Rewriting as a Special Case of Noncommutative Gröbner Basis Theory

Anne Heyworth
University of Wales, Bangor

1 Introduction

Rewriting for semigroups is a special case of Gröbner basis theory for noncommutative polynomial algebras. The fact is a kind of folklore but is not fully recognised. So our aim in this paper is to elucidate this relationship.

A good introduction to string rewriting is [2], and a recent introduction to noncommutative Gröbner basis theory is [12]. Similarities between the two critical pair completion methods (Knuth- Bendix and Buchberger's algorithm) have often been pointed out in the commutative case. The connection was first observed in [7, 5] and more closely analysed in [3, 4] and more recently in [11] and [10]. In particular it is well known that the commutative Buchberger algorithm may be applied to presentations of abelian groups to obtain complete rewrite systems.

Rewriting involves a presentation $sgp\langle X|R\rangle$ of a semigroup S and presents S as a factor semigroup $X^\dagger/=_R$ where $X^\dagger$ is the free semigroup on X and $=_R$ is the congruence generated by the subset R of $X^\dagger \times X^\dagger$. Noncommutative Gröbner basis theory involves a presentation $alg\langle X|F\rangle$ of a noncommutative algebra A over a field K and presents A as a factor algebra $K[X^\dagger]/\langle F\rangle$ where $K[X^\dagger]$ is the free K-algebra on the semigroup $X^\dagger$ and $\langle F\rangle$ is the ideal generated by F, a subset of $K[X^\dagger]$. Given a semigroup presentation $sgp\langle X|R\rangle$ we consider the algebra presentation $alg\langle X|F\rangle$ where $F := \{l - r : (l, r) \in R\}$. It is well known that the word problem for $sgp\langle X|R\rangle$ is solvable if and only if the (monomial) equality problem for $alg\langle X|F\rangle$ is solvable. Teo Mora [8] recorded that a complete rewrite system for a semigroup S presented by $sgp\langle X|Rel\rangle$ is equivalent to a noncommutative Gröbner basis for the ideal specified by the congruence $=_R$ on $X^\dagger$ in the algebra $\mathbb{F}_3[X^\dagger]$ where $\mathbb{F}_3$ is the field with elements $\{-1, 0, 1\}$.

In this paper we show that the noncommutative Buchberger algorithm applied to F corresponds step-by-step to the Knuth-Bendix completion procedure for R. This is the meaning intended for the first sentence of this paper.

2 Results

First we note that the relation between the two kinds of presentation is given by the following variation of a result of [8].

Proposition

Let K be a field and let S be a semigroup with presentation $sgp\langle X|R\rangle$. Then the algebra $K[S]$ is isomorphic to the factor algebra $K[X^\dagger]/\langle F\rangle$ where F is the basis $\{l - r|(l, r) \in R\}$.

Proof

Define $\phi : K[X^\dagger] \to K[S]$ by $\phi(k_1w_1 + \cdots + k_tw_t) := k_1[w_1]_R + \cdots + k_t[w_t]_R$ for $k_1, \ldots, k_t \in K$, $w_1, \ldots, w_t \in X^\dagger$. Define a homomorphism $\phi' : K[X^\dagger]/\langle F\rangle \to K[S]$ by $\phi'([p]_F) := \phi(p)$. It is injective since $\phi'[p]_F = \phi[q]_F$ if and only if $[p]_F = [q]_F$ (using the definitions $\phi(p) = \phi(q) \Leftrightarrow p - q \in \langle F\rangle$). It is also surjective. Let $f \in K[S]$. Then $f = k_1m_1 + \cdots + k_tm_t$ for some $k_1, \ldots, k_t \in K$, $m_1, \ldots, m_t \in S$. Since S is presented by $sgp\langle X|R\rangle$ there exist $w_1, \ldots, w_t \in X^\dagger$ such that $[w_i]_R = m_i$ for $i = 1, \ldots, t$. Therefore let $p = k_1w_1 + \cdots + k_tw_t$. Clearly $p \in K[X^\dagger]$ and also $\phi'[p]_F = f$. Hence ϕ' is an isomorphism. □

Now we give our main result.

Theorem

Let $sgp\langle X|R\rangle$ be a semigroup presentation, let K be a field and let $alg\langle X|F\rangle$ be the K-algebra presentation with $F := \{l - r : (l, r) \in R\}$. Then the Knuth-Bendix completion algorithm for the rewrite system R corresponds step-by-step to the noncommutative Buchberger algorithm for finding a Gröbner basis for the ideal generated by F.

