

One-sided Noncommutative Gröbner Bases with Applications to Computing Green's Relations *

Anne Heyworth [†]
 School of Mathematics
 University of Wales, Bangor
 Gwynedd LL57 1UT
 United Kingdom
 map130@bangor.ac.uk

June 11, 2005

Abstract

Standard noncommutative Gröbner basis procedures are used for computing ideals of free noncommutative polynomial rings over fields. This paper describes Gröbner basis procedures for one-sided ideals in finitely presented noncommutative algebras over fields. The polynomials defining a K -algebra A as a quotient of a free K -algebra are combined with the polynomials defining a one-sided ideal I of A , by using a tagging notation. Standard noncommutative Gröbner basis techniques can then be applied to the mixed set of polynomials, thus calculating A/I whilst working in a free structure, avoiding the complication of computing in A . The paper concludes by showing how the results can be applied to completable presentations of semigroups and so enable calculations of Green's relations.

1 Introduction

In 1965 Buchberger invented Gröbner basis theory, techniques enabling the computation of ideals in commutative polynomial rings over fields. Implementations of Buchberger's algorithm are now provided by all major computer algebra systems, a good cross-section of the ways in which the theory has developed may be found in [2]. Mora generalised Gröbner basis theory to noncommutative polynomial rings (algebras) [9]. Introductions to these procedures may be found in [14, 11]. This paper presents an extension of the noncommutative Gröbner basis procedures for polynomials to what we call *tagged polynomials*. The intention is to describe methods of computation that may be applied to the problem of computing right (or left) ideals in finitely presented K -algebras.

*KEYWORDS: Gröbner bases, semigroups, right ideals, left ideals.

AMS 1991 CLASSIFICATION: 16-04 16D15

[†]Supported 1995-8 by an EPSRC Earmarked Research Studentship, 'Identities among relations for monoids and categories', and 1998-9 by a University of Wales, Bangor, Research Assistantship.

The data defining the problem consists of the field K , a set of noncommuting variables X , a set of generators $P \subseteq K[X^\dagger]$ for a two-sided ideal $\langle P \rangle$, defining an algebra $A = K[X^\dagger]/\langle P \rangle$ and a set of generators $Q' \subseteq A$ for a right ideal $\langle Q' \rangle^r$. We expect elements of A to be given in terms of $K[X^\dagger]$, so Q' is specified by a set $Q \subseteq K[X^\dagger]$. The problem we address is that of computing the right A -ideal generated by Q' , written $\langle Q' \rangle^r$.

Our solution lies in using the free right K -module $K[\dashv X^\dagger]$. Here \dashv is just a symbol or tag and $K[\dashv X^\dagger]$ is bijective with $K[X^\dagger]$. We call elements of $K[\dashv X^\dagger]$ *tagged polynomials* (Definition 3.1) and write them $k_1 \dashv m_1 + \dots + k_n \dashv m_n$ where $k_1, \dots, k_n \in K$ and $m_1, \dots, m_n \in X^\dagger$. Ordinary polynomials F_P defining the two-sided ideal $\langle P \rangle$ which defines A are combined with tagged polynomials F_T defining the one-sided ideal. The mixed set of polynomials $F := (F_T, F_P)$ determines a reduction relation \rightarrow_F (Definition 3.2) on the tagged polynomials $K[\dashv X^\dagger]$.

The value of this combination and use of tagging is in computation, as will be shown in the main result (Algorithm 4.9), which describes a variant of the Buchberger algorithm. The initial mixed set of polynomials F is appended with tagged and non-tagged polynomials until the relation \rightarrow_F is complete on $K[\dashv X^\dagger]$. When the procedure terminates the usual normal form arguments apply and reduction modulo F can be used to solve the membership problem for the right ideal $\langle Q' \rangle^r$ of the finitely presented algebra A .

Previous work [12, 13] attempt the computation of one-sided ideals by using different definitions of purely one-sided reduction relation in particular algebras (e.g. $\mathbb{Q}[M]$ for a monoid M presented by a complete rewrite system). The main problem encountered is that of computing in a non-free algebra, we avoid this and base all the computations specifying the algebra at the same level (in a particular free right module) as those for the ideal and compute the two simultaneously. In other words, the methods we describe provide for local computations, concerning single ideals $\langle Q' \rangle^r$ without the requirement to compute the global structure of the algebra A or face the difficulties of calculations with elements of A . This idea follows the philosophy that computations take place in free objects.

2 Algebra Presentations and One-sided Ideals

If X is a set, then X^\dagger is the *free semigroup* of all strings of elements of X , and X^* is the *free monoid* of all strings together with the empty string, which acts as the identity *id* for X^* . A *semigroup presentation* is a pair $\text{sgp}\langle X|R \rangle$ where X is a set and $R \subseteq X^\dagger \times X^\dagger$. It *presents a semigroup* S if X is a set of generators of S and the natural morphism $\theta : X^\dagger \rightarrow S$ induces an isomorphism from $X^\dagger / =_R$ to S , where $=_R$ is the congruence generated on X^\dagger by R . Similarly, a *monoid presentation* is a pair $\text{mon}\langle X|R \rangle$ where X is a set and $R \subseteq X^* \times X^*$. It *presents a monoid* M if X is a set of generators of M and the natural morphism $\theta : X^* \rightarrow M$ induces an isomorphism from $X^* / =_R$ to M , where $=_R$ is the congruence generated on X^* by R .

Let K be a field. The *free K -algebra* $K[S]$ on a semigroup S consists of all sums of K -multiples of elements of S with the operations of addition and multiplication defined in the obvious way. In particular the elements of $K[X^\dagger]$ are called *polynomials* and written $k_1 m_1 + \dots + k_n m_n$ where $k_1, \dots, k_n \in K$

and $m_1, \dots, m_n \in X^\dagger$.

If P is a subset of an algebra Z then the *two-sided ideal* generated by P in Z is denoted $\langle P \rangle$. In the case $Z = K[X^\dagger]$ this consists of all sums of multiples of elements of P , i.e.

$$\langle P \rangle := \{k_1 u_1 p_1 v_1 + \dots + k_n u_n p_n v_n \mid p_1, \dots, p_n \in P, k_1, \dots, k_n \in K, u_1, v_1, \dots, u_n, v_n \in X^*\}.$$

Given an ideal in an algebra the *membership problem* is that of determining, for a given element of the algebra, whether it is an element of the ideal.

