ON THE COMPLEXITY OF LIE ALGEBRAS

Hans F. de Groote[1], Joos Heintz[1,2]
Stefan Möhler[1], and Heinz Schmidt[1]

1 J.W. Goethe - Universität
Fachbereich Mathematik
Robert-Mayer - Str. 6-10
D-6000 Frankfurt/Main 1
F R G

2 Consejo Nacional de Investigaciones
Científicas y Técnicas (CONICET)
Departamento de Matemáticas de la
Universidad Nacional de La Plata
La Plata, Pcia. de Buenos Aires
Argentina

1. Introduction

Some general notions from complexity theory. Complexity of Lie algebras

Let U,V,W be finite dimensional vector spaces over a field k and let $\Phi : U \times V \to W$ be a bilinear mapping. The (multiplicative) complexity $L(\Phi)$ of Φ is defined as the least $r \in \mathbb{N}$ such that there are linear forms $u_1,\ldots,u_r$, $v_1,\ldots,v_r \in (U \times V)^*$ and elements $w_1,\ldots,w_r \in W$ satisfying

$$\Phi(x,y) = \sum_{\rho=1}^{r} u_\rho(x,y)\ v_\rho(x,y)\ w_\rho \qquad \text{for all } (x,y) \in U \times V .$$

The r-tuple $((u_\rho,v_\rho,w_\rho) \in (U\times V)^* \times (U\times V)^* \times W,\ 1 \le \rho \le r)$ is then called an optimal *quadratic algorithm* for Φ.

$L(\Phi)$ is the number of non linear arithmetic operations that are necessary and sufficient to compute $\Phi(x,y)$ from x,y by a straight line program (cf. [Strassen 1973] and [de Groote 1987] for further details).

We shall use a somewhat coarser but more feasible computational model:

A *bilinear algorithm* for Φ is an r-tuple

$$\beta = ((u_\rho,v_\rho,w_\rho) \in U^* \times V^* \times W,\ 1 \le \rho \le r) \qquad \text{with the property that}$$

$$\Phi(x,y) = \sum_{\rho=1}^{r} u_\rho(x)\ v_\rho(y)\ w_\rho \qquad \text{for all } (x,y) \in U \times V .$$

Writing $L(\beta) := r$ for the *length* of β,

$$R(\Phi) := \min \{ L(\beta) ;\ \beta \text{ bilinear algorithm for } \Phi \}$$

is called the *bilinear complexity* or *rank* of Φ [Strassen 1973].

In case $L(\beta) = R(\Phi)$ we call β an optimal bilinear algorithm for Φ.

Obviously we have $L(\Phi) \leq R(\Phi)$, and it is easy to see that $R(\Phi) \leq 2\,L(\Phi)$. Hence the complexity measures $L(\Phi)$ and $R(\Phi)$ have the same size.

The main theme of the complexity theory of bilinear mappings, e.g. the multiplication in algebras, is the determination of *lower bounds* for $L(\Phi)$ and $R(\Phi)$.

Another problem, closely related to the rank problem for bilinear mappings, is the determination of the *isotropy group* of a given bilinear mapping.
Isotropy groups belong to the decisive tools in the investigation of varieties of *all* optimal algorithms for bilinear mappings (cf. [de Groote 1978]).

Let $GL(U)$, $GL(V)$, $GL(W)$ be the groups of k-linear automorphisms of U , V , W respectively. Then the group of all $\phi^* \otimes \psi^* \otimes \chi \in GL(U^* \otimes V^* \otimes W)$ with $\phi \in GL(U)$, $\psi \in GL(V)$, $\chi \in GL(W)$ such that

$$\Phi(x,y) = \chi(\Phi(\phi(x),\psi(y))) \qquad \text{for all } (x,y) \in U \times V$$

is called the *proper isotropy group* of Φ and denoted by $\Gamma(\Phi)$ (cf. [de Groote 1978]). (Here we write ϕ^*,ψ^* for the dual mappings of ϕ , ψ.)

