ALGORITHMS FOR LIE ALGEBRAS AND ASSOCIATIVE ALGEBRAS

ARJEH M. COHEN

Abstract. We discuss some methods for computing with Lie and with associative algebras. We begin with Gröbner bases and demonstrate how to find these with the GAP package GBNP. For Lie algebras, we discuss the construction of a Chevalley basis in $L$, which is particularly difficult in the most useful and interesting cases: those of characteristics 2 and 3.

Ado’s Theorem, stating that a finite-dimensional Lie algebra $L$ embeds in the Lie algebra of a finite-dimensional associative algebra $A$ (that is, the Lie algebra on the vector space $A$ with bracket $ab - ba$ for $a, b \in A$), gives a link between Lie algebras and associative algebras. We will give some examples where this observation has been helpful in that associative algebra algorithms were used for proving statements about Lie algebras.

This is the content of a colloquium talk at Münster, May 29, 2008.
1. Associative algebra

1.1. Commutative algebra. We briefly recall the commutative polynomial case where the Buchberger algorithm solves the word problem, that is, the quest for an algorithm to decide whether two given polynomials represent the same element of the quotient modulo a given ideal. The algorithm finds a suitable generating set for the ideal in a sense to be made precise below.

Let $F$ be a field and let $B$ be a finite subset $B$ of $F[X]$, the polynomial ring in the (finite number of) variables $x \in X$. We are interested in the ideal $(B)$ of $F[X]$ generated by $B$. The following algorithm finds a reduced form of $f \in F[X]$ with respect to $B$ in a finite number of steps—that is, an element representing the same element as $f$ in $F[X]/(B)$, but of as ‘small’ as we can get it by elementary operations. Here, small is measured by an ordering on monomials with suitable properties (called a reduction ordering), which refines the partial ordering by division.

**Reduction Algorithm**  Given $B \subset F[X]$ (finite) reduce $f \in F[X]$.

```plaintext
Reduce(f, B) =
  while $\exists b \in B : \text{lm}_b | \text{lm}_f$ do
    $f := f - (\text{lt}_f / \text{lt}_b)b$
  od;
  return $f$
```
If \( \text{Reduce}(f, B) = 0 \) for each \( f \in (B) \), then \( B \) is called a Gröbner basis. If \( B \) is a Gröbner basis, then the word problem for \( F[X]/(B) \) is solvable as then \( \text{Reduce}(g, B) = \text{Reduce}(h, B) \) if and only if \( g + (B) = h + (B) \).

A Gröbner basis is the kind of suitable generating set referred to above. Below is a version of the Buchberger algorithm for finding such a generating set with respect to a given reduction ordering. It needs the notion of S-polynomial. For \( f, g \in F[X] \),

\[
S(f, g) = \begin{cases} 
0 & \text{if } f = 0 \text{ or } g = 0 \\
\frac{\text{lt}_g}{\text{gcd}(\text{lm}_f, \text{lm}_g)} f - \frac{\text{lt}_f}{\text{gcd}(\text{lm}_f, \text{lm}_g)} g & \text{otherwise}
\end{cases}
\]
Gröbner Basis Algorithm. Given a finite subset $B$ of $\mathbb{F}[X]$, return a Gröbner basis of $(B)$.

$\text{GrobnerBasis}(B) =$

$$D := \{\text{Reduce}(S(f, g), B) \mid f, g \in B\} \setminus \{0\};$$

while $D \neq \emptyset$ do

choose $g \in D$;

$D := D \setminus \{g\};$

$D := \{\text{Reduce}(s, B) \mid s \in D\} \setminus \{0\};$

$D := D \cup \{\text{Reduce}(S(f, g), B \cup \{g\}) \mid f \in B\} \setminus \{0\};$

$B := B \cup \{g\}$;

od; return $B$.