A *congruence* on an algebra Z is an equivalence relation \sim on its elements such that if $p \sim q$ then $p + u \sim q + u$ and $upv \sim uqv$ for all $u, v \in Z$. Given an algebra Z and an ideal $\langle P \rangle$ ideal membership defines a congruence on the algebra by

$$p \sim q \Leftrightarrow p - q \in \langle P \rangle.$$

The *quotient algebra* $Z/\langle P \rangle$ is the algebra of congruence classes of Z under $\langle P \rangle$. A *K-algebra presentation* is a pair $\text{alg}\langle X|P \rangle$, where $P \subseteq K[X^\dagger]$. A *K-algebra* A is presented by $\text{alg}\langle X|P \rangle$ if X is a set of generators of A and the natural morphism $K[X^\dagger] \rightarrow A$ induces an isomorphism $K[X^\dagger]/\langle P \rangle \rightarrow A$.

Noncommutative Gröbner basis theory (as described in [10, 11]) uses the notion of an ordering on X^\dagger , thereby allowing the concepts of *leading monomial*, *leading term* and *leading coefficient* on the polynomials of $K[X^\dagger]$. Given any subset P of $K[X^\dagger]$ an ordering determines a Noetherian reduction relation \rightarrow_P on the elements of $K[X^\dagger]$. The reflexive, symmetric, transitive closure of this relation is a congruence relation coinciding with the ideal membership of $\langle P \rangle$.

Let A be the *K-algebra* presented by $\text{alg}\langle X|P \rangle$ and let $Q' \subseteq A$. We wish to consider the right ideal $\langle Q' \rangle^r$ generated in A by Q' , i.e.

$$\langle Q' \rangle^r := \{q'_1 a_1 + \dots + q'_n a_n \mid a_1, \dots, a_n \in A, q'_1, \dots, q'_n \in Q'\}.$$

A *right congruence* on an algebra A is an equivalence relation $\overset{r}{\sim}$ such that for all $a, b, y \in A$

$$a \overset{r}{\sim} b \Rightarrow a + y \overset{r}{\sim} b + y \text{ and } ay \overset{r}{\sim} by.$$

Membership of a right ideal $\langle Q' \rangle^r$ defines a right congruence on A , by $a \overset{r}{\sim}_{Q'} b \Leftrightarrow a - b \in \langle Q' \rangle^r$. The quotient $A/\langle Q' \rangle^r$ is the set of all the right congruence classes of A under $\overset{r}{\sim}_{Q'}$ where classes are denoted $[a]_{Q'}$ for $a \in A$. Note that for $a, b \in A$, $[a + b]_{Q'} = [a]_{Q'} + [b]_{Q'}$ and $[a]_{Q'}[b]_{Q'} = [a]_{Q'}$.

Buchberger's algorithm is a critical pair completion procedure. The algorithm begins with a set of polynomials P of a free algebra. Set $F := P$ and a search for overlapping leading terms will find all critical terms of the reduction relation \rightarrow_F . This enables a test for local confluence. Overlaps which cannot be resolved result in *S-polynomials* all of which are added to F at each stage (though some elimination is possible, for efficiency). The algorithm terminates when all the overlaps of F can be resolved, i.e. \rightarrow_F is complete (Noetherian and confluent), when this occurs F is said to be a *Gröbner basis* for the ideal $\langle P \rangle$. Obtaining a Gröbner basis F allows, in particular, the solution of

the membership problem by using \rightarrow_F as a normal form function on $K[X^\dagger]$. Thus, if F is a Gröbner basis for the ideal $\langle P \rangle$ on $K[X^\dagger]$ and $p, q \in K[X^\dagger]$, then

$$p \sim q \Leftrightarrow p - q \in \langle P \rangle \Leftrightarrow p \xrightarrow{*}_F u \text{ and } q \xrightarrow{*}_F u \text{ for some } u \in K[X^\dagger].$$

The Noetherian property ensures that the process of reduction terminates with an irreducible element; confluence ensures that any two elements of the same class reduce to the same form. In practice: reduce each polynomial as far as possible using \rightarrow_F , the original polynomials are equivalent only if their irreducible forms are equal.

In the next sections we show how to apply Buchberger's algorithm to obtain – when possible – a Gröbner basis of (two types of) polynomials, which will enable the use of normal forms arguments.

3 One-sided Noncommutative Gröbner Basis Procedures

Given a finitely presented K -algebra A and a subset Q' of A we wish to compute the right ideal $\langle Q' \rangle^r$. The meaning of ‘computing the ideal’ in this context is that of solving the ideal membership problem for $\langle Q' \rangle^r$ in A . The K -algebra A is presented by $\text{alg}\langle X|P \rangle$ and to obtain normal forms for A we would therefore apply Gröbner basis procedures to P in the free algebra $K[X^\dagger]$. Since we are interested in a one-sided ideal we introduce the tagging notation which will allow the combination of P and Q .

Definition 3.1 (Tagged polynomials) *Let K be a field, let X be a set and let \dashv be a symbol. Then $\dashv X^\dagger$ is the set of **tagged terms** $\dashv m$ where $m \in X^\dagger$ and $K[\dashv X^\dagger]$ is the free right $K[X^\dagger]$ -module of **tagged polynomials**, i.e. elements $k_1 t_1 + \dots + k_n t_n$ for $k_1, \dots, k_n \in K$, $t_1, \dots, t_n \in \dashv X^\dagger$.*

Let $>$ be a *semigroup ordering* on X^\dagger , i.e. $>$ is an irreflexive, antisymmetric, transitive relation on X^\dagger such that if $m_1 > m_2$ then $um_1v > um_2v$ for all $u, v \in X^*$. Further we require the *well-ordering* property, that there is no infinite sequence $m_1 > m_2 > m_3 > \dots$.

Let $p = k_1 m_1 + \dots + k_n m_n \in K[X^\dagger]$. The $k_i m_i$ are referred to as the *monomials* of the polynomial, where m_i is the *term* and k_i the *coefficient*. Assuming the well-ordering on X^\dagger , the leading monomial $\text{LM}(p)$ is defined to be the monomial with the largest term. The leading term $\text{LT}(p)$ and leading coefficient $\text{LC}(p)$ are the coefficient and term of this monomial.

To simplify the definitions throughout this paper we will assume all polynomials to be *monic*, i.e. their leading coefficients are all 1. There is no loss in doing this: K is a field so the polynomials F may always be divided by their leading coefficients and still generate the same ideal.