The elements of $\Gamma(\Phi)$ transform bilinear algorithms for Φ of length r into bilinear algorithms of the same length :
Let $\beta = ((u_\rho, v_\rho, w_\rho) \in U^* \times V^* \times W ,\ 1 \leq \rho \leq r)$ be a bilinear algorithm for Φ of length r . Then for $(x,y) \in U \times V$ we have

$$\Phi(x,y) = \sum_{\rho=1}^{r} u_\rho(x)\, v_\rho(y)\, w_\rho = \chi(\Phi(\phi(x),\ \psi(y)))$$

$$= \sum_{\rho=1}^{r} u_\rho(\phi(x))\, v_\rho(\psi(y))\, \chi(w_\rho) = \sum_{\rho=1}^{r} \phi^*(u_\rho)(x)\ \psi^*(v_\rho)(y)\ \chi(w_\rho) .$$

So, $((\phi^*(u_\rho), \psi^*(v_\rho), \chi(w_\rho)) \in U^* \times V^* \times W ,\ 1 \leq \rho \leq r)$ is a new bilinear algorithm for Φ of length r .

In particular, $\Gamma(\Phi)$ can be considered as a group operating on the variety A_Φ of optimal algorithms for Φ .

Let $r := R(\Phi)$ and denote by S_r the symmetric group of permutations of r elements.
For any optimal algorithm $\beta = ((u_\rho, v_\rho, w_\rho) \in U^* \times V^* \times W ,\ 1 \leq \rho \leq r)$ for Φ and any $\pi \in S_r$, $\beta_{\pi^{-1}} := ((u_{\pi(\rho)}, v_{\pi(\rho)}, w_{\pi(\rho)}) \in U^* \times V^* \times W ,\ 1 \leq \rho \leq r)$ is also an optimal algorithm for Φ . Hence S_r operates on A_Φ . Looking at $\Gamma(\Phi)$ as a group acting on A_Φ , we see that S_r and $\Gamma(\Phi)$ commute elementwise. The compositum of S_r and $\Gamma(\Phi)$ is called the *extended isotropy group* of Φ (cf. [de Groote 1978]).

In this paper we extend the results of [de Groote - Heintz 1986] on the complexity of certain classes of Lie algebras.

A *Lie algebra* over a field k is a (finite dimensional) k-vector space g, together with a bilinear mapping $(X,Y) \mapsto [X,Y]$ from $g \times g$ to g such that

(i) $[X,X] = 0$ for all $X \in g$ and

(ii) $[X,[Y,Z]] + [Y,[Z,X]] + [Z,[X,Y]] = 0$ for all $X,Y,Z \in g$.

The rank of the bilinear mapping $(X,Y) \mapsto [X,Y]$, which we consider as a bilinear mapping $[,] : g \times g \to [g,g]$, is called the rank of g, and we denote it by $R(g)$. The notions "bilinear algorithm for g" and "isotropy group of g" always refer to the bilinear map $(X,Y) \mapsto [X,Y]$. The proper isotropy group of g is denoted by $\Gamma(g)$.

From now on let k be algebraically closed and of characteristic 0, for simplicity: $k = \mathbf{C}$.
Lie algebras we are going to consider mostly are *semisimple* or *Borel subalgebras* of semisimple Lie algebras over $\mathbf{C}$. Specific attention will be paid to the case of *simple Lie algebras*. (We will freely use definitions and results from Lie algebra theory and recommend [Humphreys 1980] and [Goto - Grosshans 1978] as references.)

2. Complexity and rank of classical simple Lie algebras and their Borel subalgebras

Let g be a simple Lie algebra over $\mathbf{C}$ with $n := \dim_{\mathbf{C}} g$, Cartan subalgebra h and $\ell := \dim_{\mathbf{C}} h$. (Usually, ℓ is called the rank of g. However we will use "rank of g" only in the sense of complexity theory.)

Let g be a *classical simple Lie algebra*, i.e.

$g := sl(\ell+1,\mathbf{C})$ with Dynkin diagram A_ℓ ($\ell \geq 1$),
$g := o(2\ell+1,\mathbf{C})$ with Dynkin diagram B_ℓ ($\ell \geq 2$),
$g := sp(2\ell,\mathbf{C})$ with Dynkin diagram C_ℓ ($\ell \geq 3$),
or $g := o(2\ell,\mathbf{C})$ with Dynkin diagram D_ℓ ($\ell \geq 4$).

Concerning the complexity $L(g)$ we have the following lower bounds:

Theorem 1

(i) $L(sl(\ell+1,\mathbf{C}) \geq 2n - 2\ell$,
(ii) $L(o(2\ell+1,\mathbf{C}) \geq 2n - 4\ell + 2$,
(iii) $L(sp(2\ell,\mathbf{C}) \geq 2n - 4\ell + 2$,
(iv) $L(o(2\ell,\mathbf{C}) \geq 2n - 4\ell + 4$.

