is a nearly irreducible word of length at least 3, then the sequence in which the variables occur in w corresponds to a simple directed path in the 2-variable graph for R.*

Proof. Let Γ be the 2-variable graph for R. The path in Γ corresponding to w is directed because the length 2 subwords of w are irreducible and it is simple by Lemma 2.3. □

The following corollary is a simple application of Lemma 2.4.

Corollary 2.5. *Let R be a complete rewriting system for $\mathbb{N}^3$ whose 2-variable graph is a directed cycle $a \to b \to c \to a$. For every $i, j, k > 0$, a nearly irreducible word which represents (i, j, k) is of the form $a^i b^j c^k$, $b^j c^k a^i$ or $c^k a^i b^j$.*

There is also a strong connection between Γ and the finiteness of R.

Lemma 2.6. *If R is a reduced complete rewriting system for $\mathbb{N}^m$, then R is finite if and only if its 2-variable graph is acyclic.*

Proof. Let Γ be the 2-variable graph for R and suppose Γ contains a directed cycle from a_{i_1} to a_{i_2} to a_{i_3} to $\ldots a_{i_k}$ to a_{i_1}. If R were a finite system there would be an upper bound on the length of the words involved in its rules.

Let N be such an upper bound and consider the words $u = a_{i_1}^N a_{i_2}^N \cdots a_{i_k}^N$ and $v = a_{i_2}^N a_{i_3}^N \cdots a_{i_k}^N a_{i_1}^N$. These words represent the same element of the monoid, but neither of these words can be rewritten using the rules in R. Specifically, every subword of u or v of length at most N involves only two variables, all 2-variable rules are of the form $a_i a_j \to a_j a_i$ (Lemma 2.1), and u and v are reduced with respect to these rules. Thus R is not finite.

On the other hand, if Γ is acyclic, then Γ is the graph of a total ordering of A and by relabeling the a_i we can assume that $a_j a_i \to a_i a_j$ is a rule in R for each $i < j$. Using only these rules, every word in A^* can be reduced to a word of the form $a_1^{n_1} \cdots a_m^{n_m}$. Since these words are in one-to-one correspondence with the elements of $\mathbb{N}^m$, the 2-variable rules in R form a complete rewriting system for $\mathbb{N}^m$. Because R is reduced, these are the only rules in R and R is finite. $\square$

The rest of the classification is nearly immediate.

Theorem A. *There are exactly $m!$ finite reduced complete rewriting systems for the m-generated free commutative monoid and exactly $m!$ finite reduced Gröbner bases for the commutator ideal of the m-variable free associative algebra. In addition, each such rewriting system and Gröbner basis is induced by a shortlex ordering.*

Proof. Let R be a finite reduced complete rewriting system for $\mathbb{N}^m$ and let Γ be its 2-variable graph. By Lemma 2.6 Γ is acyclic and thus it can be used to define a total ordering on A and a corresponding shortlex ordering on A^*. There are exactly $m!$ such shortlex orderings. This shortlex ordering leads to the rewriting system R and to the corresponding Gröbner basis for the m-variable free associative algebra using the correspondence described in Theorem 1.7. $\square$

3. Potential normal forms

For the remainder of the article we restrict our attention to the case $m = 3$. Let R be a reduced complete rewriting system for $\mathbb{N}^3$ over $A = \{a, b, c\}$ and let Γ be its 2-variable graph. Of the possible 2-variable graphs, 6 are acyclic and correspond to the 6 shortlex orderings on A^*. The remaining possibilities contain a directed cycle, but with only three vertices, there are only two choices for Γ: either a directed cycle $a \to b \to c \to a$ or a directed cycle $a \to c \to b \to a$. Without loss of generality we will restrict our comments to the first case. We will assume, in other words, that R contains the rules $ba \to ab$, $cb \to bc$ and $ac \to ca$. By Corollary 2.5 the set of normal forms for such a rewriting system has all of the following properties.