The well-ordering on X^\dagger induces a well-ordering on $\dashv X^\dagger$ defined by $\dashv m_1 > \dashv m_2 \Leftrightarrow m_1 > m_2$. This gives corresponding notions of leading monomial, leading term and leading coefficient for the tagged polynomials. In detail: if $p = k_1 m_1 + \dots + k_n m_n$ where $k_1, \dots, k_n \in K$ and $m_1, \dots, m_n \in X^\dagger$ is a polynomial with leading term $\text{LT}(p) = m_i$ then the tagged polynomial $\dashv p := k_1 \dashv m_1 + \dots + k_n \dashv m_n$ has a tagged leading term $\text{LT}(\dashv p) = \dashv m_i$.

We will now introduce the definition of a reduction relation on $K[\dashv X^\dagger]$, defined by a mixed set of polynomials $F = (F_T, F_P)$ where F_T is a set of tagged polynomials, elements of the module, and F_P is a set of polynomials, elements of the algebra acting on the right of the module. The reduction relation \rightarrow_F combines the two relations so that they are defined on the free right module of tagged polynomials.

Definition 3.2 (Reduction of tagged polynomials) Let $F := (F_T, F_P)$ where $F_T \subseteq K[\dashv X^\dagger]$ and $F_P \subseteq K[X^\dagger]$. Define the reduction relation \rightarrow_F on tagged polynomials $f \in K[\dashv X^\dagger]$ by

$$f \rightarrow_F f - ku(f_i)v$$

if $u\text{LT}(f_i)v$ occurs in f with coefficient $k \in K$ for some $u \in \dashv X^* \cup \{id\}$, $v \in X^*$, $f_i \in F$.

A one-step reduction like that of the definition may also be written $f \rightarrow_{f_i} f - ku(f_i)v$. This relation may be understood to be a rewrite system on the polynomials (similarly to observations made in [12] on Mora's definitions of reduction [9]). When a multiple of the leading term of f_i for $f_i \in F$ occurs in the polynomial that is to be reduced, the rest of f_i is substituted for the leading monomial of f_i . Regarding F as a rewrite system with two types of rules that may be applied to monomials of polynomials, we could say that the non-tagged polynomials can be applied anywhere in a term, but the tagged ones apply only at the tagged side of a term.

Example 3.3 (Reduction) For example let $F_T := \{f_1, f_2\}$ where $f_1 := \dashv xyx + \dashv yx + 2 \dashv y$, $f_2 := \dashv yx^2 + \dashv x^2$ and $F_P := \{f_3, f_4\}$ where $f_3 := x^2y - 3yx$, $f_4 := yx^3 - 2xy$. Then the tagged polynomial $f := 8 \dashv xyx^2y^3 + 5 \dashv y$ cannot be reduced by f_2 or f_4 but can be reduced by f_1 to $f - 8f_1xy^3 = 5 \dashv y - 8 \dashv yx^2y^3 - 16 \dashv yxy^3$ or by f_3 to $f - 8 \dashv xyf_3y^2 = 5 \dashv y + 24 \dashv xy^2xy^2$.

These results allow the combination of two-sided and one-sided congruences, by the use of tagged polynomials. A mixed set of polynomials F defines a reduction relation on the module of all tagged polynomials. The reflexive, symmetric, transitive closure of \rightarrow_F will be denoted $\overset{*}{\leftrightarrow}_F$. The class of $f \in K[\dashv X^\dagger]$ under the equivalence relation $\overset{*}{\leftrightarrow}_F$ will be denoted $[f]_F$.

Theorem 3.4 Let A be a K -algebra finitely presented by $\text{alg}\langle X|P \rangle$ with quotient morphism θ . Let $Q \subseteq K[X^\dagger]$ and define $Q' := \theta Q$. Define $F := (\dashv Q, P)$ where $\dashv Q := \{\dashv q : q \in Q\}$. Then there is a bijection of sets

$$\frac{K[\dashv X^\dagger]}{\overset{*}{\leftrightarrow}_F} \cong \frac{A}{\langle Q' \rangle^r}$$

Proof The quotient morphism $\theta : K[X^\dagger] \rightarrow A$, defines a surjection $\theta^\dagger : K[\dashv X^\dagger] \rightarrow A$. Then $\theta^\dagger(\dashv Q) = Q'$.

Define $\phi : K[\dashv X^\dagger] / \overset{*}{\leftrightarrow}_F \rightarrow A / \langle Q' \rangle^r$ by $\phi([f]_F) := [\theta^\dagger(f)]_{Q'}$.

To prove that ϕ is well-defined we show that it preserves the right congruence $\overset{*}{\leftrightarrow}_F$. We assume all polynomials of F are monic. Let $f \in K[\dashv X^\dagger]$ and $f_i \in F$ and suppose that $f \rightarrow_F f - kuf_iv$ for some $k \in K$, $u \in \dashv X^* \cup \{id\}$, $v \in X^*$. By definition $\phi([f - kuf_iv]_F) = [\theta^\dagger(f) - \theta^\dagger(kuf_iv)]_{Q'}$.

Now either

(i) $f_i \in P \subseteq K[X^\dagger]$ and $\theta^{-1}(kuf_i v) = 0$, since $kuf_i v \in \langle P \rangle$,

or else

(ii) $f_i \in \neg Q \subseteq K[\neg X^\dagger]$ and $u = id$, so $\theta^{-1}(kuf_i v) = k\theta^{-1}(f_i v)$.

In either case $\theta^{-1}(kuf_i v) \in \langle Q' \rangle^r$, so $\phi([f]_F) = \phi([f - kuf_i v]_F)$, i.e. ϕ preserves the relation \rightarrow_F .

Furthermore if $[f]_F = [g]_F$ for some $f, g \in K[\neg X^\dagger]$, then for all $v \in X^*$,

$$\begin{aligned} \phi([fv]_F) &= [\theta^{-1}(fv)]_{Q'} \\ &= [\theta^{-1}(f)]_{Q'} \theta(v) \\ &= [\theta^{-1}(g)]_{Q'} \theta(v) \\ &= [\theta^{-1}(gv)]_{Q'} \\ &= \phi([gv]_F). \end{aligned}$$

Therefore ϕ preserves the right congruence \leftrightarrow_F^* .