Unfortunately, these lower bounds are unlikely to be reached.
For example, we have $L(sl(2,\mathbf{C}))=5$, whereas our lower bound is 4 in this case.
For the rank $R(g)$ our lower bounds are more realistic. However, we haven't yet results for $g = sp(2\ell,\mathbf{C})$.

Theorem 2

(*) $\quad R(g) \geq 2\dim_{\mathbf{C}} g - \dim_{\mathbf{C}} h = 2n - \ell$

for $g = sl(\ell+1,\mathbf{C})$, $g = o(2\ell+1,\mathbf{C})$, and $g = o(2\ell,\mathbf{C})$.
Moreover, we have $g = sl(2,\mathbf{C})$ iff equality holds in (*) .

In [de Groote - Heintz 1986] the problem to find lower bounds for the rank of a semisimple Lie algebra g is reduced to a purely algebraical counterpart, namely to find upper bounds for the dimension of so-called generic subalgebras of g .

A subalgebra a of g is called *generic* iff there exists an element $A_0 \in g$ such that $C_g(A_0) = C_g(a)$ (the *centralizer* $C_g(m)$ of $m \subseteq g$ is the set of all $X \in g$ that commute with m). A_0 is called a generic element of a . Generic subalgebras are abelian and a generic subalgebra with generic element A_0 is contained in the *double centralizer* $C_g^2(A_0) := C_g(C_g(A_0))$. $C_g^2(A_0)$, in turn, is a generic subalgebra with generic element A_0 . Thus we are left with the problem of estimating the dimension of double centralizers $C_g^2(A)$, $A \in g$.

In case $sl(\ell+1,\mathbf{C})$ we can use the classical double centralizer theorem

$$C^2_{gl(\ell+1,\mathbf{C})}(A_0) = \{ F(A_0) \; ; \; F \in \mathbf{C}[T] \} ,$$

T an indeterminate over $\mathbf{C}$ (cf. [Greub 1981], p. 422). Then it easily can be shown that for $A_0 \in sl(\ell+1,\mathbf{C})$

$$\begin{aligned} C^2_{sl(\ell+1,\mathbf{C})}(A_0) &= C^2_{gl(\ell+1,\mathbf{C})}(A_0) \cap sl(\ell+1,\mathbf{C}) \\ &= \{ F(A_0) \; ; \; F \in \mathbf{C}[T] , \; \sum_{i=1}^{\ell+1} F(\lambda_i) = 0 \} , \end{aligned}$$

where $\lambda_1,\ldots,\lambda_{\ell+1} \in \mathbf{C}$ are the (not necessarily distinct) eigenvalues of A_0 . Hence

$$\dim_{\mathbf{C}} C^2_{sl(\ell+1,\mathbf{C})}(A_0) \leq \ell .$$

From this we infer (*) in case $g = sl(\ell+1,\mathbf{C})$ (cf. [de Groote - Heintz 1986]).

In case $g = o(2\ell+1,\mathbf{C})$ or $g = o(2\ell,\mathbf{C})$ the proof that double centralizers $C_g^2(A_0)$ have dimension $\leq \ell$ is much more involved and relies essentially on the theory of elementary divisors for skew symmetric matrices over $\mathbf{C}$.

Theorem 3 Let $\mathcal{B}$ be a Borel subalgebra of a simple Lie algebra $\mathcal{g}$ with Cartan subalgebra h. Then

$$L(\mathcal{B}) \geq 2 \dim_{\mathbb{C}} [\mathcal{B},\mathcal{B}] - \dim_{\mathbb{C}} h \ .$$

The smallest Borel subalgebra among those mentioned in Theorem 3 is the non abelian two dimensional Lie algebra, the Borel subalgebra of $sl(2,\mathbb{C})$. Its structure can be generalized also in the following way:

Let $\mathcal{g}$ be a finite dimensional vector space and $\omega \in \mathcal{g}^*$ a non trivial linear form. Then

$$[X,Y] := \omega(X)\,Y - \omega(Y)\,X \qquad \text{for all } X,Y \in \mathcal{g}$$

defines a Lie structure on $\mathcal{g}$, to which we refer as *Lie null algebra* $\mathcal{g}_\omega$. The name arose from the similarity of $\mathcal{g}_\omega$ with the associative null algebra, that was treated in [de Groote 1987]. In both cases the rank is known.