Definition 3.1 (Potential normal forms)**.** Let $\mathcal{F}$ be a subset of A^* which contains exactly one representative of each element in $\mathbb{N}^3$. We will call $\mathcal{F}$ a *potential set of normal forms* if (1) $\mathcal{F}$ contains ab, bc, and ca, (2) $\mathcal{F}$ is closed under the taking of subwords, and (3) for all $i, j, k > 0$, the representative of (i, j, k) is of the form $a^i b^j c^k$, $b^j c^k a^i$ or $c^k a^i b^j$. Given a set $\mathcal{F}$ of potential normal forms, we can form a rewriting system R as follows. We call a word w *irreducible with respect to* $\mathcal{F}$ if it lies in $\mathcal{F}$ and *nearly irreducible with respect to* $\mathcal{F}$ if w is not in $\mathcal{F}$ but all of its proper subwords lie in $\mathcal{F}$. We then let R be the rewriting system which consists of all rules of the form $u \to v$ where u is nearly irreducible with respect to $\mathcal{F}$, v is irreducible with respect to $\mathcal{F}$ and u and v represent the same element of $\mathbb{N}^3$.

Such an $\mathcal{F}$ is merely a *potential* set of normal forms because it is not clear, a priori, whether or not the rewriting system defined above is terminating; in particular, it may be possible for the rules to allow a loop of rewritings $x_1 \to x_2 \to \cdots \to x_1$. If the rewriting system is terminating, it would also be complete. On the other hand, if $\mathcal{F}$ came from a reduced complete rewriting system R for $\mathbb{N}^3$ which contains the rules $ba \to ab$, $cb \to bc$ and $ac \to ca$, then this procedure simply reconstructs R from $\mathcal{F}$.

In order to classify the potential sets of normal forms, we first translate these conditions into a coloring of the first octant in $\mathbb{R}^3$.

Definition 3.2 (Octant coloring)**.** A subset S of the first octant $\mathbb{R}^3_{>0}$ is called *convex with respect to the x-axis* if for every point (x, y, z) in S and for all $0 < y' < y$ and $0 < z' < z$, (x, y', z') is also in S. Convexity with respect to the y-axis and z-axis are defined similarly. An *octant coloring* is a 3-coloring of the first octant $\mathbb{R}^3_{>0}$ such that the green portion is convex with respect to the x-axis, the blue portion is convex with respect to the y-axis, the red portion is convex with respect to the z-axis. Thus, if (x, y, z) is colored red, the entire rectangle $(0, x] \times (0, y] \times \{z\}$ is red. This subset is called a *red rectangle*. Green and blue rectangles are defined similarly. See Figure 1 for an illustration of sample rectangles in each of the three colors.

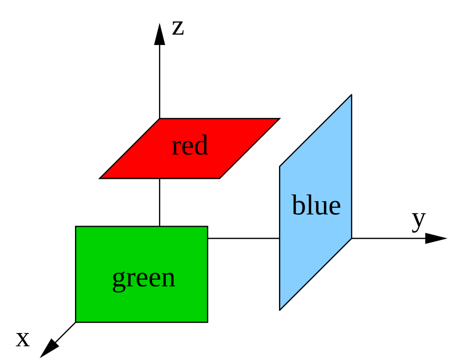

FIGURE 1. A green, red, and blue rectangle.

Definition 3.3 (Equivalent colorings)**.** Two octant colorings will be called *equivalent* if they agree on all integer lattice points. Every octant coloring is equivalent to a coloring constructed out of unit cubes of color. Simply remove the coloring from all points not in the integer lattice and then assign an uncolored (x, y, z) the same color as (i, j, k) where i, j, and k are the least integers greater than or equal to x, y, and z, respectively. This process of constructing an octant coloring from an appropriate coloring of the integer lattice is called *completing the coloring.*

Lemma 3.4. *There is a one-to-one correspondence between potential sets of normal forms and equivalence classes of octant colorings.*

