Available online at www.sciencedirect.com
SCIENCE DIRECT®
LINEAR ALGEBRA AND ITS APPLICATIONS
ELSEVIER
Linear Algebra and its Applications 382 (2004) 195–209
www.elsevier.com/locate/laa

Computing the automorphism group of a solvable Lie algebra

Bettina Eick*

Department of Mathematics, Institut fur Geometrie, TU Braunschweig, Braunschweig 38106, Germany

Received 5 October 2003; accepted 19 December 2003

Submitted by R.A. Brualdi

Abstract

We describe an effective algorithm for computing the automorphism group of a finite-dimensional solvable Lie algebra over a finite field. We show that a similar approach can be used to determine a canonical table for such a Lie algebra; that is, a description for the Lie algebra which is invariant under isomorphisms. Hence we also obtain an effective isomorphism test for finite-dimensional solvable Lie algebras over finite fields.

Keywords: Lie algebra; Automorphism group; Representation theory; Cohomology theory; Algorithmic methods

1. Introduction

The computation of the automorphism group of a Lie algebra is in general a difficult task. Let L be a Lie algebra of dimension d over a field $\mathbb{F}$. Then its automorphism group can be defined as

$$\mathrm{Aut}(L) = \{g \in GL(d, \mathbb{F}) \mid [h, k]^g = [h^g, k^g] \text{ for all } h, k \in L\},$$

where $h^g = g(h)$ for $h \in L$ and $g \in GL(d, \mathbb{F})$. If $\mathbb{F}$ is finite, then $\mathrm{Aut}(L)$ could be determined by searching through the elements $GL(d, \mathbb{F})$, but this is practical for very small d and $|\mathbb{F}|$ only.

* Tel.: +49-531-391-7525; fax: +49-531-391-8210.
E-mail address: beick@tu-bs.de (B. Eick).

0024-3795/$ - see front matter
doi:10.1016/j.laa.2003.12.009

The central aim of this paper is to present effective methods for computing $\mathrm{Aut}(L)$, where L is a finite-dimensional solvable Lie algebra defined over a finite field $\mathbb{F}$. First, we introduce a method which proceeds by induction on an arbitrary $\mathrm{Aut}(L)$-invariant chain of ideals with abelian factors in L. The induction step is performed by a sequence of stabilizer computations in this approach.

Then, we refine this first approach by choosing an ideal chain with additional useful properties as we describe in the second part of the paper. The resulting second algorithm is in many cases more effective than the first method, and it extends the range of possible applications of our algorithms in a significant manner.

A variation of the automorphism group computation is the determination of a canonical table for L; that is, we compute a commutator table for L which describes L uniquely up to isomorphism. Thus we obtain an effective isomorphism test for finite-dimensional solvable Lie algebras over finite fields. The constructed canonical table has the property that it contains comparatively few non-zero entries.

Finite-dimensional solvable Lie algebras defined over a finite field have similarities to finite solvable groups and thus our methods reminiscent algorithms for such groups. In particular, we note that the basic ideas of our first algorithm (Section 2) are related to the method for groups proposed by Robinson [2] and Smith [3].

2. The general algorithm

Let L be a finite-dimensional Lie algebra over a finite field $\mathbb{F}_q$ with q elements and suppose that L has an $\mathrm{Aut}(L)$-invariant abelian ideal I. Our central aim in this section is to describe an effective algorithm for determining $\mathrm{Aut}(L)$ from $\mathrm{Aut}(L/I)$. We consider a group as 'known' or 'determined' if generators for this group and the order of the group are given.

If L is solvable, then there exists an $\mathrm{Aut}(L)$-invariant series $L \geqslant L_2 \geqslant \cdots L_k \geqslant L_{k+1} = 0$ of ideals $L_i \trianglelefteq L$ such that each factor L_i/L_{i+1} is an abelian Lie algebra; for example, the derived series of L is of this type. The method introduce here can then be applied to determine $\mathrm{Aut}(L/L_i)$ for $1 \leqslant i \leqslant k+1$ stepwise by induction, and thus we can compute $\mathrm{Aut}(L) = \mathrm{Aut}(L/L_{k+1})$ in this case.

2.1. The overall approach

Since the ideal I is $\mathrm{Aut}(L)$-invariant, there exists a homomorphism

$$\phi : \mathrm{Aut}(L) \to \mathrm{Aut}(L/I) \times \mathrm{Aut}(I) : \alpha \mapsto (\alpha_{L/I}, \alpha_I)$$

induced by the actions of $\mathrm{Aut}(L)$ on the Lie algebras L/I and I. As I is an abelian Lie algebra of dimension d_I, say, we observe that $\mathrm{Aut}(I) = GL(d_I, q)$ and hence the group $\mathrm{Aut}(L/I) \times \mathrm{Aut}(I)$ and thus the range of ϕ is known.

Our overall approach for the determination of $\mathrm{Aut}(L)$ is to compute $\mathrm{Im}(\phi)$ and $\mathrm{Ker}(\phi)$ and then to combine these two groups to $\mathrm{Aut}(L)$. This is described stepwise in the following sections. A summary of the algorithm is then provided in Section 2.7.

2.2. Preliminaries and some notation

We write $K = L/I$ throughout to shorten notation and the corresponding natural epimorphism is denoted by $\mu : L \to K : l \mapsto l + I$. For each element k in K we fix a preimage under μ and denote this preimage with $\bar{k}$; hence $\bar{k}^{\mu} = k$ holds. Then we define a Lie bracket for $a \in I$ and $k \in K$ via $[a, k] = [a, \bar{k}]$. This Lie bracket is independent of the chosen preimage, since I is an abelian Lie algebra.