Theorem 4

$$R(\mathcal{g}_\omega) = 2 \dim_{\mathbb{C}} \mathcal{g}_\omega - 2 \ .$$

Proof: Certainly $R(\mathcal{g}_\omega) \leq 2 \dim_{\mathbb{C}} \mathcal{g}_\omega - 2$. Now consider an optimal bilinear algorithm for $\mathcal{g}_\omega$

$$((u_\rho, v_\rho, w_\rho) \in \mathcal{g}_\omega^* \times \mathcal{g}_\omega^* \times [\mathcal{g}_\omega,\mathcal{g}_\omega] \ , \ 1 \leq \rho \leq r)$$

and let $n := \dim_{\mathbb{C}} \mathcal{g}_\omega$. After a suitable renumbering we may assume that the restrictions of $u_1,\ldots,u_{n-1}$ to $[\mathcal{g}_\omega,\mathcal{g}_\omega]$ form a basis of $[\mathcal{g}_\omega,\mathcal{g}_\omega]^*$ with dual basis $X_1,\ldots,X_{n-1}$ of $[\mathcal{g}_\omega,\mathcal{g}_\omega]$.

We denote by $\mathcal{a}$ the orthogonal complement of $v_n,\ldots,v_r$. $\mathcal{a}$ is not contained in $[\mathcal{g}_\omega,\mathcal{g}_\omega] = \ker \omega$, for the converse would imply $\mathcal{a} \subseteq \bigcap_{1 \leq \rho \leq r} \ker v_\rho = 0$ and therefore $0 = \dim_{\mathbb{C}} \mathcal{a} \geq 2n - 1 - r$, which contradicts the choice of r.

Thus for some element $A_0 \in \mathcal{a} \setminus \ker \omega$:

$$[X_i, A_0] = -\omega(A_0) X_i = v_i(A_0)\, W_i \neq 0 \qquad \text{for} \quad i \leq n-1 \ ,$$

showing that $\{W_1,\ldots,W_{n-1}\}$ is a basis of $[\mathcal{g}_\omega,\mathcal{g}_\omega]$. In this case, however, $\mathcal{a}$ is even a generic subalgebra of $\mathcal{g}_\omega$ and forthwhith abelian. But abelian subalgebras of $\mathcal{g}_\omega$ containing A_0 are one dimensional, i.e. $1 = \dim_{\mathbb{C}} \mathcal{a} \geq 2n - 1 - r$. □

3. The isotropy group

Let k be any field and g be an arbitrary, finite dimensional Lie algebra over k. Let $\phi,\psi,\chi \in GL(g)$ such that $\phi^* \otimes \psi^* \otimes \chi \in \Gamma(g)$.

As one easily sees $\phi \circ \psi^{-1}$ is an endomorphism of the k-vector space g, *symmetric* in the sense that

$$[\,\phi \circ \psi^{-1}(X)\,,\,Y\,] \;=\; [\,X\,,\,\phi \circ \psi^{-1}(Y)\,] \qquad \text{holds for all} \quad X,Y \in g\,.$$

So, in a first attempt to characterize $\Gamma(g)$, one has to determine the symmetric mappings of g. These are special cases of the transposable mappings of g:
We call a k-vector space endomorphism $\sigma : g \to g$ *transposable*, if there exists a k-vector space endomorphism $\tau : g \to g$ such that

$$[\,\sigma(X)\,,\,Y\,] \;=\; [\,X\,,\,\tau(Y)\,] \qquad \text{holds for all} \quad X,Y \in g\,.$$

If g has trivial centre, then τ is uniquely determined by σ, and we write $\sigma^* := \tau$. The transposable mappings form a finite dimensional associative k-algebra $T(g)$ with involution $*$.
A k-linear endomorphism $\sigma : g \to g$ is symmetric iff $\sigma^* = \sigma$.

Now let us assume that g is a semisimple Lie algebra over $\mathbf{C}$. Then

$$g \;\cong\; \bigoplus_{i=1}^{m} (\underbrace{g_i \oplus \ldots \oplus g_i}_{n_i \text{ summands}})$$

where the g_i are simple Lie algebras such that $g_i \ncong g_j$ for $i \neq j$ and $g_1 \cong sl(2,\mathbf{C})$.
Let $\mathcal{B}$ be a Borel subalgebra of g. Then $\mathcal{B} \cong \bigoplus_{i=1}^{m} (\mathcal{B}_i \oplus \ldots \oplus \mathcal{B}_i)$ (n_i summands), where $\mathcal{B}_i$ is an ideal of $\mathcal{B}$ being a Borel subalgebra of g_i.