Proof. Given a potential set $\mathcal{F}$ of normal forms for $\mathbb{N}^3$, we can construct an octant coloring by coloring an integer lattice point (i, j, k) (with $i, j, k > 0$) blue if the normal form is $a^i b^j c^k$, red if the normal form is $b^j c^k a^i$, and green if the normal form is $c^k a^i b^j$, and then completing the coloring. The fact that the three color subsets are convex with respect to the appropriate axes follows from the fact that $\mathcal{F}$ is closed under the taking of subwords. Conversely, given an octant coloring, we can define a potential set of normal forms by including $a^i b^j$, $b^j c^k$, and $c^k a^i$ as normal forms for $i, j, k \geq 0$, and using the color of the lattice point (i, j, k) to define its normal form for $i, j, k > 0$. The convexity of the color regions shows that these normal forms are subword closed. $\square$

In the language of octant colorings, the main result of [6] is the following:

Theorem 3.5 (2-colorings are complete)**.** *If $\mathcal{F}$ is a set of potential normal forms which induces a 2-coloring of the first octant, then the rewriting system R derived from $\mathcal{F}$ is a reduced complete rewriting system.*

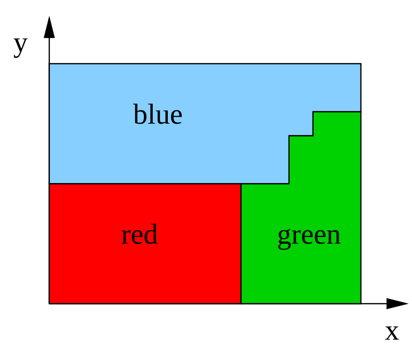

FIGURE 2. A horizontal cross section.

Let P be a plane $z = c$ which slices through an octant coloring. For each t, let $g(t) = \sup\{y|(t, y, c) \text{ is green}\}$. Note that we are allowing the possibility that $g(t) = \infty$ and we assign $g(t) = 0$ if this set is empty. Similarly define $b(t) = \sup\{x|(x, t, c) \text{ is blue}\}$.

Lemma 3.6. *If P is a plane $z = c$ which slices through an octant coloring, then the functions $g(t)$ and $b(t)$ defined above are non-decreasing, and the red portion, if nonempty, is a rectangle $(0, x] \times (0, y] \times \{c\}$ for some $x, y \in (0, \infty]$. Analogous statements are true for cross-sections by planes $x = c$ and $y = c$.*

Proof. The red, blue and green rectangles determined by points in P intersect P in red rectangles with the origin as a corner, green line segments with an open endpoint on the x-axis, and blue line segments with an open endpoint on the y-axis. See Figure 2. Suppose $t' < t$ and $y < g(t')$. The point (t, y, c) cannot be colored blue or red without violating the convexity requirements since the blue line segment or red rectangle would have to pass through the green line segment from $(t', 0, c)$ to $(t', g(t'), c)$. Thus (t, y, c) is green and $g(t) \geq g(t')$. The proof that $b(t)$ is nonincreasing is similar. Finally, if $x' < x$, $y' < y$ and (x, y', c) and (x', y, c) are both red, (x, y, c) cannot be colored blue or green without violating convexity. Thus (x, y, c) is red as well. This completes the proof. $\square$

By combining the information from all three types of cross-sections, the following corollary is immediate. See Figure 3 for an illustration of a stack of blue rectangles.

Corollary 3.7. *In any octant coloring, the portion which is red is a collection of red rectangles whose dimensions are nondecreasing as their z-coordinate increases. Similarly, the blue (green) portion is a collection of nondecreasing blue (green) rectangles.*

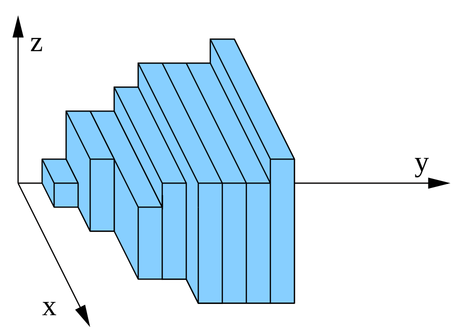

FIGURE 3. A stack of blue rectangles.