Theorem 1.1.1. For each finite $B \subset \mathbb{F}[X]$, the algorithm $\text{GrobnerBasis}(B)$ computes a Gröbner basis of $(B)$. 
1.2. Insolubility. By $\mathbb{F}(X)$ we denote the noncommutative version. The ring is no longer Noetherian: the chain

$$(\{xyx\}, \ldots, (\{xyx, \ldots, xy^i x\}), \ldots)$$

of ideals of $\mathbb{F}(x, y)$ is infinite and strictly ascending. Also, the word problem in finitely presented semigroups is insoluble.

Since a semigroup presentation can be given in terms of noncommutative binomials, this implies that there is no algorithm solving the word problem for the quotient of $\mathbb{F}(X)$ by a finitely generated ideal.
1.3. Gröbner bases. Yet the theory of Gröbner bases is not completely lost. Fix a well-founded reduction ordering on noncommutative monomials. The Reduce and Gröbner basis \( B \) of an ideal \( I \) as before: for each \( f \in I \) we have \( \text{Reduce}(f, B) = 0 \).

**Theorem 1.3.1.** If \( B \subset \mathbb{F}\langle X \rangle \) is finite and there is a finite Gröbner basis of \( (B) \), then this basis can be found by means of the algorithm to be described.

Let \( B \) be a finite subset of \( \mathbb{F}(X) \). We take all polynomials in \( B \) to be monic. An obstruction for \( B \) is a sextet \( s = (l, f, r; \lambda, g, \rho) \) where \( f, g \in B \) and \( l, r, \lambda, \rho \) are monomials such that \( \text{lt} fr = \lambda \text{lt} g \rho \). The S-polynomial of the obstruction \( s \) is

\[
S(s) = lfr - \lambda g \rho.
\]

In general, the set of all obstructions is infinite. But, a finite \( Q \) can be pointed out such that \( \text{Reduce}(S(s), B \cup Q) = 0 \) for any obstruction \( s \) for \( B \). We call \( Q \) a set of basic obstructions for \( B \).
Let $I$ be a two-sided ideal of $\mathbb{F}(X)$ and let $B, D$ be finite subsets of $\mathbb{F}(X)$. We say that $(B, D)$ is a partial Gröbner pair for $I$ if the following properties are satisfied.

1. All polynomials in $B \cup D$ are monic.
2. $I = (B)$.
3. For each $d \in D$ we have $\text{Reduce}(d, B) = d \in I$.
4. The set $D$ is basic for $B$.

**Corollary 1.3.2.** Let $I$ be a two-sided ideal of $\mathbb{F}(X)$ and let $(B, D)$ be a partial Gröbner pair for $I$. If $D$ is the empty set, then $B$ is a Gröbner Basis for $I$. 
The Gröbner basis algorithm will start with a finite set $B$ forming a basis of $I$ and with $D$ a basic set (easily determined; details omitted). Observe that $(B, D)$ is indeed a partial Gröbner pair.

The main ingredient of the algorithm is an iteration step that changes the pair $(B, D)$ to another partial Gröbner pair $(B', D')$ such that the ideal generated by the leading monomials of $B'$ strictly contains the ideal generated by the leading monomials of $B$. As the non-commutative polynomial ring $\mathbb{F}(X)$ is not Noetherian, we cannot expect the algorithm to terminate in all cases. Termination occurs when $D = \emptyset$ so that $B$ is a Gröbner basis of $I$, by Corollary 1.3.2. In the iteration step one element from $D$ is moved to $B$ and care is taken to let the new pair become partial Gröbner again.

**Theorem 1.3.3.** Let $I$ be an ideal of $\mathbb{F}(X)$ and let $(B, D)$ be a partial Gröbner pair for $I$. A routine similar to the commutative case computes a new partial Gröbner pair $(B', D')$ for $I$ with the property that the leading monomials of $B$ generate an ideal strictly contained in the ideal generated by the leading monomials of $B'$. If $D' = \emptyset$, the routine halts and $B'$ is a Gröbner basis for $I$. 
1.4. GBNP. The noncommutative Gröbner basis algorithm is implemented in GAP, in a package called GBNP. This package also deals with

- truncated versions for homogeneous polynomials
- dimension growth of quotient algebras (and finite-dimensionality tests)
- traced versions
- module determination by generating vectors with prescribed annihilators.
1.5. **Examples.** Two demos.