We now prove that ϕ is surjective. Let $a \in A$. Then there exists $f \in K[\neg X^\dagger]$ such that $\theta^{-1}(f) = a$, because θ^{-1} is a surjection. Thus for all $[a]_{Q'} \in A/\langle Q' \rangle^r$ there exists $[f]_F \in K[\neg X^\dagger]/\leftrightarrow_F^*$ such that $\phi([f]_F) = [\theta^{-1}f]_{Q'} = [a]_{Q'}$.

Finally, we prove that ϕ is injective. Let $f, g \in K[\neg X^\dagger]$ such that $\phi([f]_F) = \phi([g]_F)$. Then $[\theta^{-1}(f)]_{Q'} = [\theta^{-1}(g)]_{Q'}$. Therefore there exist $q'_1, \dots, q'_n \in Q'$ and $k_1, \dots, k_n \in K$, $a_1, \dots, a_n \in A$, such that

$$\theta^{-1}(f) - \theta^{-1}(g) = k_1 q'_1 a_1 + \dots + k_n q'_n a_n.$$

For $i = 1, \dots, n$ there exists $q_i \in Q$, $y_i \in X^*$ such that $\theta^{-1}(q_i y_i) = q'_i a_i$. Hence

$$\theta^{-1}(f) - \theta^{-1}(g) = k_1 q_1 y_1 + \dots + k_n q_n y_n.$$

Now θ^{-1} preserves $+$ and therefore $\theta^{-1}(f - g - k_1 q_1 y_1 - \dots - k_n q_n y_n) = 0$. By the definition of θ , and so θ^{-1} , therefore

$$f - g - k_1 q_1 y_1 - \dots - k_n q_n y_n = l_1 u_1 p_1 v_1 + \dots + l_m u_m p_m v_m$$

for some $p_1, \dots, p_m \in P$, $l_1, \dots, l_m \in K$ and $u_1, \dots, u_m \in \neg X^* \cup \{id\}$, $v_1, \dots, v_m \in X^*$. Therefore $f \leftrightarrow_F^* g$, from the definition. Therefore ϕ is a well-defined bijection of sets. \square

Corollary 3.5 *Let S be a semigroup with presentation $sgp\langle X|R \rangle$. Let $P := \{l - r : (l, r) \in R\}$, $Q \subseteq K[X^\dagger]$. Define $F := (P, \neg Q)$. Then there is a bijection of sets*

$$\frac{K[S]}{\langle Q' \rangle^r} \cong \frac{K[\neg X^\dagger]}{\leftrightarrow_F^*}$$

Here it is appropriate to observe the link to rewrite systems which is used in the proof of this corollary, in particular, $alg\langle X|P \rangle$ is a presentation of $K[S]$ [10, 12, 5]. This corollary (also see the next result) provides an alternative approach to that of Reinert and Zecker [13] for attempting the computation of ideals in $\mathbb{Q}[M]$, where M is a monoid. Our computations are based in $\mathbb{Q}[X^*]$ where X is a set of generators for M , the computations of Reinert and Zecker are made within $\mathbb{Q}[M]$, (also using a presentation of M).

Theorem 3.6 Let X be a set of generators for the terms of a K -algebra A and let $P \subseteq K[X^*]$ such that the natural morphism $\theta : K[X^*] \rightarrow A$ induces an isomorphism $K[X^*]/\langle P \rangle \rightarrow A$. Let $Q \subseteq K[X^*]$ and define $Q' := \theta Q$. Define $F := (\neg Q, P)$ where $\neg Q := \{\neg q : q \in Q\}$. Then there is a bijection of sets

$$\frac{K[\neg X^*]}{\xrightarrow{*}_F} \cong \frac{A}{\langle Q' \rangle^r}$$

Proof Define $\phi : K[\neg X^*]/\xrightarrow{*}_F \rightarrow A/\langle Q' \rangle^r$ by $\phi([f]_F) := [\theta^{-1}(f)]_{Q'}$. The verification that ϕ is a well-defined bijection on the congruence classes is similar to that detailed in the proof of Theorem 3.4. \square

4 The Noncommutative Buchberger Algorithm for One-sided Ideals

Recall that $F = (F_T, F_P)$ is a mixed set of polynomials $F_T \subseteq K[\neg X^\dagger]$ and $F_P \subseteq K[X^\dagger]$. The definition of reduction of a tagged polynomial f requires that a tagged term $\neg m$ of f is some multiple of a leading term from the polynomials f_i of F . This definition of reduction will allow the application of the standard noncommutative Buchberger algorithm to F to attempt to complete \rightarrow_F .

Definition 4.1 (Gröbner basis of mixed polynomials) A set $F = (F_T, F_P)$ where $F_T \subseteq K[\neg X^\dagger]$ and $F_P \subseteq K[X^\dagger]$ is a **Gröbner basis** on $K[\neg X^\dagger]$ with respect to $>$ if \rightarrow_F is complete.

Lemma 4.2 (Noetherian property) Let $F = (F_T, F_P)$ where $F_T \subseteq K[\neg X^\dagger]$ and $F_P \subseteq K[X^\dagger]$. Let $>$ be a semigroup well-ordering on X^\dagger . Then the reduction relation \rightarrow_F is Noetherian on $K[\neg X^\dagger]$.

Proof According to the definition, the process of reduction replaces one monomial with monomials which are smaller with respect to $>$ (since $>$ is a term order on X^\dagger). The existence of an infinite sequence of reductions $f_1 \rightarrow_F f_2 \rightarrow_F \dots$ of polynomials $f_1, f_2, \dots \in K[\neg X^\dagger]$ would imply the existence of an infinite sequence $m_1 > m_2 > \dots$ of terms $m_1, m_2, \dots \in X^\dagger$. Therefore \rightarrow_F is Noetherian. \square

Definition 4.3 (Matches and S-polynomials of tagged and non-tagged polynomials)

Let $F = (F_T, F_P)$ where $F_T \subseteq K[\neg X^\dagger]$ and $F_P \subseteq K[X^\dagger]$. A pair of polynomials $f_1, f_2 \in F$ has a **match** if their leading terms m_1, m_2 coincide. If a pair of polynomials have a match then an **S-polynomial** is defined. There are five possible cases:

	match	S-polynomial	
both f_1 and f_2 in F_T	(i) $m_1 v = m_2$	$f_1 v - f_2$	where $v \in X^*$
f_1 in F_T and f_2 in F_P	(ii) $m_1 v = u m_2$	$f_1 v - u f_2$	where $u \in \neg X^* \cup \{id\}, v \in X^*$
	(iii) $m_1 = u m_2 v$	$f_1 - u f_2 v$	
both f_1 and f_2 in F_P	(iv) $u m_1 = m_2 v$	$f_1 v - u f_2$	where $u, v \in X^*$
	(v) $m_1 = u m_2 v$	$f_1 - u f_2 v$	

A match is said to **resolve** if the resulting S-polynomial can be reduced to zero by F .