Proof Both the Knuth-Bendix algorithm for R and the Buchberger algorithm for F begin by specifying a monomial ordering on $X^\dagger$ which we denote $>$.

The correspondence between terminology in the two cases is

(i)	rewrite system	basis
(ii)	rule	two-term polynomial
(iii)	word	monomial
(iv)	reduction	reduction
(v)	left hand side	leading monomial
(vi)	subword	submonomial
(vii)	right hand side	remainder
$(viii)$	overlap	match
(ix)	critical pair	S-polynomial

This key part of the correspondence (viii) and (ix) is illustrated diagrammatically in the next section

(x)	resolve	reduce to zero
(xi)	reduced critical pair	reduced S-polynomial
(xii)	complete rewrite system	Gröbner basis

In terms of rewriting we consider the rewrite system R which consists of a set of rules of the form (l, r) orientated so that $l > r$. A word $w \in X^\dagger$ may be reduced with respect to R if it contains the left hand side l of a rule (l, r) as a subword i.e. if $w = ulv$ for some $u, v \in X^*$. To reduce $w = ulv$ using the rule (l, r) we replace l by the right hand side r of the rule, and write $ulv \to_R urv$. The Knuth-Bendix algorithm looks for overlaps between rules. Given a pair of rules (l_1, r_1), (l_2, r_2) there are four possible ways in which an overlap can occur: $l_1 = u_2l_2v_2$, $u_1l_1v_1 = l_2$, $l_1v_1 = u_2l_2$ and $u_1l_1 = l_2v_2$. The critical pair resulting from an overlap is the pair of words resulting from applying each rule to the smallest word on which the overlap occurs. The critical pairs resulting from each of the four overlaps are: $(r_1, u_2r_2v_2)$, $(u_1r_1v_1, r_2)$, (r_1v_1, u_2r_2) and (u_1r_1, r_2v_2) respectively (see diagram). In one pass the completion procedure finds all the critical pairs resulting from overlaps of rules of R. Both sides of each of the critical pairs are reduced as far as possible with respect to R to obtain a reduced critical pair (c_1, c_2). The original pair is said to resolve if $c_1 = c_2$. The reduced pairs that have not resolved are orientated, so that $c_1 > c_2$, and added to R forming R_1. The procedure is then repeated for the rewrite system R_1, to obtain R_2 and so on. When all the critical pairs of a system R_n resolve (i.e. $R_{n+1} = R_n$) then R_n is a complete rewrite system.

In terms of Gröbner basis theory applied to this special case we consider the basis F which consists of a set of two-term polynomials of the form $l - r$ multiplied by ± 1 so that $l > r$. A monomial $m \in X^\dagger$ may be reduced with respect to F if it contains the leading monomial l of a polynomial $l - r$ as a submonomial i.e. if $m = ulv$ for some $u, v \in X^*$. To reduce $m = ulv$ using the polynomial $l - r$ we replace l by the remainder r of the polynomial, and write $ulv \to_F urv$. The Buchberger algorithm looks for matches between polynomials. Given a pair of polynomials $l_1 - r_1$, $l_2 - r_2$ there are four possible ways in which an match can occur: $l_1 = u_2l_2v_2$, $u_1l_1v_1 = l_2$, $l_1v_1 = u_2l_2$ and $u_1l_1 = l_2v_2$. The S- polynomial resulting from a match is the difference between the pair of monomials resulting from applying each two-term polynomial to the smallest monomial on which the match occurs. The S-polynomials resulting from each of the four matches are: $r_1 - u_2r_2v_2$, $u_1r_1 - v_1, r_2$, $r_1v_1 - u_2r_2$ and $u_1r_1 - r_2v_2$ respectively (see diagram). In one pass the completion procedure finds all the S-polynomials resulting from matches of polynomials of F. The S-polynomials are reduced as far as possible with respect to F to obtain a reduced S-polynomial $c_1 - c_2$. Note that reduction can only replace one term with another so the reduced S-ploynomial will have two terms unless the two terms reduce to the same thing $c_1 = c_2$ in which case the original S-polynomial is said to reduce to zero. The reduced S-polynomials that have not been reduced to zero are multiplied by ± 1, so that $c_1 > c_2$, and added to F forming F_1. The procedure is then repeated for the basis F_1, to obtain F_2 and so on. When all the S-polynomials of a basis F_n reduce to zero (i.e. $F_{n+1} = F_n$) then F_n is a Gröbner basis.