A construction of a particular representation for $\text{PSL}(2,13)$. Starting from the presentation [Kantor, Seress et al.]

\[
<u, t \mid u^3 t^2 = (tu)^7 = (tu^2(tu)^2)^{13} = (tu^2(tu)^2 t)^3 = ((tu^2(tu)^2)^4 t(tu^2(tu)^2)^7 t)^2 = 1 >
\]

we find matrices for a particular 14-dimensional representation by spinning a module from a vector annihilated by

\[p - 1 \text{ and } z^2 + z + 1,\]

where

\[
p := tu^2(tu)^2,
\]

\[
z := (tu)^3 tu^2 tu(tu)^3 tu(tu)^2.
\]
The universal enveloping algebra of a Lie algebra. Consider the Lie algebra with generators $e$, $f$, and $h$, and relations
\[
e^2f - 2efe + fe^2 + 2e = 0 \\
-ef^2 + 2fee - f^2e - 2f = 0
\]
This is the well-known Lie algebra $\mathfrak{sl}_2(\mathbb{F})$. We construct the corresponding universal enveloping algebra of this Lie algebra and show how one can prove that $f^2$ belongs to the ideal generated by $e^2$ in that associative algebra. Let $A = \mathbb{F}(e, f, h)$. Enter the relations
\[
f e - e f + h, \quad h e - e h - 2e, \quad h f - f h + 2f.
\]
Turns out to be a Gröbner basis.

Now add the relation $e^2 = 0$ and compute a Gröbner basis with trace. Find proof of $f^2 = 0$. 

2. Lie algebra


Example Three kinds.

- \textit{Lie}(A) for $A$ an associative algebra. In particular $\mathfrak{gl}(V) = \text{Lie}(\text{End}(V))$.
- \textit{Lie}(G) for $G$ an algebraic group. Examples
  - $\mathfrak{gl}_n(\mathbb{F}) = \mathfrak{gl}(\mathbb{F}^n) = \text{Lie}(\text{GL}_n(\mathbb{F}))$.
  - $\mathfrak{sl}_n(\mathbb{F}) = \mathfrak{sl}(\mathbb{F}^n) = \text{Lie}(\text{SL}_n(\mathbb{F}))$.
- \textit{Der}(A) for $A$ any algebra. For instance, if $A = \mathbb{F}[z]$, we find $\text{Der}(A)$ to be the Lie algebra spanned by $z^i \partial_z$ and Lie bracket
  \[ [z^i \partial_z, z^j \partial_z] = (j - i)z^{i+j-1} \partial_z, \]

A representation of $L$ is a homomorphism $L \rightarrow \mathfrak{gl}(V)$. Extends to an associative algebra representation $U(L) \rightarrow \mathfrak{gl}(V)$. 

Lemma 2.1.1. Left multiplication by $x \in L$, denoted $\text{ad}_x$, is a derivation of $L$, giving a representation $\text{ad} : L \to \mathfrak{gl}(L)$.

Universal enveloping algebra $U(L)$ of a Lie algebra $L$: this is the quotient of the tensor algebra $\mathbb{F}\langle X \rangle$, for $X$ the coordinate functions on $L$, modulo the ideal generated by all

$$xy - yx - [x, y] \quad \text{for} \quad x, y \in L.$$

Theorem 2.1.2 (Ado). The Lie algebra $L$ embeds naturally into $\mathbf{Lie}(U(L))$.