Remark 4.4 If a match of any of the types above occurs between f_1 and f_2 then the match may be represented: $u_1m_1v_1 = u_2m_2v_2$, where $u_1, u_2, v_1, v_2 \in \neg X^* \cup X^*$. A match of f_1 and f_2 may occur when either, neither, or both of f_1 and f_2 are tagged. However, if one or both has a tag, the tag forms part of the match and the resulting S-polynomial will be tagged.

The following lemma is proved in the same way as in the standard commutative non-tagged situation as described in [1].

Lemma 4.5 *Let $F = (F_T, F_P)$ where $F_T \subseteq K[\neg X^\dagger]$ and $F_P \subseteq K[X^\dagger]$. Let $g_1, g_2 \in K[\neg X^\dagger]$ where $g_1 - g_2 \xrightarrow*_F 0$. Then there exists a tagged polynomial $h \in K[\neg X^\dagger]$ such that $g_1 \xrightarrow*_F h$ and $g_2 \xrightarrow*_F h$.*

Proof The *length* of a reduction sequence is defined to be the number of one-step reductions of which it is made up. This proof is by induction on the length of the reduction sequence $g_1 - g_2 \xrightarrow*_F 0$.

For the basis of induction suppose the length of the reduction sequence is zero. Then $g_1 - g_2 = 0$ so $g_1 = g_2$.

For the induction step, assume that if $g'_1 - g'_2 \xrightarrow*_F 0$ is a reduction sequence of length n then there exists $h \in K[\neg X^\dagger]$ such that $g'_1 \xrightarrow*_F h$ and $g'_2 \xrightarrow*_F h$.

Suppose $g_1 - g_2 \xrightarrow{f_i} g \xrightarrow*_F 0$ where $g \xrightarrow*_F 0$ is a reduction sequence of length n .

Let $t \in \neg X^\dagger$ be the tagged term in $g_1 - g_2$ to which the reduction by f_i is applied. Let $u \in \neg X^* \cup \{id\}$, $v \in X^*$ such that $t = u\text{LT}(f_i)v$, and let k_1, k_2 be the coefficients of t in g_1, g_2 respectively. Now $k_1 - k_2 \neq 0$ since it is the coefficient of t in $g_1 - g_2$.

Depending on whether k_1 and k_2 are zero or not we have the following zero- or one-step reductions:

$$g_1 \xrightarrow{f_i} g_1 - k_1 u f_i v, \quad g_2 \xrightarrow{f_i} g_2 - k_2 u f_i v.$$

Since $g = (g_1 - k_1 u f_i v) - (g_2 - k_2 u f_i v)$ and $g \xrightarrow*_F 0$ in n steps, by the induction hypothesis there exists $h \in K[\neg X^\dagger]$ such that $g_1 - k_1 u f_i v \xrightarrow*_F h$ and $g_2 - k_2 u f_i v \xrightarrow*_F h$. Hence $g_1 \xrightarrow*_F h$ and $g_2 \xrightarrow*_F h$. \square

Theorem 4.6 (Test for confluence) *The reduction relation \rightarrow_F generated by F is complete on $K[\neg X^\dagger]$ if and only if all matches of F resolve.*

Proof In Lemma 4.2 we proved that \rightarrow_F is Noetherian and therefore, by Newman's Lemma for reduction relations on sets, we need only to prove that \rightarrow_F is locally confluent.

Let $f, g_1, g_2 \in K[\neg X^\dagger]$ such that $f \rightarrow_F g_1$ and $f \rightarrow_F g_2$. Then $g_1 = f - k_1 u_1 f_1 v_1$ and $g_2 = f - k_2 u_2 f_2 v_2$ for some $f_1, f_2 \in F$, $k_1, k_2 \in K$, $u_1, u_2, v_1, v_2 \in \neg X^* \cup X^*$. Let $m_1 := \text{LT}(f_1)$ and $m_2 := \text{LT}(f_2)$.

If the reductions do not overlap on f , i.e. $u_1 m_1 v_1 \neq u_2 m_2 v_2$ then it is immediate that $g_1 \rightarrow_F h$ and $g_2 \rightarrow_F h$ where $h = f - k_1 u_1 f_1 v_1 - k_2 u_2 f_2 v_2$.

Otherwise $u_1m_1v_1 = u_2m_2v_2$. In this case m_1 and m_2 may or may not coincide.

If they do not coincide, i.e. if there exists $w \in X^*$ such that $u_1m_1v_1 = u_1m_1wm_2v_2$ or $u_1m_1v_1 = u_2m_2wm_1v_1$ then again $g_1 \xrightarrow{*}_F h$ and $g_2 \xrightarrow{*}_F h$ where $h = f - u_1f_1wm_2v_2 - u_1m_1wf_2v_2$ or $h = f - u_2m_2wf_1v_1 - u_2f_2wm_1v_1$ respectively.

If the leading terms m_1 and m_2 do coincide then $u_1m_1v_1 = u_2m_2v_2$ represents a multiple of a match between f_1 and f_2 , i.e. there exist $u'_1, u'_2, v'_1, v'_2, w, z \in \neg X^* \cup X^*$, such that $u_1 = wu'_1$, $v_1 = v'_1z$, $u_2 = wu'_2$, $v_2 = v'_2z$ and $u'_1m_1v'_1 = u'_2m_2v'_2$ represents a match between f_1 and f_2 . In this case $u'_1f_1v'_1 - u'_2f_2v'_2 \xrightarrow{*}_F 0$ by assumption, and therefore $wu'_1f_1v'_1z - wu'_2f_2v'_2z = u_1m_1v_1 - u_2m_2v_2 \xrightarrow{*}_F 0$. By Lemma 4.5 this implies that there exists $h \in K[\neg X^\dagger]$ such that $g_1 \xrightarrow{*}_F h$ and $g_2 \xrightarrow{*}_F h$.