4. Directional orderings

This section shows that a special case of normal forms leads to an uncountable family of distinct reduced complete rewriting systems induced by total division orderings. This uncountable collection of examples enables us to establish Theorem B and Theorem C.

We begin by defining a collection of total division orderings on A^* which are lifts of term orderings (or total division orderings) on the commutative polynomial ring $K[a, b, c]$. Partial results are known toward classification of all total division orderings on A^* (see, for example, [15]), including a proof that there are uncountably many total division orderings on the set of words over an alphabet with at least two generators [14]. Total division orderings have been completely classified for words over two generators [10], [13]; the orderings we define here utilize the orderings in [10].

Definition 4.1 (Path)**.** Let w be a word in A^*. One possible representation of w is as path in $\mathbb{R}^3$ starting at the origin where, as we read w from left to right, the path moves one unit in the x-direction when we see an a, one unit in the y-direction when we see a b and one unit in the z-direction when we see a c. We will call this the *path for* w.

Definition 4.2 (2-variable numbers)**.** Let w be a word in A^* representing the element $(i, j, k) \in \mathbb{N}^3$. The 1-*variable numbers for* w are $N_a(w) = i$, $N_b(w) = j$ and $N_c(w) = k$. The 2-*variable number* $N_{ba}(w)$ will encode information about the projection of the path for w into the xy-plane. In particular, it will denote the area below the projected path, but inside the rectangle $[0, i] \times [0, j]$. Combinatorially, $N_{ba}(w)$ denotes the number of ways w can be written as $xbyaz$ where x, y and z are possibly empty words in A^*. As an example, if $w = abab^2ca^2b^3$, then $N_a(w) = 4$ and $N_{ba}(w) = 7$. The numbers $N_{ac}(w)$ and $N_{cb}(w)$ are defined similarly.

The following relationship between these numbers is immediate.

Lemma 4.3. *For all words* $u, v \in A^*$,

$$N_{ab}(uv) = N_{ab}(u) + N_{ab}(v) + N_a(u)N_b(v).$$

Definition 4.4 (Directional-ordering)**.** Let α, β, and γ be any three positive real numbers. We will call these numbers *weights*. Corresponding to these weights we define a function $\textsc{wt}(w) = \alpha N_{ba}(w) + \beta N_{cb}(w) + \gamma N_{ac}(w)$, for each $w \in A^*$, where $N_{ba}(w)$, $N_{cb}(w)$, and $N_{ac}(w)$ are the 2-variable numbers for w.

Let $>_c$ be any total division ordering on the elements of $\mathbb{N}^3$, and let $>_{lex}$ be the lexicographic ordering induced by any total ordering of A. For any word $u \in A^*$, let $[u]$ denote the corresponding element of $\mathbb{N}^3$. For $u, v \in A^*$, define $u > v$ if

- $[u] >_c [v]$, or
- $[u] = [v]$ and $\textsc{wt}(u) > \textsc{wt}(v)$, or
- $[u] = [v]$, $\textsc{wt}(u) = \textsc{wt}(v)$, and $u >_{lex} v$.

where $[u]$ denotes the element of $\mathbb{N}^3$ that u represents. This ordering $>$ will be called the *directional-ordering* corresponding to α, β, γ, $>_c$, and $>_{lex}$.

Lemma 4.5. *For any positive real numbers α, β and γ, for any total division ordering $>_c$ on $\mathbb{N}^3$, and for any lexicographic ordering on A^*, the corresponding directional-ordering $>$ is a total division ordering on A^*.*

Proof. We start by showing that $>$ is well-founded. Suppose $w_1 > w_2 > \cdots$ is an infinite descending sequence. Since $>_c$ is well-founded, the element of $\mathbb{N}^3$ represented by w_i eventually stops changing as one proceeds through the w_i. At this point the remaining w_i lie in a single congruence class. Because this congruence class is finite, there are only a finite number of possible values for $\textsc{wt}(w_i)$, and this also eventually stops changing. Finally, for this finite set of words in a single congruence class with the same weight, $>_{lex}$ is a total order which eventually stops changing, giving a contradiction.

