Gröbner Bases for Noncommutative Polynomials

Arjeh M. Cohen

8 January 2007

first lecture of
Three aspects of exact computation
a tutorial at
Mathematics: Algorithms and Proofs (MAP)
Leiden, January 8–12, 2007
Outline

1. Introduction
2. Rewriting
3. Gröbner bases
4. Gröbner algorithm
5. Examples
6. Conclusion

Based on work with Dié Gijsbers
1. Introduction

Gröbner bases are generating sets of ideals in commutative polynomial rings $k[x_1, \ldots, x_n]$ that help

- solve polynomial systems of equation by triangularization
- solve linear equations over $k[x_1, \ldots, x_n]$ (ideal membership)
- describe quotient algebras effectively

The theory fails for non-commutative polynomial rings to a considerable extent, but still there are things we can do.
Our concern

Finding Gröbner bases for finite generating sets of ideals in noncommutative polynomial rings $k\langle x_1, \ldots, x_n \rangle$ that help

- describe quotient algebras effectively
Limitations

There are infinitely generated ideals, eg \((n = 2)\)

\[(x_1 x_2^i x_1 : i = 1, 2, 3, \ldots)\]
Limitations

There are infinitely generated ideals, eg \((n = 2)\)

\[(x_1x_2^i x_1 : i = 1, 2, 3, \ldots)\]

The word problem for finitely presented groups is a special case.

This is known not to be solvable.

Hence a noncommutative Gröbner basis algorithm will not always terminate.
Motivation by example

The transpositions $r_1 = (1, 2)$, $r_2 = (2, 3)$, and $r_3 = (3, 4)$ generate the symmetric group $\Sigma_4$.

These satisfy the relations

\[
\begin{align*}
    r_1 r_2 r_1 - r_2 r_1 r_2 &= 0 \\
    r_2 r_3 r_2 - r_3 r_2 r_3 &= 0 \\
    r_1 r_3 - r_3 r_1 &= 0 \\
    r_1^2 - 1 &= 0 \\
    r_2^2 - 1 &= 0 \\
    r_3^2 - 1 &= 0
\end{align*}
\]

In order to prove that this is a presentation of $\Sigma_4$: get canonical forms for the 24 elements of $\Sigma_4$ as words in $r_1$ and $r_2$. 
Brauer diagrams for permutations

Figure 1: A diagram for (2, 3, 4)

Permutations represented by diagrams; multiplication by composition
Brauer diagrams with horizontal strands

Figure 2: A Brauer diagram

Closed loop (after compositions) $\sim \delta$ (an element of $k$)
Towards generators of the Brauer algebra

Figure 3: Elements $e_i$
Example

Figure 4: This Brauer diagram equals $r_2 e_1 r_3 r_2 r_3$
BMW Algebra

This is a deformation of the Brauer algebra with generators $g_i$ (replacing $r_i$) and $e_i$ as before and relations parametrized by diagram

```
    1   2   3
```

as follows, where $m(1 - \delta) = l - l^{-1}$

<table>
<thead>
<tr>
<th>Condition</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>for $i$</td>
<td>$g_i^2 = 1 - m(g_i - l^{-1}e_i)$</td>
</tr>
<tr>
<td></td>
<td>$e_ig_i = l^{-1}e_i$</td>
</tr>
<tr>
<td></td>
<td>$g_ie_i = l^{-1}e_i$</td>
</tr>
<tr>
<td>for $i \not\sim j$</td>
<td>$g_ig_j = g_jg_i$</td>
</tr>
<tr>
<td>for $i \sim j$</td>
<td>$g_ig_ig_i = g_jg_ig_j$</td>
</tr>
<tr>
<td></td>
<td>$e_ig_je_i = le_i$</td>
</tr>
</tbody>
</table>


BMW algebra dimension

To compute the BMW algebra given by the above relations, find a Gröbner basis and compute dimension.

Input 17 polynomials (the relations) such as
\[ e_1 - lm^{-1}g_1^2 - lg_1 + lm^{-1} \text{ and } g_1g_2g_1 - g_2g_1g_2 \]

\[ m = 7, \ l = 11. \] The computation took 350 msecs.

One of the 89 output polys:
\[ g_1g_2e_3g_2e_1 + 7g_2e_3g_2e_1 - g_2g_3g_2e_1 + 7e_3e_2e_1 + 49e_3g_2e_1 + 7e_2e_1e_3 - 7g_3g_2e_1 + 49g_2e_1e_3 - 7g_2g_3e_1 + 343e_1e_3 - 49g_3e_1 - 49g_2e_1 - 350e_1 \]

Dimension of the quotient algebra is \( 105 = 3 \cdot 5 \cdot 7 \).