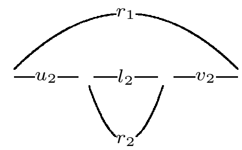
A critical pair in R will occur if and only if a corresponding S-polynomial occurs in F. Reduction of the pair by R is equivalent to reduction of the S-polynomial by F. Therefore at any stage any new rules correspond to the new two-term polynomials and $F_i := \{l - r : (l, r) \in R_i\}$. Therefore the completion procedures as applied to R and F correspond to each other at every step. □

3 Illustration

This is a picture of the correspondence (viii) and (ix) between critical pairs and S-polynomials and the four ways in which they can occur, as described in the above proof.

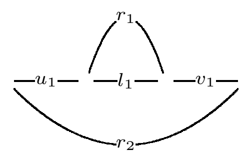
possible overlaps of rules $l_1 \to r_1$ and $l_2 \to r_2$		possible matches of polynomials $l_1 - r_1$ and $l_2 - r_2$

$l_1 = u_2 l_2 v_2$
$(r_1, u_2 r_2 v_2)$



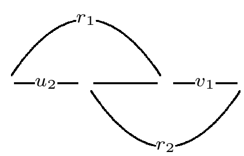
$l_1 = u_2 l_2 v_2$
$u_2 r_2 v_2 - r_1$

$u_1 l_1 v_1 = l_2$
$(u_1 r_1 v_1, r_2)$



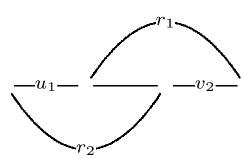
$u_1 l_1 v_1 = l_2$
$r_2 - u_1 r_1 v_1$

$l_1 v_1 = u_2 l_2$
$(r_1 v_1, u_2 r_2)$



$l_1 v_1 = u_2 l_2$
$u_2 r_2 - r_1 v_1$

$u_1 l_1 = l_2 v_2$
$(u_1 r_1, r_2 v_2)$



$u_1 l_1 = l_2 v_2$
$r_2 v_2 - u_1 v_1$

4 Remarks

The result that the Knuth-Bendix algorithm is a special case of the noncommutative Buchberger algorithm is something that requires further investigation. Rewriting techniques and the Knuth-Bendix algorithm have recently been applied to presentations of Kan extensions over sets [6] and it is not immediately obvious what this will imply for noncommutative Gröbner bases. Another interesting line of investigation would be to attempt to adapt rewriting procedures for constructing crossed resolutions of group presentations [6] to the more general Gröbner basis situation.

References

[1] F.Baader and T.Nipkow : Term Rewriting and All That, *Cambridge University Press* (1998).

[2] R.Book and F.Otto : String-Rewriting Systems, *Springer-Verlag, New York,* (1993).

[3] B.Buchberger : Basic Features and Development of the Critical Pair Completion Procedure, in Rewriting Techniques and Applications, J.Jouannaud (ed), *Springer-Verlag, LCNS vol.202 p1-45* (1986).

[4] B.Buchberger : History and Basic Features of the Critical Pair / Completion Procedure, *J.Symbolic Computation, vol.3, p3-38* (1987).

[5] B.Buchberger and R.Loos : Algebraic Simplification, *Computing Supplement, vol.4 p11-43* (1982).

[6] A.Heyworth : Applications of Rewriting Systems and Gröbner Bases to Computing Kan Extensions and Identities Among Relations, *PhD Thesis, University of Wales, Bangor* (1998)

[7] R.Loos : Term Reduction Systems and Algebraic Algorithms, in Proc 5th German Workshop on Artificial Intelligence, J.Siekmann (ed), *Springer-Verlag, Informatik Fachberichte, vol.47 p214-234* (1981).

[8] T.Mora : Gröbner Bases and the Word Problem, *Preprint, University of Genova* (1987).

[9] T.Mora : An Introduction to Commutative and Noncommutative Gröbner Bases, *Theoretical Computer Science vol.134 p131-173*(1994).

[10] B.Reinert : On Gröbner Bases in Monoid and Group Rings *PhD Thesis, Universität Kaiserslautern* (1995).

[11] K.Stokkermans : A Categorical Framework and Calculus for Critical Pair Completion, *Phd Thesis, Royal Institute for Symbolic Computation, Johannes Kepler University, Linz* (1995).

[12] V.Ufnarovski : Introduction to Noncommutative Gröbner Bases Theory, in Gröbner Bases and Applications, B.Buchberger and F.Winkler (eds), *Proc. London Math. Soc. vol.251 p305-322* (1998).

Acknowledgements

This research work was supported by an Earmarked EPSRC Research Studentship 1995-98 'Identities among Relations for Monoids and Categories'. I would like to thank Larry Lambe for pointing out this likely connection, Ronnie Brown for discussion on the paper, and Neil Dennis for encouraging my work.