Theorem 2.1.3 (Apel, PBW). The above set of relations in $\mathbb{F}\langle X \rangle$ is a Gröbner basis.
Presentation on computer by
• generators and relations (Van Leeuwen, De Graaf, Gerdt & Kornyak)
• generating matrices inside \(\text{gl}(V)\)
• multiplication table

**Example**  \(\mathfrak{sl}_2 = F e + F f + F h\) with

\[
[e, f] = h, \quad [h, e] = 2e, \quad [h, f] = -2f.
\]

Realized by

\[
e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.
\]

Connection with previous relations given by substitution of \(ef - fe\) for \(h\) (data from first equation). Then the other two equations become

\[
[h, e] = 2e \quad \Rightarrow \quad fe^2 - 2efe + e^2 f = (ef - fe)e - e(ef - fe) = 2e
\]

\[
[h, f] = -2f \quad \Rightarrow \quad ef^2 - 2fe f + f^2 e = (ef - fe)f - f(ef - fe) = -2f
\]
2.2. Classical Lie algebras. A classical Lie algebra is the Lie algebra of a linear algebraic group. Think of a subgroup of $\text{GL}(V)$ given by polynomial equations. A typical example is

$$\text{SL}(V) = \{ x \in \text{GL}(V) \mid \det(x) = 1 \}. $$

Then

$$\mathfrak{sl}(V) = \text{Lie}(G) = \{ X \in \mathfrak{gl}(V) \mid \det(1 + X) = 1 \}$$

$$= \{ X \in \mathfrak{gl}(V) \mid \text{trace}(X) = 0 \}. $$
2.3. **Extremal elements.** $x \in L$ is called extremal if $[x, [x, L]] \subseteq \mathbb{F}x$.

$x \in L$ is called a sandwich if $[x, [x, L]] = \{0\}$.

**Example**  
$x, y \in \mathfrak{sl}_2$ are extremal elements, but not sandwiches.

**Example**  
The Witt algebra $W$ over $\mathbb{F}$ of characteristic 5 and of dimension 5 can be defined as follows. As a vector space $W$ has basis $z^i \partial_z$, for $i = 0, \ldots, 4$. The Lie bracket is defined on two of these elements by

$$[z^i \partial_z, z^j \partial_z] := (j - i) z^{i+j-1} \partial_z,$$

with the convention that

$$z^k := 0 \text{ whenever } k \notin \{0, \ldots, 4\}.$$

Now $z^4 \partial_z$ is a sandwich and $x = z^2 \partial_z$ is extremal but not a sandwich in $W$. 
Lemma 2.3.1. Suppose \( \mathfrak{sl}_2 \cong S \leq L \) and \( x \in S \) is extremal in \( L \). Then \( \text{ad}_x^2(L/S) = 0 \).

Theorem 2.3.2 (Kostrikin, Premet, 1987). If \( F = F \) and \( L \) is simple, then \( L \) has a nontrivial extremal element.
Theorem 2.3.3 (Premet, AMC, Ivanyos, Roozemond, 2007). If $p \neq 2, 3$ and $L$ is simple and has an extremal element that is not a sandwich, then

- either $p = 5$ and $L$ is isomorphic to $W$,
- or $L$ is generated by extremal elements.

About the proof. Suppose $x \in L$ is extremal. By Jacobson-Morozov, we can find $y \in L$ with $\langle x, y \rangle \cong \mathfrak{sl}_2(\mathbb{F})$. Consider $L$ as a module on which $S$ acts. Obviously $S$ is an invariant subspace, so $L/S$ is an $S$-module.

Claim. $\text{ad}_y$ acts quadratically on $L/S$, i.e., $\text{ad}_y^2(L/S) = 0$.