Script done on Sun 07 Jan 2007 05:40:42 PM CET
Commutative Gröbner basis algorithm, briefly

Given: a set $B$ of polynomials in $k[x_1, \ldots, x_n]$.

$P := \{\text{unordered pairs of elts from } B\}$;

while $P \neq \emptyset$

    choose $\{f, g\} \in P$;
    $P := P \setminus \{f, g\}$;
    $c := \text{NormalForm}(S(f, g), B)$;
    if $c \neq 0$ then
        $B := B \cup \{c\}$;
        $P := P \cup \{\{b, c\} : b \in B\}$;
    endif

endwhile

return $B$

$S(f, g)$ is a $k[x_1, \ldots, x_n]$-linear combination of $f$ and $g$ in which leading terms cancel.
Commutative Gröbner basis algorithm, briefly

Given: a set $B$ of polynomials in $k[x_1, \ldots, x_n]$.

$P := \{\text{unordered pairs of elts from } B\}$;

while $P \neq \emptyset$

    choose $\{f, g\} \in P$;
    $P := P \setminus \{f, g\}$;
    $c := \text{NormalForm}(S(f, g), B)$;
    if $c \neq 0$ then
        $B := B \cup \{c\}$;
        $P := P \cup \{\{b, c\} : b \in B\}$;
    endif

endwhile

return $B$

$S(f, g)$ is a $k[x_1, \ldots, x_n]$-linear combination of $f$ and $g$ in which leading terms cancel.

Termination: Ideal generated by $L(B)$ increases and $k[x_1, \ldots, x_n]$ is Noetherian.
2. Rewriting

- Reduction ordering on monomials
- $\text{NormalForm}(\text{polynomial}, \text{basis})$
- $S$-polynomials obstructions
- Gröbner basis
Reduction ordering

$k$ is a field.

$T$ is the free monoid on $n$ generators $x_1, \ldots, x_n$.

An ordering $<$ on $T$ is called a reduction ordering if, for all $t_1, t_2, l, r \in T$ with $t_1 < t_2$,

$$1 \leq lt_1r < lt_2r.$$
Examples

- **lex(igraphic) not a reduction ordering**
  
  \(a^{j+1}b < a^j b\) conflicts with \(a > 1\).

- **deglex: total degree first, then lexicographic**
  
  \[1 < a < b < a^2 < ab < b^2 < a^3 < a^2b < aba < ab^2 < ba^2 < bab < b^2a < b^3 < \ldots\]
Reduction ordering, cont’d

Fix a reduction ordering $<$ on $T$.

The reduction ordering is extensible to finite sets of monomials: $A <_F B$ iff $A \neq B$ and $\forall u \in A \setminus B \exists v \in (B \setminus A) v > u$.

deglex $<$ is Noetherian and hence (by well known lemma) its extension $<_F$. 
Ordered form of a polynomial

Each \( f \in k\langle T \rangle \) is a unique linear combination of monomials \( t_i \):

\[
f = \sum_{i=1}^{s} c_i t_i \quad \text{with} \quad c_i \in k \setminus \{0\} \quad \text{and} \quad t_i \in T, \text{ such that } t_1 > \cdots > t_s.
\]

This is the ordered form of \( f \).

\( f \) is called monic if \( c_1 = 1 \).

\( L(f) := t_1 \), the largest monomial of \( f \).
Normal form

Let $G \subset k\langle T \rangle$, finite, and denote by $I$ the ideal generated by $G$.

For a polynomial $f$, $\text{NormalForm}(f, G)$ is ‘minimal elt’ of $k\langle T \rangle$ with

- $f - \text{NormalForm}(f, G) \in I$
- either $\text{NormalForm}(f, G) = 0$
  or $L(g) \not| L(\text{NormalForm}(f, G))$ for each $g \in G$.

Computable
Normal form is not unique

Figure 5: Two normal forms of $xyx$ wrt $\{xy - x, yx - y\}$
3. Gröbner basis

A finite generating set $G$ of an ideal $I$ of $k\langle T \rangle$ is called a basis of $I$.