The Lie algebra L can be described as an extension of I by K using two mappings: the representation induced by K on I and the cocycle defining L as an extension of I by K. More precisely, these maps are defined as

$$\begin{aligned} \text{representation:} \quad & \rho : K \to \mathrm{Der}(I) : k \mapsto \kappa \text{ where } \kappa : I \to I : a \mapsto [a, k] \\ \text{cocycle:} \quad & \gamma : K \times K \to I : (k, h) \mapsto [\bar{k}, \bar{h}] - \overline{[k, h]} \end{aligned}$$

Note that $\mathrm{Der}(I) = M(d_I, q)$, the set of all $(d_I \times d_I)$-matrices, since I is an abelian Lie algebra of dimension d_I, and thus the range of ρ is known.

This representation and its impact on $\mathrm{Aut}(L)$ is considered in Section 2.3, and the cocycle and its impact on $\mathrm{Aut}(L)$ is considered in Section 2.4.

2.3. The group of compatible pairs and the image of ϕ

We determine the image of the homomorphism ϕ in two steps and the first of these steps is outlined in this section. We define the set of compatible pairs as

$$\begin{aligned} \mathrm{Comp}(K, I) = \big\{ & (\alpha,\beta) \in \mathrm{Aut}(K) \times \mathrm{Aut}(I) \mid [a^{\beta},k^{\alpha}] = [a,k]^{\beta} \\ & \text{for } a \in I, k \in K \big\}. \end{aligned}$$

Then $\mathrm{Comp}(K, I)$ is a subgroup of $\mathrm{Aut}(K) \times \mathrm{Aut}(I)$; in fact, one can consider $\mathrm{Comp}(K, I)$ as those pairs in $\mathrm{Aut}(K) \times \mathrm{Aut}(I)$ which are compatible with the representation ρ induced by K on I. The following theorem yields a connection between $\mathrm{Comp}(K, I)$ and $\mathrm{Im}(\phi)$.

Theorem 1. $\mathrm{Im}(\phi) \leqslant \mathrm{Comp}(K, I)$.

Proof. Let $\sigma \in \mathrm{Aut}(L)$ with $(\alpha, \beta) = \sigma^{\phi} \in \mathrm{Im}(\phi)$. Let $a \in I$ and $k \in K$. Then $k^{\alpha} = \bar{k}^{\sigma} + I$ and thus $[a, k]^{\beta} = [a, \bar{k}]^{\beta} = [a, \bar{k}]^{\sigma} = [a^{\sigma}, \bar{k}^{\sigma}] = [a^{\beta}, k^{\alpha}]$. Hence we obtain that $(\alpha, \beta) \in \mathrm{Comp}(K, I)$. □

We determine $\mathrm{Comp}(K, I)$ as the first step towards computing $\mathrm{Im}(\phi)$. For this purpose we give a description of $\mathrm{Comp}(K, I)$ as a stabilizer in $\mathrm{Aut}(K) \times \mathrm{Aut}(I)$. We define

$$\mathrm{Hom}(K, \mathrm{Der}(I)) = \{\iota : K \to \mathrm{Der}(I) \mid \iota \text{ is linear}\}.$$

Then the representation $\rho : K \to \mathrm{Der}(I)$ is contained in $\mathrm{Hom}(K, \mathrm{Der}(I))$. Further, the group $\mathrm{Aut}(K) \times \mathrm{Aut}(I)$ acts on $\mathrm{Hom}(K, \mathrm{Der}(I))$ via

$$\iota^{(\alpha,\beta)} : K \to \mathrm{Der}(I) : k \mapsto \beta^{-1} \cdot ((k^{\alpha^{-1}})^{\iota}) \cdot \beta = ((k^{\alpha^{-1}})^{\iota})^{\beta}.$$

Using this action, we can consider the stabilizer of ρ in $\mathrm{Aut}(K) \times \mathrm{Aut}(I)$. This yields the following.

Theorem 2. $\mathrm{Comp}(K, I) = \mathrm{Stab}_{\mathrm{Aut}(K)\times\mathrm{Aut}(I)}(\rho)$.

Proof. We compute

$$\begin{aligned}(\alpha, \beta) \in \mathrm{Comp}(K, I) &\Leftrightarrow (\alpha^{-1}, \beta^{-1}) \in \mathrm{Comp}(K, I)\\ &\Leftrightarrow [a^{\beta^{-1}}, k^{\alpha^{-1}}]^{\beta} = [a, k] \text{ for } a \in I, k \in K\\ &\Leftrightarrow \beta^{-1} \cdot (k^{\alpha^{-1}})^{\rho} \cdot \beta = k^{\rho} \text{ for } k \in K\\ &\Leftrightarrow \rho^{(\alpha,\beta)} = \rho\\ &\Leftrightarrow (\alpha, \beta) \in \mathrm{Stab}_{\mathrm{Aut}(K)\times\mathrm{Aut}(I)}(\rho)\end{aligned}$$

and thus we obtain that $\mathrm{Comp}(K, I) = \mathrm{Stab}_{\mathrm{Aut}(K)\times\mathrm{Aut}(I)}(\rho)$ as desired. □

Hence we can compute $\mathrm{Comp}(K, I)$ as a stabilizer. The computation of a stabilizer under the action of a finite group is a well-known problem in algorithmic group theory and there are effective solutions available to this problem.

Remark 3. $\mathrm{Hom}(K, \mathrm{Der}(I))$ is a vector space of dimension $d_K d_I^2$ over $\mathbb{F}_q$, where $d_K = \dim(K)$ and $d_I = \dim(I)$, and the action of $\mathrm{Aut}(K) \times \mathrm{Aut}(I)$ on $\mathrm{Hom}(K, \mathrm{Der}(I))$ is linear. Thus $\mathrm{Comp}(K, I)$ is the stabilizer of an element in $\mathbb{F}_q^{d_K d_I^2}$ under the action of a subgroup of $GL(d_K d_I^2, q)$.