Proof (of the claim). Write $e, f$ for the action of $\text{ad}_x, \text{ad}_y$, respectively, on $L/S$. By Lemma 2.3.1, $e^2 = 0$. We list the known relations for $e$ and $f$, and the quadraticity of $e$ that we just found.

\begin{align*}
(1) & \quad e^2f - 2efe + fe^2 + 2e = 0 \\
(2) & \quad -ef^2 + 2fef - f^2e - 2f = 0 \\
(3) & \quad e^2 = 0 \\
(4) & \quad efe - e = 0.
\end{align*}

(1) and (3) immediately imply

\begin{align*}
(5) & \quad e^2f = 0.
\end{align*}

Denote by $R_2$ the left hand side of the second relation. Then, by the third,

\begin{align*}
0 & = fR_2fe - fefR_2 + 2f^2eR_2 - R_2fef + efR_3f - 3fR_2f \\
& \quad -2fefR_2f + 3R_2f - 2fefR_2f - 6R_2f + 2eR_3f^2 \\
& = 12f^2 - 3ef^3 + 7fef^2 - 5f^2ef + f^3e + 3eef^3 \\
& \quad -7eefef^2 + 5f^2eef - f^3eef.
\end{align*}

Replacing $efe$ by $e$ and $e^2$ by 0, using the fourth and third relation, we find

\begin{align*}
0 & = 12f^2 - 3ef^3 + 7fef^2 - 5f^2ef + f^3e + 3eef^3 \\
& \quad -7eefef^2 + 5f^2eef - f^3e \\
& = 12f^2.
\end{align*}

As $p \neq 2, 3$, we conclude that $f^2 = 0$. 
2.4. **Algorithms for classical Lie algebras.** In particular reductive ones. Dynkin diagram determines a Cartan matrix $C$.

**Example**

\[
C(A_3) = \begin{pmatrix}
2 & -1 & 0 \\
-1 & 2 & -1 \\
0 & -1 & 2
\end{pmatrix}
\]  
for $\mathfrak{sl}(4(F))$

and

\[
C(B_3) = \begin{pmatrix}
2 & -1 & 0 \\
-1 & 2 & -1 \\
0 & -2 & 2
\end{pmatrix}
\]  
for orthogonal groups in dimension 7.

**Lemma 2.4.1.** Spin versions correspond to factorizations $C = A^T B$

with factors having integer entries.

**Example**

\[
det (C(A_3)) = 4. 
\text{Factorizations}
\]

- $A = l_3$, $B = C$
- $A = C^T$, $B = l_3$
- $A^T = \begin{pmatrix}
1 & 0 & 0 \\
-1 & 1 & 0 \\
-1 & 0 & 2
\end{pmatrix}$  
  $B = \begin{pmatrix}
2 & -1 & 0 \\
1 & 1 & -1 \\
1 & -1 & 1
\end{pmatrix}$.

\[
det (C(B_3)) = 2. 
\text{Factorizations}
\]

- $A = l_3$, $B = C$
- $A^T = C$, $B = l_3$
Definition: The pair \((A, B)\) is the root datum for \(G\).

Idea: columns \(\alpha_i\) of \(A\) and columns \(\alpha_j^*\) of \(B\) form bases for a pair of root systems in duality:

- \(s_i : x \mapsto x - (x^T \alpha_i^*) \alpha_i\) are reflections acting on \(\mathbb{Z}^n\).
- The \(s_i (i = 1, \ldots, n)\) generate a finite group \(W\).
- Let \(\Phi\) be the union of \(W\)-orbits of \(\alpha_i\).
- The map \(\alpha_i \mapsto \alpha_i^*\) extends to a correspondence \(\alpha \in \Phi \mapsto \alpha^* \in \Phi^*\).

Then \(L = \text{Lie}(G)\), for \(G\) a split reductive algebraic group, has a commutative split toroidal subalgebra \(H \cong \mathbb{Z}^n \otimes \mathbb{Z} F\). Such an \(H\) is called a split Cartan subalgebra. All split cartan subalgebras are \(G\)-conjugate. There is a direct sum decomposition

\[
L = H \oplus \sum_{\alpha \in \Phi} F X_\alpha
\]

for certain vectors \(X_\alpha\). The multiplication is given by the following rules, where \(\alpha, \beta \in \Phi\) and \(y, z \in \mathbb{Z}^n\) and \(N_{\alpha, \beta}\) are integral structure constants.