$G$ is a Gröbner basis of $I$ if

- $G$ is a basis of $I$ and
- $\text{NormalForm}(h, G) = 0$ for each $h \in I$. 
Examples

\[ G = [xy - x, yx - y] \]

\[ \text{NormalForm}(s(1, 1, x; x, 2, 1), G) = x^2 - x \quad [xyx] \]

\[ \text{NormalForm}(s(y, 1, 1; 1, 2, y), G) = y^2 - y \quad [yxy] \]

\[ G \cup [x^2 - x, y^2 - y] \text{ is a Gröbner basis.} \]
Obstruction

Let \( G = (g_i)_{1 \leq i \leq k} \) be a list of monic polynomials. An obstruction of \( G \) is a six-tuple
\[
(l, i, r; \lambda, j, \rho)
\]
with \( i, j \in \{1, \ldots, k\} \) and \( l, \lambda, r, \rho \in T \) such that
\[
L(g_i) \leq L(g_j) \text{ and } lL(g_i)r = \lambda L(g_j)\rho.
\]

\( S \)-polynomial

Given an obstruction we define the corresponding \( S \)-polynomial as
\[
s(l, i, r; \lambda, j, \rho) = lg_ir - \lambda g_j\rho.
\]
Obstruction example

\[ G = [xy - x, yx - y] \]

\[ s(1, 1, x; x, 2, 1) = xyx - x^2 - yxy + xy = -x^2 + xy \]

\[ NormalForm(x^2 - xy, G) = x^2 - x \]

Figure 6: New rewrite rule for \( G \)
Reducing the number of obstructions

\( G = (g_h) \) is a list of monic polynomials. A poly \( f \) is \textit{weak with respect to} \( G \) if there are \( c_h \in k \) and \( l_h, r_h \in T \) such that

\[
 f = \sum_h c_h l_h g_h r_h \quad \text{with} \quad l_h L(g_h) r_h \leq L(f).
\]

We call an obstruction \((l, i, r; \lambda, j, \rho)\) of \( G \) \textit{weak} if its S-polynomial \( s(l, i, r; \lambda, j, \rho) \) is weak wrt \( G \).

The S-polynomial of a weak obstruction \((l, i, r; \lambda, j, \rho)\) can be written as follows with \( c_h \in k \) and \( l_h, r_h \in T \).

\[
 s = lg_i r - \lambda g_j \rho = \sum_h c_h l_h g_h r_h \quad \text{with} \quad l_h L(g_h) r_h \leq L(s) < lL(g_i) r.
\]
Reducibility

\[ G = (g_h) \] is a list of monic polynomials in \( k\langle T \rangle \).
\[ H = \{s_1, \ldots, s_m\} \] is a set of polynomials.

A polynomial \( s \) is called reducible from \( H \) wrt \( G \) if weakness wrt \( G \) of all elements of \( H \) implies weakness of \( s \) wrt \( G \).

If \( s \) is weak then it is reducible from \( \emptyset \).

**Lemma** Each \( s(\omega_1 i, r\omega_2; \omega_1 \lambda, j, \rho\omega_2) \) is reducible from \( s(l, i, r; \lambda, j, \rho) \).
Overlap

For $b \in T$, two monomials $t_1 \leq t_2$ are said to have overlap $b$ if there are $a, c \in T$ such that one of

- $t_1 = ab$ and $t_2 = bc$
- $t_1 = ba$ and $t_2 = cb$
- $t_1 = b$ and $t_2 = abc$

If 1 is the only overlap between $t_1$ and $t_2$, the two monomials $t_1$ and $t_2$ are said to have no overlap.

An obstruction $(l, i, r; \lambda, j, \rho)$ is said to have no overlap if $L(g_i)$ and $L(g_j)$ do not overlap in $lL(g_i)r$. 
Overlap, cont’d

If $L(g_i)$ and $L(g_j)$ have no overlap, then every obstruction $(l, i, r; \lambda, j, \rho)$ with $l, r, \rho, \lambda \in T$ has no overlap.

The converse is not true:
if $L(g_i) = x_1x_2$ and $L(g_j) = x_2x_3$, then these monomials have overlap $x_2$ but $(1, i, x_2x_3; x_1x_2, j, 1)$ has no overlap.

$$1 \cdot (x_1x_2) \cdot (x_2x_3) = (x_1x_2) \cdot (x_2x_3) \cdot 1.$$
Reducibility

**Lemma**  
Every obstruction that has no overlap is reducible from an S-polynomial with overlap wrt $G$.

Basic sets

A set $H$ of polynomials is called *basic for* $G$ if every S-polynomial of $G$ is reducible from $H$ wrt $G$. 
Basic obstructions

A basic set $H$ of $S$-polynomials of $G$ can be chosen so that every element of $H$ comes from an obstruction with overlap and with

$$[l = 1 \text{ or } \lambda = 1] \quad \text{and} \quad [r = 1 \text{ or } \rho = 1].$$

The irreducible ones among these are the basic obstructions (finite).
Proposition

Let $G$ be a finite set of monic polynomials.