Finally, we note that the stabilizer computation to determine $\mathrm{Comp}(K, I)$ can be time-consuming if the orbit of ρ is large. This problem can be reduced by breaking one large stabilizer computation into a sequence of smaller computations. For example:

- Determine $\mathrm{Ker}(\rho) \leqslant K$ and compute $A_K = \mathrm{Stab}_{\mathrm{Aut}(K)}(\mathrm{Ker}(\rho))$ using a stabilizer algorithm.
- Construct $A_I = \mathrm{Stab}_{\mathrm{Aut}(I)}(\mathrm{Im}(\rho))$ the subgroup in $GL(d_I, q)$ stabilizing the subspace $\mathrm{Im}(\rho) \leqslant \mathrm{Der}(I)$.
- Then $\mathrm{Comp}(K, I) \leqslant A_K \times A_I$ and thus we compute $\mathrm{Comp}(K, I) = \mathrm{Stab}_{A_K\times A_I}(\rho)$ using a stabilizer algorithm.

2.4. Inducible pairs and the image of ϕ

In this section we describe the second step towards computing generators for $\mathrm{Im}(\phi)$. We define the second cohomology groups of K and I as

$$
\begin{aligned}
C^2(K,I) &= \{\epsilon : K \times K \to I \text{ bilinear and skew-symmetric}\},\\
Z^2(K,I) &= \{\epsilon \in C^2(K,I) \mid (k,[h,l])^\epsilon + (h,[l,k])^\epsilon + (l,[k,h])^\epsilon\\
&\qquad = [(h,l)^\epsilon,k] + [(l,k)^\epsilon,h] + [(k,h)^\epsilon,l]\},\\
B^2(K,I) &= \{\epsilon \in C^2(K,I) \mid (k,h)^\epsilon = [k,h]^\nu - [k^\nu,h]\\
&\qquad + [h^\nu,k] \text{ for a linear map } \nu : K \to I\}.
\end{aligned}
$$

Then $Z^2(K,I)$ corresponds to the set of extensions of I by K. More precisely, each element ϵ in $Z^2(K,I)$ defines an extension $L_\epsilon = K \times I$ having a Lie bracket defined by $[(k,a),(h,b)] = ([k,h],(k,h)^\epsilon + [a,h] - [b,k])$. It is straightforward to check that L_ϵ is a Lie algebra.

Further, the set $Z^2(K,I)$ is a vector space over $\mathbb{F}_q$ and $B^2(K,I)$ is a subspace of $Z^2(K,I)$. The elements in $B^2(K,I)$ correspond to those extensions of I by K which are split extensions. We denote $H^2(K,I) = Z^2(K,I)/B^2(K,I)$. In the following we introduce some notation.

- The group of compatible pairs $\mathrm{Comp}(K,I)$ acts on the vector space $Z^2(K,I)$ via $\epsilon^{(\alpha,\beta)} : K \times K \to I : (k,h) \mapsto ((k^{\alpha^{-1}},h^{\alpha^{-1}})^\epsilon)^\beta$.
- The subspace $B^2(K,I)$ is setwise invariant under this action and thus the group $\mathrm{Comp}(K,I)$ also acts on the factor $H^2(K,I)$.
- Let $\gamma \in Z^2(K,I)$ such that $L = L_\gamma$. We define the group of inducible pairs via $\mathrm{Indu}(K,I,\gamma) = \mathrm{Stab}_{\mathrm{Comp}(K,I)}(\gamma + B^2(K,I))$.

The inducible pairs are those elements in $\mathrm{Comp}(K,I)$ which induce an automorphism of L as the following theorem establishes.

Theorem 4. $\mathrm{Im}(\phi) = \mathrm{Indu}(K,I,\gamma)$.

Proof. Let $(\alpha,\beta) \in \mathrm{Indu}(K,I,\gamma)$. Then $\gamma^{(\alpha,\beta)} \equiv \gamma \bmod B^2(K,I)$. Thus there exists an element $\epsilon \in B^2(K,I)$ such that $\gamma^{(\alpha,\beta)} + \epsilon^{(\alpha,\beta)} = \gamma$. Hence we obtain that $(k^\alpha,h^\alpha)^\gamma = ((k,h)^\gamma + (k,h)^\epsilon)^\beta$. Let $\nu : K \to I$ such that ν induces ϵ. Then we define $\sigma : L \to L : (k,a) \mapsto (k^\alpha, a^\beta + (k^\nu)^\beta)$. Clearly, σ leaves I invariant and induces α and β on K and I, respectively. It remains to show that σ is a homomorphism of L:

$$
\begin{aligned}
[(k,a),(h,b)]^\sigma &= ([k,h],(k,h)^\gamma + [a,h] - [b,k])^\sigma\\
&= ([k,h]^\alpha,((k,h)^\gamma + [a,h] - [b,k])^\beta + ([k,h]^\nu)^\beta)\\
&= ([k,h]^\alpha,((k,h)^\gamma)^\beta + [a,h]^\beta - [b,k]^\beta\\
&\quad + ((k,h)^\epsilon + [k^\nu,h] - [h^\nu,k])^\beta)\\
&= ([k^\alpha,h^\alpha],((k,h)^\gamma)^\beta + ((k,h)^\epsilon)^\beta + [a^\beta,h^\alpha] - [b^\beta,k^\alpha]\\
&\quad + [(k^\nu)^\beta,h^\alpha] - [(h^\nu)^\beta,k^\alpha])\\
&= ([k^\alpha,h^\alpha],(k^\alpha,h^\alpha)^\gamma + [a^\beta + (k^\nu)^\beta,h^\alpha] - [b^\beta + (h^\nu)^\beta,k^\alpha])
\end{aligned}
$$

$$= [(k^\alpha, a^\beta + (k^\nu)^\beta), (h^\alpha, b^\beta + (h^\nu)^\beta)]$$
$$= [(k, a)^\sigma, (h, b)^\sigma].$$