\[
[y, z] = 0,
[y, X_\beta] = (\beta, y) X_\beta,
[X_\alpha, X_\beta] = \begin{cases} 
N_{\alpha, \beta} X_{\alpha + \beta} & \text{if } \alpha + \beta \in \Phi, \\
\alpha^* & \text{if } \beta = -\alpha, \\
0 & \text{otherwise.}
\end{cases}
\]

A root is long if it is conjugate to an \(\alpha_i\) for \(i\) in long part of the Dynkin diagram.
Corollary 2.4.2. $X_\alpha$ for $\alpha$ a long root in $\Phi$ is an extremal element.

Lemma 2.4.3. Root datum determines $\text{Lie}(G)$ precisely up to isomorphism.
2.4.1. Finding Cartan subalgebras. $\mathbb{F} = \mathbb{F}_q$. Now $|L| = q^n$. Finding a split Cartan subalgebra is done by a Las Vegas algorithm.

A Las Vegas algorithm is an algorithm that may either return failure or be successful. It is successful with a specified probability. The art is to find an algorithm with a good running time.

Solution (rough version): There are small constants $c, c_i \in \mathbb{N}$ such that there are at least

$$|L| \cdot \left(1 - \sum_{i=1}^{n} \frac{c_i}{q^i}\right) \left(1 - \frac{1}{q}\right)^{a} \frac{1}{c}$$

(regular semi-simple) elements in $L$ whose centralizers in $L$ are split Cartan subalgebras.
2.5. **Chevalley bases.** Suppose we are given a split Cartan subalgebra $H$. How to find a Chevalley basis with respect to this $H$? Not so hard in general:

- Find simultaneous eigenspaces for $\{\text{ad}_h \mid h \in H\}$. These give $FX_\alpha (\alpha \in \Phi)$.
- Scale these spaces to find $X_\alpha$.

Hard cases identified.

**Example**  $L$ of type $A_2^{sc}$ and $\mathbb{F}$ of characteristic 3. $\dim (L) = 8 = 2 + 3 + 3$:

$$C(A_2) = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

Now $\alpha_1 = (-1, -1) = \alpha_2 = - (\alpha_1 + \alpha_2)$ so root $\alpha_1$ occurs with multiplicity 3.

Same for $-\alpha_1$.

Trick: $\text{Der}(L)$ is of type $G_2$, dimension 14. More structure available. Chevalley basis for $\text{Der}(L)$ leads to Chevalley basis for $L$. 
2.6. **Application: effective Sylow theorems.** Lie algebra analysis of use to finite Chevalley groups: that is the $\mathbb{F}_q$ rational points $G(\mathbb{F}_q)$ of a simple algebraic group $G$.

Many of the finite simple groups are (almost) of the form $G(\mathbb{F}_q)$.

Problem: Suppose given two Sylow $r$-subgroups of $G(\mathbb{F}_q)$, find an element of $G(\mathbb{F}_q)$ conjugating one to the other.

Idea of solution

- WLOG $\gcd(r, q) = 1$.
- Each Sylow occurs in a canonical Cartan subalgebra (well controled field-twisted version of a split cartan subalgebra).
- Find a Cartan subalgebra in the fixed point space of the $r$-torsion of the center of the Sylow subgroup.
- Find the corresponding Chevalley basis
- The basis transformation from standard Chevalley basis to new Chevalley basis is an element of $\text{Aut}(L)$.
- Move a little in the normalizer of the canonical Cartan subalgebra to get this element in $G(\mathbb{F}_q)$.
Conclusion: two variations on classical algorithms.

- Gröbner bases for noncommutative polynomials (GBNP) very useful for group theory and Lie algebra theory.
  No termination guarantee
- Lie algebra algorithms intriguing and useful for finite simple groups.
  Las Vegas

Based on joint work with Dié Gijsbers, Maxim Hendriks, Gábor Ivanyos, Jan Willem Knopper, Dan Roozemond.

Danke schön