Next we show that $>$ is a division ordering. Suppose that u, v, w are words in A^* with $u > v$. The proof that $uw > vw$ will be in several cases depending on the reason why $u > v$. If $u > v$ because $[u] >_c [v]$, then $uw > vw$ because $>_c$ is a division ordering. Next, suppose $[u] = [v]$ and $\textsc{wt}(u) > \textsc{wt}(v)$. Since $[u] = [v]$ implies $[uw] = [vw]$ we only need to show $\textsc{wt}(uw) > \textsc{wt}(vw)$. Using the definition of the weight function and Lemma 4.3 we can write

$$\begin{aligned}
\textsc{wt}(uw) &= \alpha N_{ba}(uw) + \beta N_{cb}(uw) + \gamma N_{ac}(uw) \\
&= \quad \alpha(N_{ba}(u) + N_{ba}(w) + N_b(u)N_a(w)) \\
&\quad +\beta(N_{cb}(u) + N_{cb}(w) + N_c(u)N_b(w)) \\
&\quad +\gamma(N_{ac}(u) + N_{ac}(w) + N_a(u)N_c(w)) \\
&= \textsc{wt}(u) + \textsc{wt}(w) \\
&\quad +\alpha N_b(u)N_a(w) + \beta N_c(u)N_b(w) + \gamma N_a(u)N_c(w)
\end{aligned}$$

Similarly,

$$\begin{aligned}
\textsc{wt}(vw) &= \textsc{wt}(v) + \textsc{wt}(w) \\
&\quad +\alpha N_b(v)N_a(w) + \beta N_c(v)N_b(w) + \gamma N_a(v)N_c(w)
\end{aligned}$$

Since $[u] = [v]$, we know that $N_a(u) = N_a(v)$, $N_b(u) = N_b(v)$, and $N_c(u) = N_c(v)$. Thus the expansions of $\textsc{wt}(uw)$ and $\textsc{wt}(vw)$ differ only in their initial summands, and $\textsc{wt}(uw) > \textsc{wt}(vw)$. Lastly, if $[u] = [v]$, $\textsc{wt}(u) = \textsc{wt}(v)$ and $u >_{lex} v$, then $[uw] = [vw]$, the expansions above show that $\textsc{wt}(uw) = \textsc{wt}(vw)$, and $uw >_{lex} vw$ because $>_{lex}$ is a division ordering.

Finally, $>$ is a total ordering because $>_c$ is a total ordering on $\mathbb{N}^3$, any two weights can be compared and $>_{lex}$ is a total ordering on A^*. □

Lemma 4.6. *Let α, β and γ be positive real numbers, let $>_c$ be a total division ordering on $\mathbb{N}^3$, and let $>_{lex}$ be any lexicographic ordering of A^*. The corresponding directional-order $>$ determines a unique reduced complete rewriting system R for the commutator ideal which is independent of $>_c$.*

Proof. By Lemma 4.5 the directional-ordering $>$ is a total division ordering. Thus $>$ restricted to a congruence class has a unique minimum element, and, as described in Definition 1.4 there is a unique reduced complete rewriting system R for the commutator ideal with these minimum elements as normal forms. Since $>_c$ plays no role in the selection of the minimum element in a congruence class, R is independent of $>_c$. □

Lemma 4.7. *Let $>$ be a directional-ordering associated to positive real numbers α, β and γ and the lexicographic ordering $>_{lex}$, and let R be the corresponding reduced complete rewriting system. The octant coloring derived from R is equivalent to one in which the line defined by the equations $\frac{x}{\beta} = \frac{y}{\gamma} = \frac{z}{\alpha}$ is in the boundary of all three regions of color.*