Let $(\alpha, \beta) \in \mathrm{Im}(\phi)$. Then there exists an element $\sigma \in \mathrm{Aut}(L)$ such that $\sigma^\phi = (\alpha, \beta)$. Let $\nu : K \to I$ be defined by $(0, (k^\nu)^\beta) = (k, 0)^\sigma - (k^\alpha, 0)$. Then ν is a linear map and thus it induces an element $\epsilon \in B^2(K, I)$. We prove that $\gamma^{(\alpha,\beta)} + \epsilon^{(\alpha,\beta)} = \gamma$ in the following.

$$\begin{aligned}
&([k, h]^\alpha, ((k, h)^\gamma)^\beta + ([k, h]^\nu)^\beta) \\
&\quad = ([k, h], (k, h)^\gamma)^\sigma \\
&\quad = [(k, 0), (h, 0)]^\sigma \\
&\quad = [(k, 0)^\sigma, (h, 0)^\sigma] \\
&\quad = [(k^\alpha, (k^\nu)^\beta), (h^\alpha, (h^\nu)^\beta)] \\
&\quad = [k^\alpha, h^\alpha], (k^\alpha, h^\alpha)^\gamma + [(k^\nu)^\beta, h^\alpha] - [(h^\nu)^\beta, k^\alpha] \\
&\quad = [k, h]^\alpha, (k^\alpha, h^\alpha)^\gamma + [k^\nu, h]^\beta - [h^\nu, k]^\beta \\
&\quad = [k,h]^\alpha, (k^\alpha, h^\alpha)^\gamma + ([k,h]^\nu)^\beta - ((k, h)^\epsilon)^\beta.
\end{aligned}$$

Thus we obtain $\gamma^{(\alpha,\beta)} \equiv \gamma \bmod B^2(K, I)$ and hence $(\alpha, \beta) \in \mathrm{Indu}(K, I, \gamma)$ as desired. □

By Theorem 4, we can compute $\mathrm{Im}(\phi)$ as a stabilizer of a cocycle γ under the action of the group $\mathrm{Comp}(K, I)$. The proof of Theorem 4 also yields a method to compute preimages under ϕ for an element in $\mathrm{Indu}(K, I, \gamma)$. This is outlined explicitly in the following corollary.

Corollary 5. *Let $(\alpha, \beta) \in \mathrm{Indu}(K, I, \gamma)$. Then there exists an element $\epsilon \in B^2(K, I)$ with $\gamma^{(\alpha,\beta)} + \epsilon^{(\alpha,\beta)} = \gamma$. Suppose that ϵ is induced by the linear map $\nu : K \to I$. Then $\sigma : L \to L : (k, a) \mapsto (k^\alpha, a^\beta + k^{\nu\beta})$ is a preimage of (α, β) under ϕ.*

Remark 6. $H^2(K, I)$ is a vector space and the action of $\mathrm{Comp}(K, I)$ on $H^2(K, I)$ is linear. Thus $\mathrm{Im}(\phi)$ is the stabilizer of an element in $\mathbb{F}_q^d$ under the action of a subgroup of $GL(d, q)$, where $d = \dim(H^2(K, I)) \leqslant d_K^2 d_I$ for $d_K = \dim(K)$ and $d_I = \dim(I)$.

2.5. Comments on the computation of $Z^2(K, I)$ and $B^2(K, I)$

In this section we observe that bases for $Z^2(K, I)$ and $B^2(K, I)$ can be computed using linear algebra techniques. Let $k_1, \ldots, k_{d_K}$ be a basis of K. We define a map

$$\psi : Z^2(K, I) \to M(d_K, I) : \epsilon \mapsto ((k_i, k_j)^\epsilon)_{ij},$$

where $M(d_K, I)$ denotes the set of all $d_K \times d_K$-matrices with entries in the Lie algebra I. Then the entries in an image ϵ^ψ are the tails which are needed to enlarge

the structure constants table of K with respect to the given basis to structure constants table of the extension L_ϵ. Thus an algorithmically useful description for L_ϵ can be read off from ϵ^ψ.

Lemma 7. $H^2(K, I) \cong Z^2(K, I)^\psi / B^2(K, I)^\psi$.

Proof. Using the structure constants tables, it is straightforward to observe that each $\epsilon \in \mathrm{Ker}(\psi)$ defines a split extension of I by K. Hence we obtain that $\mathrm{Ker}(\psi) \leqslant B^2(K, I)$. This implies that $H^2(K, I) \cong Z^2(K, I)^\psi / B^2(K, I)^\psi$. □

The definition of $Z^2(K, I)$ yields that $Z^2(K, I)^\psi$ is the nullspace of a system of linear homogenous equations in $M(d_K, I)$. Thus we can compute a basis for $Z^2(K, I)^\psi$ using the Gaussian elimination algorithm. Similarly, the definition of $B^2(K, I)$ yields that $B^2(K, I)^\psi$ is the image of a linear map and we can determine a basis of $B^2(K, I)^\psi$ readily.

2.6. *The kernel of ϕ*

The following lemma yields a description of $\mathrm{Ker}(\phi)$ which can be used to compute generators for this kernel. We define the first cohomology group of K and I as

$$Z^1(K, I) = \{\nu : K \to I \text{ linear} \mid [k, h]^\nu = [k^\nu, h] - [h^\nu, k]\}.$$

Thus $Z^1(K, I)$ is a vector space over $\mathbb{F}_q$.