Let $H$ be the set of all non-zero normal forms of $S$-polynomials wrt $G$ corresponding to all basic obstructions of $G$.

Then $H$ is a basic set for $G$. 
Further trimming of the basic set

There are obstructions that can be removed from the list of those that need to be considered.
Partial Gröbner pair

Let $I$ be a two sided ideal of $k\langle T \rangle$ and let $G, D$ be finite subsets of $k\langle T \rangle$.

$(G, D)$ is a partial Gröbner pair for $I$ if

(i) all elts of $G \cup D$ are monic

(ii) $G$ is a basis of $I$

(iii) $D \subseteq I$

(iv) Each elt of $D$ is in normal form wrt $G$

(v) the set $D$ is basic for $G$

(vi) $\text{NormalForm(NormalForm}(f, G \setminus \{f\}), G \cup D) = 0$ for each $f \in G$
Main theorem

Let \((G, D)\) be a partial Gröbner pair for \(I\).
If \(D = \emptyset\), then \(G\) is a Gröbner Basis for \(I\).

The Gröbner basis algorithm starts with

- a finite set \(G\) forming a basis of \(I\) and with
- the basic set \(D\) determined by the proposition.
4. Gröbner algorithm

Let \((G, D)\) be a partial Gröbner pair for \(I\). The four steps below compute a new partial Gröbner pair \((G', D')\) for \(I\).

1. Move one polynomial \(f\) from \(D\) to \(G\). Write \(G = \{g_1, \ldots, g_{N-1}, g_N = f\}\).

2. Compute the basic obstructions \(b\) of \(G\) involving \(f\). Update \(D\) with the non-zero \(\text{NormalForm}(b, G \cup D)\). The new \(D\) is a basic set for the new \(G\).

3. For each \(i \leq N - 1\) compute \(g'_i = \text{NormalForm}(g_i, G \setminus \{g_i\})\).
   If \(g'_i = 0\) remove \(g_i\) from \(G\). Otherwise, if \(g'_i \neq g_i\),
   (a) replace \(g_i\) by \(g'_i\);
   (b) compute the basic obstructions of the new \(G\) involving \(g'_i\);
   (c) if \(\text{NormalForm}(b, G \cup D) \neq 0\) for such an obstruction \(b\), add it to \(D\).

4. Replace each \(d \in D\) by \(\text{NormalForm}(d, (G \cup D) \setminus \{d\})\).
Termination

Repeat the four steps until termination, if ever.

If $D = \emptyset$, then the routine terminates and $G$ is a Gröbner basis for $I$.

$k\langle T \rangle$ is not Noetherian.
Dimensions of quotient algebras

Obtained by finding those monomials that are not contained in the order ideal of leading terms of the Gröbner basis.

Example: Coxeter group of type $W(E_6)$ and order 51840

There exists a growth rate version.
5. Examples

\[ G = [xy - x, yx - y] \]

\[ \text{NormalForm}(s(1, 1, x; x, 2, 1), G) = x^2 - x \text{ \hspace{1em}} [xyx] \]

\[ \text{NormalForm}(s(y, 1, 1; 1, 2, y), G) = y^2 - y \text{ \hspace{1em}} [yxy] \]

\[ G \cup [x^2 - x, y^2 - y] \text{ is a Gröbner basis.} \]
Loading GBNP 0.9.2 (Non-commutative Gröbner bases)

G1 := [[[1,2],[1]],[1,-1]]; G2 := [[[2,1],[2]],[1,-1]]; KI:=[G1,G2];

PrintNPList(KI);
xy - x, yx - y

GB := SGrobnerTrace(KI); PrintNPListTrace(GB);
x^2 - x, xy - x, yx - y, y^2 - y

PrintTraceList(GB);
- G(1)x + G(1) + xG(2), G(1), G(2), yG(1) - G(2)y + G(2)