The converse of the above is easily checked. Suppose that \rightarrow_F is confluent. Then any S-polynomial arising from a match between polynomials is the result of reducing one term in two different ways, i.e. $f \rightarrow_F g_1$ and $f \rightarrow_F g_2$ for some $f, g_1, g_2 \in K[X^\dagger]$. The S-polynomial is equal to $g_1 - g_2$. The relation \rightarrow_F is locally confluent and so there exists $h \in K[\neg X^\dagger]$ such that $g_1 \rightarrow_F h$ and $g_2 \rightarrow_F h$. Therefore $g_1 - g_2 \xrightarrow{*}_F h - h = 0$ as required. \square

We may now apply the noncommutative version of Buchberger's algorithm (as described in [11]) to attempt to complete a mixed set of tagged and non-tagged polynomials. To verify steps 4 and 5 of the algorithm we observe the following two technical lemmas.

Lemma 4.7 (Addition of S-polynomials) *Let $F = (F_T, F_P)$. If f is an S-polynomial resulting from a match of F , then the congruences $\xrightarrow{*}_F$ and $\xrightarrow{*}_{F \cup \{f\}}$ coincide.*

Proof The result is proved by showing that, in each of the five cases, an S-polynomial f resulting from a match of polynomials $f_1, f_2 \in F$ can be written in the form $u_1f_1v_1 - u_2f_2v_2$ and therefore $f \xrightarrow{*}_F 0$. \square

Lemma 4.8 (Elimination of redundancies) *Let $F = (F_T, F_P)$. If $f \in F$ is such that $f \rightarrow_{F \setminus \{f\}} 0$ then the relations $\xrightarrow{*}_F$ and $\xrightarrow{*}_{F \setminus \{f\}}$ coincide.*

Proof The result is immediate, since for all $g \rightarrow_{\{f\}} h$ then $g = h + kufv \xrightarrow{*}_{F \setminus \{f\}} h$ where $k \in K$, $ufv \in \neg X^\dagger$. \square

Algorithm 4.9 (Noncommutative Buchberger Algorithm with tags) *Given a set of tagged and non-tagged polynomials the algorithm attempts to complete the set with respect to a given ordering so that the reduction relation generated is complete.*

1. (Input:) A mixed set of tagged and non-tagged polynomials $F = (F_T, F_P)$ where $F_T \subseteq K[\neg X^\dagger]$ and $F_P \subseteq K[X^\dagger]$.
2. (Initialise:) Put $\text{OLD} := F$ and $\text{SPOL} := \emptyset$.

3. (Search for matches:) If the leading monomials of any of the polynomials overlap then calculate the resulting S -polynomial and attempt to reduce it using \rightarrow_F . Record all non-zero reduced S -polynomials in the list SPOL.
4. (Add unresolved S -polynomials:) When all matches have been considered define $\text{NEW} := \text{OLD} \cup \text{SPOL}$.
5. (Eliminate redundancies:) Pass through NEW removing each polynomial in turn and reducing it with respect to the other polynomials in NEW. If a polynomial reduces to zero, delete it from NEW. Otherwise replace each with its reduced form.
6. (Loop:) Whilst $\text{OLD} \neq \text{NEW}$ set $\text{OLD} := \text{NEW}$, $\text{SPOL} := \emptyset$ and return to step 3.
7. (Output:) A set $F := \text{NEW}$ of polynomials such that \rightarrow_F is a complete reduction relation on $K[\dashv X^\dagger]$.

Remark 4.10 (Left Ideals) Placing tags to the right of polynomials rather than the left, i.e. working in $K[X^\dagger \dashv]$ or $K[X^* \dashv]$, by similar arguments we can compute left ideals. The tags act as a block to multiplication: to calculate left ideals, one blocks the right multiplication with a tag on the right; to calculate right ideals, one blocks the left multiplication with a tag on the left. It is natural that two-sided ideals have no tags, since both multiplications are defined.

Remark 4.11 (Implementation) The use of the free monoid $(X \cup \{\dashv\})^*$ is possible in Definition 3.2, i.e. $f \rightarrow_F f - kuf_i v$ if $u\text{LT}(f_i)v$ occurs in f with coefficient k $u, v \in (X \cup \{\dashv\})^*$. If a match of any of the five types described above occurs between f_1 and f_2 then there exist $u_1, u_2, v_1, v_2 \in (X \cup \{\dashv\})^*$ such that $u_1 m_1 v_1 = u_2 m_2 v_2$ (the converse is not true). Unmeaningful monomials such as $\dashv x x \dashv \dashv x$ do not arise as a result of any procedure we describe, including Algorithm 4.9. Therefore there is no problem with the computations taking place inside the free K -algebra $K[(X \cup \{\dashv\})^*]$. This is useful computationally as it allows us to use a standard noncommutative Gröbner basis program as an implementation of the procedures. In other words, this widens the scope of a noncommutative Gröbner basis program without modifying it: the program can now attempt to compute bases for one-sided ideals in finitely presented algebras.

5 Application to Green's Relations

The standard way of expressing the structure of an (abstract) semigroup is in terms of Green's relations. The relations enable the expression of the local structure of the semigroup in terms of groups with certain actions on them. Eggbox diagrams depict the partitions of a semigroup into their L -classes R -classes, D -classes and H -classes as defined by Green's relations. We can sometimes determine the classes by using Gröbner bases applied directly to the presentation. The examples show that there is also the possibility of dealing with infinite semigroups having infinitely many H -classes, L -classes or R -classes. First we recall some definitions [6].

A nonempty subset A of a semigroup S is a *right ideal* of S if $AS \subseteq A$, where $AS := \{as : a \in A, s \in S\}$. It is a *left ideal* of S if $SA \subseteq A$. If x is an element of S then the smallest right ideal of S containing

x is $xS \cup \{x\}$, we denote this $\langle x \rangle^r$ as it is called the *right ideal generated by x* . Similarly the *left ideal generated by x* is $Sx \cup \{x\}$ and is denoted $\langle x \rangle^l$.

Green's Relations

Let S be a semigroup and let s and t be elements of S . We say that s and t are *L-related* if the left ideal generated by s in S is equal to the left ideal generated by t :

$$s \sim_L t \Leftrightarrow \langle s \rangle^l = \langle t \rangle^l.$$

Similarly they are *R-related* if the right ideals are the same:

$$s \sim_R t \Leftrightarrow \langle s \rangle^r = \langle t \rangle^r.$$

The *L*-relation is a right congruence on S and the *R*-relation is a left congruence on S . (The right action of S on itself is preserved by the mapping to the *L*-classes - so $[x^y]_{\sim_L} = [xy]_{\sim_L} = [x]_{\sim_L}^y$, similarly for the left action and *R*-classes.) The elements s and t are said to be *H-related* if they are *both L-related and R-related*, and are *D-related* if they are *either L-related or R-related*.