Proof. Note that R contains the rules $ba \to ab$, $cb \to bc$, and $ac \to ca$ as a consequence of the definition of the weight function. Next, by Corollary 2.5, every irreducible word is of the form $a^i b^j c^k$, $b^j c^k a^i$ or $c^k a^i b^j$. Since $\mathrm{WT}(a^i b^j c^k) = \gamma ik$, $\mathrm{WT}(b^j c^k a^i) = \alpha ij$, and $\mathrm{WT}(c^k a^i b^j) = \beta jk$, the normal forms for R are

$$\begin{array}{ll} a^i b^j c^k & \text{when } \gamma ik \leq \alpha ij \text{ and } \gamma ik \leq \beta jk \\ b^j c^k a^i & \text{when } \alpha ij < \gamma ik \text{ and } \alpha ij \leq \beta jk \\ c^k a^i b^j & \text{when } \beta jk < \gamma ik \text{ and } \beta jk < \alpha ij \end{array}$$

Recall that the normal forms in this array correspond to blue, red and green, respectively. The coloring of the integer lattice associated to these normal forms can be extended to an octant coloring by coloring (x, y, z) blue if $\gamma z \leq \alpha y$ and $\gamma x \leq \beta y$, red if $\alpha y < \gamma z$ and $\alpha x \leq \beta z$, and green if $\beta y < \gamma x$ and $\beta z < \alpha x$. From these inequalities, it follows immediately that the line defined in the statement lies in the boundary of all three regions of color. □

Corollary 4.8. *Let $>_{lex}$ be a fixed lexicographic ordering of A^*. If R is the unique reduced complete rewriting system determined by $>_{lex}$ and the positive real numbers α, β, γ and R' is the unique reduced complete rewriting system determined by $>_{lex}$ and the positive real numbers α', β', γ', then R and R' are the same rewriting system if and only if the vectors (α, β, γ) and $(\alpha', \beta', \gamma')$ are parallel.*

Proof. If (α, β, γ) and $(\alpha', \beta', \gamma')$ are parallel (and the same lexicographic ordering is used for both directional-orderings) then the octant colorings described in Lemma 4.7 are identical. Since R and R' can be recovered from this coloring, R and R' are identical. On the other hand, if these vectors are not parallel then sufficiently far from the origin we can find lattice points which are assigned different colors, and thus R and R' are distinct. □

Theorem B. *There are uncountably many reduced complete rewriting systems for the m-generated free commutative monoid which are compatible with a total division ordering when $m \geq 3$. As a consequence there are uncountably many reduced noncommutative Gröbner bases with respect to total division orderings for the commutator ideal in the m-variable free associative algebra, each with a distinct set of normal forms.*

Proof. For $m = 3$ this result is immediate from Corollary 4.8. For $m > 3$, let $A = \{a_1, \ldots, a_m\}$ and let $a = a_1$, $b = a_2$, and $c = a_3$. Let $>$ be a directional-ordering on $\{a, b, c\}^*$ and define the rewriting system R consisting of all of the rules induced by $>$ together with the rules $a_j a_i \to a_i a_j$ for all $3 < j$ and $i < j$. It is straightforward to show that the total division ordering $>$ on $\{a, b, c\}^*$ can be extended to total division ordering on A^* so that R is the reduced complete rewriting system derived from this extension, and that the normal forms for R are normal forms derived from $>$ followed by $a_4^{r_4} \cdots a_m^{r_m}$. Since two rewriting systems constructed in this way will be identical if and only if their restrictions to $\{a,b,c\}^*$ are identical, Corollary 4.8 shows there are uncountably many reduced complete rewriting systems for A^* as well. $\square$

In our final result we use directional-orderings to construct the universal Gröbner basis for the commutator ideal in the free associative algebra $K\langle a,b,c\rangle$. We will need the following lemma which limits the set of rules that need to be considered.