Lemma 8. $\mathrm{Ker}(\phi) \cong Z^1(K, I)$ *as abelian groups*.

Proof. Let $\sigma \in \mathrm{Ker}(\phi)$. Then $\sigma \in \mathrm{Aut}(L)$ has the form $\sigma : L \to L : l \mapsto l + a_l$ for certain elements $a_l \in I$. We observe that

$$\begin{aligned} a_{[l,h]} &= [l, h]^\sigma - [l, h] = [l^\sigma, h^\sigma] - [l, h] \\ &= [l + a_l, h + a_h] - [l, h] = [l, h] + [a_l, h] + [l, a_h] - [l, h] \\ &= [a_l, h] - [a_h, l]. \end{aligned}$$

Further, $a_l = a_h$ if $l \equiv h \bmod I$ and thus we can identify a_l with a_{l+I}. This yields a map $\nu : K \to I : k \mapsto a_k$ with $\nu \in Z^1(K, I)$. Hence we can define a map $\mathrm{Ker}(\phi) \to Z^1(K, I) : \sigma \mapsto \nu$. It is easy to observe that this map is a group homomorphism from the multiplicative group $\mathrm{Ker}(\phi)$ into the additive group $Z^1(K, I)$. Clearly, the map is bijective and hence an isomorphism. □

Let $k_1, \ldots, k_{d_K}$ be a basis of K. We denote the structure constants of K with S_{ij} for $1 \leqslant i, j \leqslant d_K$. With respect to this basis, the space $Z^1(K, I)$ embeds into the space $V(d_K, I)$ of all d_K-dimensional vectors with entries in I via

$$\psi : Z^1(K, I) \to V(d_K, I) : \nu \mapsto ((k_i^\nu))_i.$$

Since $I \cong \mathbb{F}_q^{d_I}$, we can consider the elements of $V(d_K, I)$ as matrices of dimension $d_I \times d_K$ over $\mathbb{F}_q$. For such a matrix m we observe that

$$m \in Z^1(K, I)^\psi \Leftrightarrow [k_i, k_j]m - [k_i m, k_j] + [k_j m, k_i] = 0 \quad \text{for } 1 \leqslant i < j \leqslant d_K$$

$$\Leftrightarrow S_{i,j}m - \sum_{l=1}^{d_K} (m_{il} S_{lh} - m_{jl} S_{lj}) = 0 \quad \text{for } 1 \leqslant i < j \leqslant d_K.$$

This yields that $Z^1(K, I)^\psi$ is the solution space of a system of $d_K(d_K - 1)/2$ linear homogeneous equations over $\mathbb{F}_q$.

2.7. A summary of the general automorphism group algorithm

In this section we summarize the method introduced in the above sections. Let L be a solvable Lie algebra over the finite field $\mathbb{F}_q$. Let $L \geqslant L_2 \geqslant \cdots L_k \geqslant L_{k+1} = 0$ be an $\mathrm{Aut}(L)$-invariant chain of ideals $L_i \trianglelefteq L$ such that each factor L_i/L_{i+1} is abelian. For example, the derived series of L is of this type and can be computed readily.

AutomorphismGroup(L)

initialize $A = GL(d, q)$ where $d = \dim(L/L_2)$
for i in $[2 \ldots k]$ do
  set $K = L/L_i$ and $I = L_i/L_{i+1}$
  set $D = A \times GL(d_I, q)$ where $d_I = \dim(I)$
  compute as in Theorem 2 and Remark 3:
    $\rho : K \to \mathrm{Der}(I)$ the representation induced by K on I
    $C = \mathrm{Comp}(K, I) = \mathrm{Stab}_D(\rho)$
  compute as in Theorem 4 and Remark 6:
    $\gamma : K \times K \to I$ the cocycle defining L/L_{i+1} as an extension of I by K
    $B = \mathrm{Indu}(K, I, \gamma) = \mathrm{Stab}_C(\gamma)$
  compute using Corollary 5 and Lemma 8:
    $U = \mathrm{Ker}(\phi)$ and, based on this, P with $P^\phi = B$
    reset $A = P$
end for
return A

In summary, this algorithm needs various applications of the Gaussian elimination algorithm and two applications of a stabilizer computation of a vector under the action of a matrix group over $\mathbb{F}_q$. These two stabilizer computations are usually the time- and space-consuming part of the algorithm. It is also the part of the algorithm which is limiting its range of applications. Hence all our later improvements of the algorithm will consider these two stabilizer computations.

The overall approach of the automorphism group computation as outlined above could be applied to solvable Lie algebras over infinite fields also. In fact, all the applications of the Gaussian elimination algorithm can be performed over many infinite fields as well. The problem is in the stabilizer computations, since it is not generally possible to determine the stabilizer of a vector under the action of an infinite linear group.

2.8. A variation to compute canonical tables

A variation of the method in Section 2.7 can be used to determine a canonical table for a solvable Lie algebra L over a finite field $\mathbb{F}_q$. We compute canonical elements in orbits instead of stabilizers in this case. For this purpose we use minimal elements in a set of vectors; for example, the lexicographically smallest vector among all vectors of minimal weight, where the weight of a vector is the number of its non-zero entries, can be used.