To determine whether s and t are *R* (or *L*)-related we can compute the appropriate Gröbner bases and compare them. First let K be (any) field. Let S have presentation $sgp\langle X | Rel \rangle$. Let P be a Gröbner basis for $K[S]$ (so $K[X^\dagger]/=P \cong K[S]$). We would add the polynomial $\neg s$ to the Gröbner basis system for $K[S]$ and compute the Gröbner basis, and see whether this was equivalent to the basis obtained for $\neg t$.

6 Examples

Throughout the examples we will use the field \mathbb{Q} and the standard length-lexicographical ordering $>$.

Example 6.1 The first example is a two element semigroup with presentation $sgp\langle x | x^3 = x^2 \rangle$.

The Gröbner basis for the right ideal $\langle x \rangle^r$ is $\{\neg x, x^3 - x^2\}$ and the Gröbner basis for $\langle x^2 \rangle^r$ is $\{\neg x^2, x^3 - x^2\}$. The Gröbner bases are different and therefore x and x^2 are not *R-related*. Similarly, the Gröbner basis for the left ideal $\langle x \rangle^l$ is $\{x\neg, x^3 - x^2\}$ and the Gröbner basis for $\langle x^2 \rangle^l$ is $\{x^2\neg, x^3 - x^2\}$ so the elements are not *L-related*. Therefore this semigroup has two *H*-classes.

Example 6.2 The following example is for the finite monoid $Sym(2)$ with semigroup presentation

$$sgp\langle e, s | e^2 = e, s^3 = s, s^2e = e, es^2 = e, sese = ese, eses = ese \rangle.$$

The Gröbner basis equivalent to the rewrite system is

$$F := \{e^2 - e, s^3 - s, s^2e - e, es^2 - e, eses - ese, sese - ese\}.$$

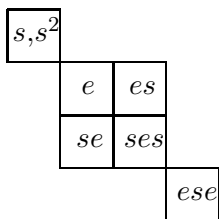
The elements are $\{e, s, es, se, s^2, ese, ses\}$, where s^2 is the identity element. We calculate Gröbner bases for the right and left ideals for each of the elements. The results are displayed in the table below. In detail, a Gröbner basis for $\langle ses \rangle^r$ in $K[S]$ in $K[\neg X^\dagger]$ is calculated by adding $\neg ses$ to the set of polynomials F . A match s occurs on $\neg sesse$ between $sse - e$ and $\neg ses$. This results in the

S-polynomial $\neg se(e) - (0)se$ which reduces to $\neg se$. Another match of es occurs on $\neg seses$ between $eses - ese$ and $\neg ses$. This results in the S-polynomial $\neg s(ese) - (0)es$ which reduces to $\neg ese$. All further matches result in S-polynomials which reduce to zero. The polynomials we add to F to obtain a Gröbner basis are $\{\neg se, \neg ese\}$ (note that $\neg ses$ is a multiple of $\neg se$ so it is not required in the Gröbner basis). The table lists the polynomials which, together with F , will give the Gröbner bases for the right and left ideals generated by single elements.

<i>element</i>	<i>right ideal</i>	<i>left ideal</i>
e	$\neg e$	$e\vdash$
s	$\neg e, \neg s$	$e\vdash, s\vdash$
es	$\neg e$	$es\vdash, ese\vdash$
se	$\neg se, \neg ese$	$e\vdash$
ss	$\neg e, \neg s$	$e\vdash, s\vdash$
ese	$\neg ese$	$ese\vdash$
ses	$\neg se, \neg ese$	$es\vdash, ese\vdash$

Two elements whose right ideals are generated by the same Gröbner basis have the same right ideal (similarly left), and so it is immediately deducible that the R -classes are $\{s, s^2\}, \{e, es\}, \{se, ses\}$ and $\{ese\}$, the L -classes are $\{s, s^2\}, \{e, se\}, \{es, ses\}$ and $\{ese\}$, the H -classes are $\{s, s^2\}, \{e\}, \{se\}, \{es\}, \{ses\}$ and $\{ese\}$ and the D -classes are $\{s, s^2\}, \{e, es, se, ses\}$ and $\{ese\}$.

The eggbox diagram is as follows where L -classes are columns, R -classes are rows, D -classes are diagonal boxes and H -classes are the small boxes:



This example could have been calculated by enumerating the elements of each of the fourteen ideals – a time consuming procedure which calculates details which we do not require.

Example 6.3 The next example is the Bicyclic monoid which is infinite. We use the semigroup presentation $\langle p, q, i \mid pi = p, qi = q, ip = p, iq = q, pq = i \rangle$.

The equivalent Gröbner basis, defined on $K[\{p, q, i\}^\dagger]$, is $\{pi - p, qi - q, ip - p, iq - q, pq - i\}$. We begin the table as before:

<i>element</i>	<i>right ideal</i>	<i>left ideal</i>
id	$\neg i.$	$i \vdash.$
p	$\neg i.$	$p \vdash.$
q	$\neg q.$	$q \vdash.$
p^2	$\neg i.$	$p^2 \vdash.$
qp	$\neg q.$	$p \vdash.$
q^2	$\neg q^2.$	$i \vdash.$
\dots	\dots	\dots
$q^n p^m$	$\neg q^n.$	$p^m \vdash.$

It can be seen that there are infinitely many L -classes and infinitely many R -classes. Representatives for the L -classes are the elements of $\{q\}^*$ because $q^n p^m \vdash \rightarrow q^n \vdash$ (using the S-polynomial resulting from $p^n (q^n p^m \vdash) \rightarrow p^n \vdash$ with $(p^n q^n) p^m \vdash \rightarrow p^m \vdash$). Similarly the elements of $\{p\}^*$ are representatives for the R -classes. All elements are D -related and none of them are H -related. So the eggbox diagram would be an infinitely large box of cells with one element in each cell. This means that the monoid is *bisimple*.