With this notation we have

Theorem 5

(i) $\quad T(g) \;\cong\; \mathbf{C}^s$

(ii) $\quad T(\mathcal{B}) \;\cong\; \mathbb{M}_2(\mathbf{C})^{n_1} \times (\,\mathbf{C}[T]/(T^2)\,)^{s-n_1}$,
where $s = \sum_{i=1}^{m} n_i$, $\mathbb{M}_2(\mathbf{C})$ is the associative $\mathbf{C}$-algebra of 2×2-matrices over $\mathbf{C}$, and T is an indeterminate over $\mathbf{C}$.

(iii) $\quad \sigma \in T(g)$ symmetric iff $\sigma \in \mathbf{C}\,id_{g_1} \oplus \ldots \oplus \mathbf{C}\,id_{g_s}$ and
$\sigma \in T(\mathcal{B})$ symmetric iff $\sigma \in \mathbf{C}\,id_{\mathcal{B}_1} \oplus \ldots \oplus \mathbf{C}\,id_{\mathcal{B}_s}$.

For the isotropy group of g we have

Theorem 6

(i) $$\Gamma(g) \cong \bigtimes_{i=1}^{m} S_{n_i} \ltimes \Big(\mathbb{C}_0^{s} \times \underbrace{GL(g_1) \times \ldots \times GL(g_1)}_{n_1 \text{ factors}} \times \bigtimes_{i=2}^{m} \underbrace{(\mathrm{Aut}(g_i) \times \ldots \times \mathrm{Aut}(g_i))}_{n_i \text{ factors}} \Big) \qquad \text{for} \quad m > 1$$

(ii) $$\Gamma(g) \cong S_{n_1} \ltimes \Big(\mathbb{C}_0^{s+1} \times \big(\underbrace{GL(g_1) \times \ldots \times GL(g_1)}_{n_1 \text{ factors}} \big) / \mathbb{C}_0 \Big) \qquad \text{for} \quad m = 1,$$

where $s := n_1 - 2 + 2 \sum_{i=2}^{m} n_i$ and $\mathbb{C}_0 := \mathbb{C} \setminus \{0\}$.

In particular, for g simple we obtain

$$\Gamma(g) \cong \mathrm{Aut}(g) \qquad \text{if} \quad g \ncong sl(2,\mathbb{C})$$

and $$\Gamma(g) \cong GL(g)/\mathbb{C}_0 \qquad \text{if} \quad g \cong sl(2,\mathbb{C})$$

(compare [de Groote - Heintz 1986], [Mirwald 1986]).

The same results hold, if we replace in the above formulae each Lie algebra by its Borel subalgebra.

Finally let us mention that the extended isotropy group operates transitively on the algorithm variety of $sl(2,\mathbb{C})$. This means that there exists essentially only one optimal bilinear algorithm which computes the bilinear mapping $[,] : sl(2,\mathbb{C}) \times sl(2,\mathbb{C}) \longrightarrow sl(2,\mathbb{C})$.
This is by now the only case of a Lie algebra of which the algorithm variety is known ([Mirwald 1986]).

References

Goto, M. & Grosshans, F.D. : Semisimple Lie Algebras. M. Dekker, New York & Basel 1978.

Greub, W. : Linear Algebra. 4th edition. GTM 23, Springer, New York 1981.

de Groote, H.F. : On varieties of optimal algorithms for the computation of bilinear mappings. I. The isotropy group of a bilinear mapping. Theoret. Comput. Sci. 7 (1978) 1-24.

de Groote, H.F. : Lectures on the Complexity of Bilinear Problems.
LN Comput. Sci. 245, Springer, Berlin 1987.

de Groote, H.F. & Heintz, J. : A lower bound for the bilinear complexity of some semisimple Lie algebras.
in: Algebraic Algorithms and Error Correcting Codes. Proc. AAECC-3, Grenoble 1985.
LN Comput. Sci. 229 (1986) 211-222.

Humphreys, J.E. : Introduction to Lie Algebras and Representation Theory. 3rd printing revised.
GTM 9, Springer, New York 1980.

Mirwald, R. : The algorithmic structure of sl(2,k).
in: Algebraic Algorithms and Error Correcting Codes. Proc. AAECC-3, Grenoble 1985.
LN Comput. Sci. 229 (1986) 274-287.

Strassen, V. : Vermeidung von Divisionen.
J. Reine Angew. Math. 264 (1973) 184-202.