Script done on Wed 27 Dec 2006 02:56:18 PM CET
Tracing example

In BMW algebra, for the 21-st Gröbner elt:

\[
GB_{21} = g_{2}g_{1}e_{2} - e_{1}e_{2} \\
= \frac{11}{78}G(1)g_{1}e_{2} - \frac{11}{78}g_{1}G(1)e_{2} + \frac{11}{78}e_{1}g_{2}G(1)g_{2}g_{1} - \frac{77}{78}G(1)g_{2}g_{1}e_{2} - \frac{121}{78}G(1)g_{2}g_{1} \\
- \frac{11}{78}e_{1}g_{2}g_{1}G(2) - \frac{7}{78}e_{1}G(2)g_{1}e_{2} + \frac{77}{78}g_{2}g_{1}G(2)e_{2} - \frac{77}{78}g_{2}g_{1}G(2)e_{2} + \frac{121}{78}g_{2}g_{1}G(2) \\
+ \frac{121}{546}e_{1}g_{2}G(4)g_{2} + \frac{121}{78}e_{1}g_{2}G(4) - \frac{121}{78}G(4)g_{2}e_{2} - \frac{847}{78}G(4)e_{2} \\
+ \frac{121}{546}e_{1}g_{2}g_{1}G(4) - \frac{1331}{546}G(4)g_{2} - \frac{121}{78}g_{1}G(4)e_{2} - \frac{1331}{78}G(4) \\
- \frac{1331}{546}g_{1}G(4) + \frac{11}{78}G(7)e_{2} - \frac{121}{78}g_{2}g_{1}g_{2}G(8) - \frac{11}{78}g_{2}gG(8) \\
- \frac{11}{78}G(10)g_{2}g_{1} + \frac{7}{78}e_{1}G(11)
\]

Script done on Sun 07 Jan 2007 06:28:39 PM CET
A recent satisfied customer, Thu, 28 Dec 2006 10:35:31

I’ve been trying to compute a quotient algebra with GAP and your package for non-commutative Groebner bases.

The generating vector space is 10 dimensional and the relations are homogeneous quadratic (the file with relations is sent as an attachment).

The Groebner package does an impressive work for computing the Groebner basis, at least in comparison with other programs I’ve tried before, most notably × × × ×.

Leandro Vendramin

The dimension of the quotient algebra is: 8,294,400
\times \times \times \times \in \{\text{Bergman, Opal, Plural}\} \setminus \{GBNP\}
An earlier satisfied customer

Input is $aaab - \frac{651}{25}aba + \frac{651}{25}abaa - baaa,$
$bbba - \frac{651}{25}bbab + \frac{651}{25}babb - abbb$

Wanted: dimensions of homogeneous parts

Number of found Grobner Basis elements is 29

List of dimensions by degree:
$[ 1, 2, 4, 8, 14, 24, 40, 64, 100, 154, 232, 344, 504, 728, 1040, 1472, 2062 ]$

Cumulative list of dimensions by degree:
$[ 1, 3, 7, 15, 29, 53, 93, 157, 257, 411, 643, 987, 1491, 2219, 3259, 4731, 6793 ]$

The computation took 33667272 msecs.
The customer’s reaction, Thu Apr 17 23:19:25 2003

It ended up having a large impact. See the attached paper; joint with Tatsuro Ito.

I spent several weeks in Japan this past January, working with Tatsuro and trying to find a good basis for the algebra on two symbols subject to the q-Serre relations. After much frustration, we thought of feeding your data into Sloane’s online handbook of integer sequences. We did it out of curiosity more than anything; we did not expect the handbook data to be particularly useful. But it was.

The handbook told us that the graded dimension generating function, using your data for the coefficients, matched the q-series for the inverse of the Jacobi theta function \( \vartheta_4 \); armed with this overwhelming hint we were able to prove that the graded dimension generating function was indeed given by the inverse of \( \vartheta_4 \). With that info we were able to get a nice result about tri-diagonal pairs.

Paul Terwilliger
6. Conclusion

- No termination guarantee in general
- If there exists a finite Gröbner basis, it can be found by effective means
- Useful for Todd-Coxeter type algorithms for algebras
- Useful for proving identities in finitely presented algebras
- Useful for equation solving?
- Implementation in GAP Package GBNP
  [http://www.win.tue.nl/~amc/pub/grobner/chap0.html](http://www.win.tue.nl/~amc/pub/grobner/chap0.html)
Finish

- Next lecture on graph non-isomorphism
- Uses permutation group algorithms and focuses on proof production
- Thursday’s lecture on algebras for knot theory and other rewriting systems
References