Example 6.4 Now consider the Polycyclic monoid P_n which has monoid presentation

$$\text{mon}\langle x_1, \dots, x_n, y_1, \dots, y_n, o, id \mid ox_i = x_i o = oy_i = y_i o = o, x_i y_i = id, x_i y_j = o \text{ for } i, j = 1, \dots, n-1, i \neq j \rangle$$

and therefore the Gröbner basis for $K[P_n]$, where K is a field, is

$$\{x_i y_i - id, x_i y_j - 0 \text{ for } i, j = 1, \dots, n-1, i \neq j\}.$$

Green's relations for the polycyclic monoids are naturally similar to those for the Bicyclic monoid. The L -classes are represented by sequences of y_i 's and the R -classes are represented by sequences of x_i 's. To verify this, let $X = x_{i_1} \cdots x_{i_k}$ be a general word in the x_i 's, and let Y be $y_{j_1} \cdots y_{j_l}$ a general word in the y_j 's. Then we can show that $YX \sim_L X$. To do this consider $\langle YX \vdash \rangle$ and $\langle X \vdash \rangle$. To find a Gröbner basis for $\langle YX \vdash \rangle$ consider the match $x_{j_l} \cdots x_{j_1} y_{j_1} \cdots y_{j_l} x_{i_1} \cdots x_{i_k} \vdash$. This results in the S-polynomial $(id)x_{i_1} \cdots x_{i_k} \vdash - x_{j_l} \cdots x_{j_1} (0)$ which simplifies to $x_{i_1} \cdots x_{i_k} \vdash = X \vdash$. This is a Gröbner basis for $\langle YX \vdash \rangle$, and so $\langle YX \vdash \rangle = \langle X \vdash \rangle$. Similarly $\langle \neg YX \rangle = \langle \neg Y \rangle$ so $YX \sim_R X$ for any $Y = y_{j_1} \cdots y_{j_l}$, $X = x_{i_1} \cdots x_{i_k}$.

The eggbox diagram is drawn below. As before the L classes are the columns and the R -classes the rows, H -classes are the cells, and there is just one D -class other than the one containing the zero. This proves that the polycyclic monoids are bisimple. The diagram is more conventional than the previous one, as classes are listed but not individual elements, instead the number of elements in each cell is indicated.

	[0]	[\mathcal{A}]	[y_1]	[y_2]	-	[y_1^2]	[y_1y_2]	-	-	[Y]	-
[0]	1										
[\mathcal{A}]		1	1	1	-	1	1	-	-	1	-
[x_1]		1	1	1	-	1	1	-	-	1	-
[x_2]		1	1	1	-	1	1	-	-	1	-
[x_1^2]		1	1	1	-	1	1	-	-	1	-
[x_1x_2]		1	1	1	-	1	1	-	-	1	-
[X]		1	1	1	-	1	1	-	-	1	-

These examples illustrate the fact that Buchberger’s algorithm can be used to compute Green’s relations for (infinite) semigroups which have finite complete presentations. Previous methods for calculating minimal ideals from presentations of semigroups were variations on the classical Todd-Coxeter enumeration procedure [3]. This is an alternative computational approach to that given in [7, 8] which uses the transformation representation of a semigroup rather than a presentation. As with [8] the methods described in this paper provide for local computations, concerning a single R -class, without computing the whole semigroup. The one-sided Gröbner basis methods have limitations in that a complete rewrite system with respect to the chosen order might not be found, but they do give the possibility of calculating the structure of infinite semigroups and do not require the determination of a transformation representation for those semigroups which arise naturally as presentations.

The calculations of the examples were achieved using a GAP3 implementation of the Gröbner basis procedures for polynomials in noncommutative variables over \mathbb{Q} as described in [10]. Further details of this program can be found in [4] or e-mail the author. Other implementations (e.g. OPAL, Bergman) are more powerful: the key point of this paper is to point out that such programs can be used for a wider range of problems than has previously been recorded.

References

- [1] F.Baader and T.Nipkow : Term Rewriting and All That, *Cambridge University Press* 1998.
- [2] B.Buchberger and F.Winkler : “Gröbner Bases and Applications”, “33 Years of Gröbner Bases” *RISC-Linz 2-4 Feb 1998, Proc. London Math. Soc. vol.251* 1998.

- [3] C.M.Campbell, N.Rušćuc, E.F.Robertson and R.M.Thomas : “Rewriting a Semigroup Presentation”, *International Journal of Algebra and Computation*, vol.5 no.1 p81-103 1995.
- [4] A. Heyworth, “Rewriting and Noncommutative Gröbner Bases with Applications to Kan Extensions and Identities Among Relations”, *UWB Math Preprint 98.23*, <http://xxx.soton.ac.uk/abs/math/9812097>, 1998.
- [5] A. Heyworth, “Rewriting as a Special Case of Noncommutative Gröbner Basis Theory”, *UWB Math Preprint 98.22*, <http://xxx.soton.ac.uk/abs/math/9901044>, 1998.
- [6] J.M.Howie: “Fundamentals of Semigroup Theory”, *LMS new series vol.12*, *Oxford Science Publications* 1995.
- [7] S.A.Linton, G.Peiffer, E.F.Robertson and N.Rušćuc: “Groups and Actions in Transformation Semigroups,” *Mathematische Zeitschrift vol.228 p435-450*, 1998.
- [8] S.A.Linton, G.Peiffer, E.F.Robertson and N.Rušćuc : “Computing Transformation Semigroups”, *Journal of Symbolic Computation vol.11 p1-18*, 1998.
- [9] F.Mora : “Gröbner Bases for Noncommutative Polynomial Rings” , *Proc. AAEECC-3, LNCS 229, p353-362*, Springer, 1985.
- [10] T.Mora : “Gröbner Bases and the Word Problem” , *Preprint, University of Genova* 1987.
- [11] T.Mora : “An Introduction to Commutative and Noncommutative Gröbner Bases”, *Theoretical Computer Science vol.134 p131-173* 1994.
- [12] B.Reinert : “On Gröbner Bases in Monoid and Group Rings”, *PhD Thesis, Universität Kaiserslautern* 1995.
- [13] B.Reinert and D.Zecker : “MRC - A System for Computing Gröbner Bases in Monoid and Group Rings” , *Universität Kaiserslautern Preprint* 1998.
- [14] V.Ufnarovski : “Introduction to Noncommutative Gröbner Basis Theory” , *in Gröbner Bases and Applications, B.Buchberger and F.Winkler (eds), Proc. London Math. Soc. vol.251 p305-322* 1998.