CanonicalForm(L)
  initialize $A = GL(d, q)$ where $d = \dim(L/L_2)$
  initialize $H = L/L_2$
  initialize $\iota : H \to L/L_2$ the identity map
  for i in $[2 \dots k]$ do
    set $K = L/L_i$ and $I = L_i/L_{i+1}$ such that $\iota : H \to K$
    set $D = A \times GL(d_I, q)$ where $d_I = \dim(I)$
    compute as in Theorem 2 and Remark 3:
      $\rho : H \to \mathrm{Der}(I)$ the representation induced by H on I via ι
      $\bar{\rho}$ a minimal element in the orbit ρ^D
      $C = \mathrm{Comp}(H, I) = \mathrm{Stab}_D(\bar{\rho})$
    compute as in Theorem 4 and Remark 6:
      $\gamma : H \times H \to I$ the cocycle defining L/L_{i+1} as an extension of I by H via $\bar{\rho}$
      $\bar{\gamma}$ a minimal element in the orbit γ^C
      $B = \mathrm{Indu}(H, I, \bar{\gamma}) = \mathrm{Stab}_C(\bar{\gamma})$
    compute with Corollary 5 and Lemma 8
      H the extension of I by H via $\bar{\rho}$ and $\bar{\gamma}$
      A such that $A^{\phi} = B$ and $A = \mathrm{Aut}(H)$
      $\iota : H \to L/L_{i+1}$ the induced isomorphism
  end for
  return H

3. Improvements to the general algorithm

In this section we introduce a variation for the automorphism group method of Section 2. Let L be a finite-dimensional Lie algebra over the finite field $\mathbb{F}_q$

with q elements and let N be the nilradical of L; that is, the largest nilpotent ideal of L. Suppose that $\dim(N) \neq 0$ and note that this is the case if L is solvable.

Let $N = N_1 > \cdots > N_c > N_{c+1} = 0$ be the lower central series of N. Then $N_i \trianglelefteq L$ and this series is an $\mathrm{Aut}(L)$-invariant series with abelian factors. We compute $\mathrm{Aut}(L)$ stepwise along this series. For this purpose distinguish two cases:

(1) *Initial step*: Compute $\mathrm{Aut}(L/N_2)$ (Section 3.1).
(2) *Iteration steps*: Compute $\mathrm{Aut}(L/N_{i+1})$ from $\mathrm{Aut}(L/N_i)$ for $i > 1$ (Section 3.2).

Before we investigate the two cases (1) and (2), we recall some elementary facts on nilpotent Lie algebras which will be used throughout. A summary of the improved algorithm is provided in Section 3.3.

Lemma 9. *Let $I_i = N_i/N_{i+1}$ for $1 \leqslant i \leqslant c$.*

(a) *The map $\varphi : I_1 \otimes I_i \to I_{i+1} : (k + N_2) \otimes (h + N_{i+1}) \mapsto [k, h] + N_{i+2}$ is an epimorphism for $1 \leqslant i \leqslant c - 1$.*
(b) *Let $\alpha \in \mathrm{Aut}(N)$. Then α acts on the factors of the lower central series of N and this action is compatible with φ such that $(a \otimes b)^\alpha = a^\alpha \otimes b^\alpha$ for $a \in I_1$ and $b \in I_i$.*
(c) *Let $\delta \in \mathrm{Der}(N)$. Then δ acts on the factors of the lower central series of N and this action is compatible with φ such that $(a \otimes b)^\delta = (a^\delta \otimes b) + (a \otimes b^\delta)$ for $a \in I_1$ and $b \in I_i$.*
(d) *N/N_i is the nilradical of L/N_i for $2 \leqslant i \leqslant c + 1$.*

Proof. (a) Consider the map $I_1 \times I_i \to I_{i+1} : (k + N_2, h + N_{i+1}) \mapsto [k, h] + N_{i+2}$. First, we note that this map is well defined, since $[N_i, N_j] \leqslant N_{i+j}$ holds for the lower central series of N. Also, the map is bilinear, since the Lie bracket is. By the fundamental mapping property of the tensor product, there is an induced homomorphism $\varphi : I_1 \otimes I_i \to I_{i+1} : k + N_2 \otimes h + N_{i+1} \mapsto [k, h] + N_{i+2}$. Since $N_{i+1} = [N, N_i]$, we obtain that φ is an epimorphism.

(b,c) Clearly, the factors of the lower central series of N are invariant under the actions of α and δ. Let $a \in I_1$ and $b \in I_i$. Then $(a \otimes b)^\alpha = [a, b]^\alpha = [a^\alpha, b^\alpha] = a^\alpha \otimes b^\alpha$ and $(a \otimes b)^\delta = [a, b]^\delta = [a^\delta, b] + [a, b^\delta] = (a^\delta \otimes b) + (a \otimes b^\delta)$.

(d) Clearly, N/N_i is a nilpotent ideal of L/N_i. Suppose that M/N_i is a nilpotent ideal of L/N_i with $M \geqslant N$. Then there exists an M-central series through N/N_i and thus the adjoint action of M on I_1 and I_{i-1} induces two nilpotent representations of M. Hence the action of M on the tensor $I_1 \otimes I_{i-1}$ is unipotent and, by (c), so is the action of M on I_i. Thus M/N_{i+1} is nilpotent. By induction, M is nilpotent and thus $M = N$, since N is the nilradical of L. □

3.1. The initial step

Let L be a Lie algebra over $\mathbb{F}_q$ with an abelian nilradical I. We denote this abelian nilradical with I and we write $K = L/I$ for its factor. Also, as in Section 2, we denote the representation of K on I with ρ. The following lemma investigates the structure of ρ.