Lemma 4.10. *If R is a reduced complete rewriting system for $\mathbb{N}^3$ which contains the rules $ba \to ab$, $cb \to bc$ and $ac \to ca$, then each of the remaining rules is of one of the following six forms with $i,j,k > 0$:*

$$\begin{array}{ll} ab^jc^k \to b^jc^ka & a^ib^jc \to ca^ib^j \\ b^jc^ka \to ab^jc^k & bc^ka^i \to c^ka^ib \\ ca^ib^j \to a^ib^jc & c^ka^ib \to bc^ka^i \end{array}$$

Proof. Let $u \to v$ be a rule in R different from the three specified in the hypothesis. Lemma 2.1 and the fact that R is reduced show that u and v must involve all three variables while Corollary 2.5 shows each of u and v must be in one of the forms $a^ib^jc^k$, $b^jc^ka^i$, or $c^ka^ib^j$ with $i,j,k > 0$. Suppose $u = a^ib^jc^k$ and $v = b^jc^ka^i$. If $i > 1$ then, since proper subwords of u and v are irreducible, ab^jc^k and b^jc^ka are irreducible words representing the same element of $\mathbb{N}^3$. This contradiction shows $i = 1$ when u and v have these forms. The other possibilities for u and v lead to similar conclusions. $\square$

Theorem C. *The universal Gröbner basis for the commutator ideal in the free associative algebra $K\langle a,b,c\rangle$ consists of the binomials*

$$\begin{array}{lll} ab - ba & bc - cb & ca - ac \\ ab^jc^k - b^jc^ka & bc^ka^i - c^ka^ib & ca^ib^j - a^ib^jc \\ ac^kb^j - c^kb^ja & ba^ic^k - a^ic^kb & cb^ja^i - b^ja^ic \end{array}$$

for all positive integers i, j, and k.

Proof. The finite reduced complete rewriting systems for $\mathbb{N}^3$ analyzed in Section 2 contain all six rules of the form $ab \leftrightarrow ba$, $ac \leftrightarrow ca$, and $bc \leftrightarrow cb$ and only these rules. Thus the corresponding binomials $ab - ba$, $ac - ca$, and $bc - cb$ are elements of the universal Gröbner basis.

Next, let R be an infinite reduced complete rewriting system in which ab, bc, and ca are normal forms. Lemma 4.10 severely restricts the form of the 3-variable rules in R, and we will now show that every rule listed in the lemma is, in fact, a rule in some infinite reduced complete rewriting system. Let j and k be positive integers. We first choose a real number α between $\frac{k-1}{j}$ and $\frac{k}{j}$, and then we choose a real number β greater than both $\frac{\alpha}{k}$ and $\frac{1}{j}$, and finally let $\gamma = 1$. Let R be the rewriting system corresponding to the directional-ordering $>$ derived from α, β, and γ and any choice of lexicographic ordering $>_{lex}$. With respect to R, the word b^jc^ka is irreducible and the word ab^jc^k is nearly irreducible (in particular, b^jc^k and ab^jc^{k-1} are irreducible). This shows that R contains the rule $ab^jc^k \to b^jc^ka$ and that the universal Gröbner basis contains the binomial $ab^jc^k - b^jc^ka$. The proof for the other rules listed in Lemma 4.10 is similar.

Finally, for infinite reduced complete rewriting systems in which ba, cb, and ac are normal forms, a relabeling of the variables reduces this to the previous case and produces the binomials listed in the third row of the array in the statement. Since every reduced complete rewriting system for this commutator ideal is either finite, contains ab, bc and ca as normal forms, or contains ba, cb and ac as normal forms, the proof is complete. □

Notice that this proof actually shows more. Since the restrictions on the possible rules in a reduced complete rewriting system R for the commutator ideal did not require R to be compatible with a total division ordering, but all of the examples proving such rules actually occur came from rewriting systems which were compatible with a total division ordering, the universal Gröbner basis for the commutator ideal of the 3-variable free associative algebra is same whether or not the Gröbner bases are required to be compatible with a total division ordering.

5. Open Question

In Section 3, we introduced a class of potential normal forms and showed that the rewriting systems associated to these sets are the only possible complete reduced rewriting systems for $\mathbb{N}^3$. Although we have shown that various special cases of these potential normal forms actually do give rise to reduced complete rewriting systems, the rest remain merely potential.