Lemma 10. *The representation* $\rho : K \to \mathrm{Der}(I)$ *is faithful.*

Proof. Let $C \leqslant L$ such that $C/I = \mathrm{Ker}(\rho)$. Then C annihilates I and thus C is nilpotent of class 2. By construction, the kernel C is an ideal in L. Thus $C = I$, since I is the largest nilpotent ideal in L. □

Hence we identify K and $\mathrm{Im}(\rho)$ in the following. Let $d_I = \dim(I)$ and recall that $\mathrm{Aut}(I) = GL(d_I, q)$. We denote $N_{\mathrm{Aut}(I)}(K) = \{\beta \in \mathrm{Aut}(I) \mid k^\beta \in K \text{ for } k \in K\}$ the normalizer of K in $\mathrm{Aut}(I)$ under the natural conjugation action of $\mathrm{Aut}(I)$. Lemma 10 implies the following theorem on the compatible pairs $\mathrm{Comp}(K, I)$.

Theorem 11. *The map* $\mathrm{Comp}(K, I) \to N_{\mathrm{Aut}(I)}(K) : (\alpha, \beta) \mapsto \beta$ *is an isomorphism.*

Proof. By the definition of $\mathrm{Comp}(K, I)$, this map defines an epimorphism. Let $(\alpha, \mathrm{i}d)$ be an element of the kernel of this map. Then $[a, k^\alpha] = [a, k]$ for all $a \in I$ and $k \in K$. Thus $k^\rho = (k^\alpha)^\rho$ for all $k \in K$. Since ρ is injective, this yields that $\alpha = \mathrm{i}d$. Thus the map is injective and hence an isomorphism. □

Thus it is sufficient to determine $N_{\mathrm{Aut}(I)}(K)$ to obtain $\mathrm{Comp}(K, I)$. There are two essentially different approaches to this problem:

(1) *Start with* $\mathrm{Aut}(I)$: List generators for the normalizer using a stabilizer computation for the conjugation action of $\mathrm{Aut}(I)$ on the d_K-dimensional subspaces of the matrix space $M(d_I, q)$. Since K is solvable, one can break such a stabilizer computation in a sequence of smaller ones using a chain of $N_{\mathrm{Aut}(I)}(K)$-invariant ideals through K.

(2) *Start with* $\mathrm{Aut}(K)$: Determine kernel and image of the map $N_{\mathrm{Aut}(I)}(K) \to \mathrm{Aut}(K)$. The kernel of this map is the centralizer $C_{\mathrm{Aut}(I)}(K)$ and this can be determined using an iterated stabilizer computation acting with $\mathrm{Aut}(I)$ on each of the generators of K. The image is the subgroup of $\mathrm{Aut}(K)$ of those automorphisms which can be realized by matrices in $\mathrm{Aut}(I)$. This can be computed using a stabilizer computation under the action of $\mathrm{Aut}(K)$.

Which of the two approaches is more efficient depends heavily on the given Lie algebra K. However, both approaches are significantly more effective than the general approach to compute $\mathrm{Comp}(K, I)$ as outlined in Section 2.3, since in Section 2.3 we started with $\mathrm{Aut}(K) \times \mathrm{Aut}(I)$, whereas here we either start with $\mathrm{Aut}(I)$ or with $\mathrm{Aut}(K)$.

3.2. The iteration step

Let L be a Lie algebra over $\mathbb{F}_q$ with a non-abelian nilradical N. Let $I = N_c$ be the last non-trivial ideal in the central series of N and denote $K = L/I$. We consider the computation of $\mathrm{Aut}(L)$ from $\mathrm{Aut}(K)$. As in Section 2, we use the natural homomorphism $\phi : \mathrm{Aut}(L) \to \mathrm{Aut}(K) \times \mathrm{Aut}(I)$ and we want to determine $\mathrm{Im}(\phi)$. By Lemma 9, we find that $I = T/U$ where $T = I_1 \otimes I_{c-1}$ and U is a suitable subspace of T. The group $\mathrm{Aut}(K)$ acts on I_1 and on I_{c-1}. Thus $\mathrm{Aut}(K)$ acts on T via $(a \otimes b)^\alpha = a^\alpha \otimes b^\alpha$.

Lemma 12. *Let* $S = \mathrm{Stab}_{\mathrm{Aut}(K)}(U)$. *Then* S *acts on* $T/U = I$ *and thus there exists a homomorphism* $S \to \mathrm{Aut}(I) : \alpha \mapsto \bar{\alpha}$. *Let* $D = \{(\alpha, \bar{\alpha}) \mid \alpha \in S\}$. *Then* $\mathrm{Im}(\phi) \leqslant D$.

Proof. Let $\gamma \in \mathrm{Aut}(L)$ with $(\alpha, \beta) = \gamma^\phi$. By Lemma 9, the action of γ on I is compatible with the representation of I as a factor of the tensor T. Thus $((a \otimes b) + U)^\beta = ((a \otimes b) + U)^\gamma = (a^\gamma \otimes b^\gamma) + U = (a^\alpha \otimes b^\alpha) + U$. Hence $(\alpha, \beta) \in D$. □

Hence we can improve the computation of $\mathrm{Im}(\phi)$ using D as defined in Lemma 12: Instead of starting with $\mathrm{Aut}(K) \times \mathrm{Aut}(I)$ in the stabilizer computations, we start with the significantly smaller group D.