Problem 5.1. If $\mathcal{F}$ is a potential set of normal forms for $\mathbb{N}^3$, does $\mathcal{F}$ give rise to a rewriting system R which is reduced, complete, and compatible with a (total) division ordering? In other words, is $\mathcal{F}$ the set of minimal representatives with respect to some (total) division ordering?

The problem is proving that the rewriting system derived from $\mathcal{F}$ must terminate. For some of these open cases we have run tests, using the rewriting software Herky (RRL) [7], and in each case the software has failed to find a potential infinite chain of rewritings.

References

[1] David J. Anick. On the homology of associative algebras. *Trans. Amer. Math. Soc.*, 296(2):641–659, 1986.

[2] Volker Diekert. Commutative monoids have complete presentations by free (noncommutative) monoids. *Theoret. Comput. Sci.*, 46(2-3):319–327, 1986.

[3] David Eisenbud, Irena Peeva, and Bernd Sturmfels. Non-commutative Gröbner bases for commutative algebras. *Proc. Amer. Math. Soc.*, 126(3):687–691, 1998.

[4] C. Eschenbach. Die verwendung von zeichenkettenordnungen im zusammenhang mit semi-thue systemen. Tech. Report FBI - HH - B - 122/86, Fachbereich Informatik, Universität Hamburg, 1986.

[5] Ed Green, Teo Mora, and Victor Ufnarovski. The non-commutative Gröbner freaks. In *Symbolic rewriting techniques (Ascona, 1995)*, pages 93–104. Birkhäuser, Basel, 1998.

[6] Susan M. Hermiller, Xenia H. Kramer, and Reinhard C. Laubenbacher. Monomial orderings, rewriting systems, and Gröbner bases for the commutator ideal of a free algebra. *J. Symbolic Comput.*, 27(2):133–141, 1999.

[7] D. Kapur and H. Zhang. An overview of rewrite rule laboratory (RRL). *Comput. Math. Appl.*, 29(2):91–114, 1995.

[8] Klaus Madlener and Birgit Reinert. Relating rewriting techniques on monoids and rings: congruences on monoids and ideals in monoid rings. *Theoret. Comput. Sci.*, 208(1-2):3–31, 1998. Rewriting techniques and applications (New Brunswick, NJ, 1996).

[9] U. Martin. Private communication.

[10] Ursula Martin. On the diversity of orderings on strings. *Fund. Inform.*, 24(1-2):25–46, 1995.

[11] Teo Mora. An introduction to commutative and noncommutative Gröbner bases. *Theoret. Comput. Sci.*, 134(1):131–173, 1994. Second International Colloquium on Words, Languages and Combinatorics (Kyoto, 1992).

[12] Irena Peeva, Victor Reiner, and Bernd Sturmfels. How to shell a monoid. *Math. Ann.*, 310(2):379–393, 1998.

[13] Samuel M. H. W. Perlo-Freeman and Péter Pröhle. Scott's conjecture is true, position sensitive weights. In *Rewriting techniques and applications (Sitges, 1997)*, volume 1232 of *Lecture Notes in Comput. Sci.*, pages 217–227. Springer, Berlin, 1997.

[14] Wayne B. Powell. Total orders on free groups and monoids. In *Words, languages and combinatorics (Kyoto, 1990)*, pages 427–434. World Sci. Publishing, River Edge, NJ, 1992.

[15] T. Saito, M. Katsura, Y. Kobayashi, and K. Kajitori. On totally ordered free monoids. In *Words, languages and combinatorics (Kyoto, 1990)*, pages 454–479. World Sci. Publishing, River Edge, NJ, 1992.

[16] Charles C. Sims. *Computation with finitely presented groups*. Cambridge University Press, Cambridge, 1994.

Dept. of Math., University of Nebraska, Lincoln, NE 68588-0130
E-mail address: `smh@math.unl.edu`

Dept. of Math., U. C. Santa Barbara, Santa Barbara, CA 93106
E-mail address: `jon.mccammond@math.ucsb.edu`