3.3. A summary of the improved algorithm

In the following we provide a summary of the new algorithm.

```
AutomorphismGroup(L)
    compute the nilradical N of L
    compute its central series N = N_1 > ··· > N_c > N_{c+1} = 0
    set K = L/N and I = N/N_2
    compute S = N_{Aut(I)}(K) as used in Theorem 11
    read off C = Comp(K, I)≅S by Theorem 11
    compute B = Indu(K, I, γ) as in Section 2.4
    compute A with A^φ = B as in Section 2.6
    for i in [2...c] do
        set K = L/N_i and I = N_i/N_{i+1}
```

set $T = I_1 \otimes I_{i-1}$ and $U \leqslant T$ with $I = T/U$
compute the action of A on T and $S = \mathrm{Stab}_A(U)$
set $D = \{(\alpha, \bar{\alpha}) \mid \alpha \in S\}$
compute as in Theorem 2 and Remark 3:
$\rho : K \to \mathrm{Der}(I)$ the representation induced by K on I
$C = \mathrm{Comp}(K, I) = \mathrm{Stab}_D(\rho)$
compute as in Theorem 4 and Remark 6:
$\gamma : K \times K \to I$ the cocycle defining L/L_{i+1} as an extension of I by K
$B = \mathrm{Indu}(K, I, \gamma) = \mathrm{Stab}_C(\gamma)$
compute using Corollary 5 and Lemma 8:
$U = \mathrm{Ker}(\phi)$ and, based on this, P with $P^\phi = B$
reset $A = P$
end for
return A

The advantage of this method is in the simplified stabilizer computations. A disadvantage of the new algorithm is that it requires the precomputation of the nilradical of the given Lie algebra. Thus this new method is usually more efficient than the first algorithm if the considered Lie algebra L has large dimension, but it can be less efficient if L has small dimension.

4. Examples and runtimes

The algorithms presented here have been implemented by the author in GAP [4]. There are a variety of algorithms for Lie Algebras included in GAP; we refer to DeGraaf's book [1] for background.

This section contains an outline of various example computations for this GAP implementation. As the canonical tables algorithm performs very similar to the automorphism group algorithm in Section 2, we provide examples and runtimes for the automorphism group algorithms only.

For the automorphism group algorithm in Section 2 we first have to choose a series of ideals through L: let $L = L_1 > \cdots > L_l > L_{l+1} = \{0\}$ with L_{i+1} the smallest ideal of L_i with nilpotent factor L_i/L_{i+1}. The nilpotent factors of this series can be refined by their lower central series. The resulting refined series is called lower nilpotent series of L and it is used for our induction process. It can be computed readily by its definition.

For the automorphism group algorithm in Section 2 we first have to compute the nilradical of L. An algorithm for this purpose is available in GAP; we refer to [1] for background.

All runtimes outlined in the tables have been obtained in running GAP under Linux on a PC with processor type P4 and 512 MB ram and they are given in seconds.

4.1. Upper triangular matrices

In Tables 1 and 2 compare the performance of the algorithms in the Sections 2 and 3 for a few well-known small Lie algebras. Let $L = L(n, q)$ be the Lie algebra of all upper triangular matrices of dimension $n \times n$ over the field $\mathbb{F}_q$ with q elements.

4.2. A larger example

Let $L = \langle a_1, \ldots, a_{15} \rangle$ be the 15-dimensional Lie algebra over $\mathbb{F}_2$ defined by the Table 3 of commutators $[a_i, a_j]$. The table contains the commutators for $j \geqslant i$ only,

Table 1
Upper triangular Lie algebras over $\mathbb{F}_2$

(n, q)	dim(L)	|Aut(L)|	Section 2	Section 3
(2, 2)	3	4	0.05	0.01
(3, 2)	6	64	0.21	0.18
(4, 2)	10	1024	3.60	3.29
(5, 2)	15	32 768	?	83.55

Table 2
Upper triangular Lie algebras over $\mathbb{F}_3$

(n, q)	dim(L)	|Aut(L)|	Section 2	Section 3
(2, 3)	3	36	0.10	0.08
(3, 3)	6	3888	0.90	1.01
(4, 3)	10	629 856	?	65.30

Table 3

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
a_1	·	·	·	·	·	·	·	·	·	a_{13}	a_8	a_4	·	a_2	a_1
a_2		·	·	·	·	·	a_2	·	·	a_{14}	a_9	a_5	a_2	·	a_2
a_3			·	·	·	$a_7 + a_{13}$	·	a_4	a_5	·	a_{12}	·	·	·	a_3
a_4				·	·	a_8	·	·	a_2	a_{12}	a_7	·	a_4	a_5	a_4
a_5					·	a_9	a_5	a_2	·	·	a_{14}	·	·	·	a_5
a_6						·	·	·	·	·	·	a_{11}	·	·	a_6
a_7							·	·	a_9	·	·	·	·	a_{14}	·
a_8								·	·	a_{11}	·	a_7	a_8	a_9	·
a_9									·	·	·	a_{14}	·	·	·
a_{10}										·	·	·	·	·	a_{10}
a_{11}											·	·	a_{11}	·	a_{11}
a_{12}												·	a_{12}	·	·
a_{13}													·	a_{14}	·
a_{14}														·	·
a_{15}															·

as we can determine the remaining commutators by $[a_j, a_i] = -[a_i, a_j]$. The entry $\cdot$ denotes 0.

Then the nilradical I of L is abelian and has the basis a_2, a_5, a_9, a_{14}. Using this ideal, we can compute $\mathrm{Aut}(L)$ in 12.9 s and we obtain that $|\mathrm{Aut}(L)| = 11\,520$. This example shows that the improved version of Section 3 is significantly more powerful on examples of this type, since the more general approach of Section 2 did not succeed with this automorphism group computation after several minutes.

References

[1] W. DeGraaf, Lie Algebras: Theory and Algorithms, North-Holland, 2000.
[2] D.J. Robinson, Applications of cohomology to the theory of groups, in: C.M. Campbell, E.F. Robertson (Eds.), Groups—St. Andrews 1981, LMS Lecture Note Series, number 71, Cambridge University Press, 1981, pp. 46–80.
[3] M.J. Smith, Computing Automorphisms of Finite Soluble Groups, Ph.D. thesis, Australian National University, Canberra, 1995.
[4] The GAP Group, GAP—Groups, Algorithms and Programming, 2000. Available from <http://www.gap-system.org>.