CLASSIFYING SEMISIMPLE ORBITS OF $\theta$-GROUPS

WILLEM A. DE GRAAF AND FRANCESCO ORIENTE

Abstract. $\theta$-groups are a class of reductive algebraic groups arising from $\mathbb{Z}/m\mathbb{Z}$-gradings of simple Lie algebras. They were introduced by Vinberg in the 70s, who developed the theory of their orbits. In this paper we describe algorithms to compute certain objects arising in this theory, namely a Cartan subspace, and the little Weyl group. We have implemented the algorithms in the language of the computer algebra system Magma. Practical experiences with the implementations are discussed.

1. Introduction

Let $G$ be a linear algebraic group, acting on a vector space $V$. An orbit of $G$ is said to be closed if it is closed in the Zariski topology. In general it is very hard to classify the closed orbits of $G$. In this paper we consider this problem for the case where $G$ is a connected reductive algebraic group over $\mathbb{C}$ and $(G,V)$ is a $\theta$-representation (see below for the definitions). These form a wide class of linear reductive algebraic groups, where there is a well developed theory of closed orbits, which enables us to develop algorithms for classifying them.

Example 1.1. Maybe the most well-known example of the kind of group action that we deal with is provided by $G = \text{GL}_n(\mathbb{C})$ acting by conjugation on $V = M_n(\mathbb{C})$ (the space of $n \times n$-matrices). In this case an orbit is closed if and only if it consists of semisimple elements. Therefore they are also called semisimple orbits. Every semisimple orbit has a point in the space $D_n(\mathbb{C})$ of diagonal matrices. Moreover, two elements of $D_n(\mathbb{C})$ lie in the same $G$-orbit if and only if they have the same eigenvalues, or, in other words, if they are conjugate under the symmetric group $S_n$, which acts on $D_n(\mathbb{C})$ by permuting the diagonal entries.

This example can be generalised by taking $G$ to be a reductive algebraic group over $\mathbb{C}$, and $V = \mathfrak{g}$, its Lie algebra. Then $G$ acts on $\mathfrak{g}$ by the adjoint representation. An $x \in \mathfrak{g}$ is called semisimple if the adjoint map $\text{ad}_\mathfrak{g}x$ is semisimple (where $\text{ad}_\mathfrak{g}x : \mathfrak{g} \to \mathfrak{g}$ is defined by $\text{ad}_\mathfrak{g}x(y) = [x,y]$). Also in this case the closed orbits are the ones that consist of semisimple elements. Let $\mathfrak{h}$ be a fixed Cartan subalgebra of $\mathfrak{g}$; then, since all Cartan subalgebras are $G$-conjugate (cf. [9], Corollary 16.4), every semisimple orbit has a point in $\mathfrak{h}$. Moreover, two elements of $\mathfrak{h}$ are $G$-conjugate if and only if they are conjugate under the Weyl group $W = N_G(\mathfrak{h})/Z_G(\mathfrak{h})$, which is a finite group.
A further generalisation was introduced by Vinberg (24). We let \( G, \mathfrak{g} \) be as above. Vinberg considered automorphisms \( \theta \) of \( \mathfrak{g} \) of order \( m \). They yield a \( \mathbb{Z}/m\mathbb{Z} \)-grading of \( \mathfrak{g} \),

\[
\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_{m-1},
\]

where \( \mathfrak{g}_i \) is the eigenspace of \( \theta \) with eigenvalue \( \omega^i \), where \( \omega \) is a primitive \( m \)-th root of unity. Let \( G_0 \) be the connected subgroup of \( G \) with Lie algebra \( \mathfrak{g}_0 \). Then \( G_0 \) is reductive and acts on \( \mathfrak{g}_1 \). The group \( G_0 \), together with its action on \( \mathfrak{g}_1 \), is called a \( \theta \)-group. The representation of \( G_0 \) on \( \mathfrak{g}_1 \) is also called a \( \theta \)-representation. Also in this situation an orbit is closed if and only if it consists of elements of \( \mathfrak{g}_1 \) that are semisimple (as elements of \( \mathfrak{g} \)).

**Example 1.2.** Let \( \mathfrak{g} = \mathfrak{sl}_5(\mathbb{C}) \); then \( G = \text{SL}_5(\mathbb{C}) \) acts on \( \mathfrak{g} \) by conjugation. Let \( \omega \in \mathbb{C} \) be a primitive third root of unity. Let \( \theta \) be the automorphism of order 3 of \( \mathfrak{g} \), given by the following matrix:

\[
\begin{pmatrix}
1 & \omega & \omega^2 & \omega^2 & \omega^2 \\
\omega^2 & 1 & \omega & \omega & \omega \\
\omega & \omega^2 & 1 & 1 & 1 \\
\omega & \omega^2 & 1 & 1 & 1 \\
\omega & \omega^2 & 1 & 1 & 1
\end{pmatrix}.
\]

Here, if on position \((i, j)\) there is \( \omega^k \), then \( \theta(e_{i,j}) = \omega^k e_{i,j} \), where \( e_{i,j} \) is the matrix with a 1 on position \((i, j)\) and zeroes elsewhere. Let \( h_i = e_{i,i} - e_{i+1,i+1} \). Then we see that \( \mathfrak{g}_0 \) is spanned by \( h_1, h_2, h_3, h_4, e_{i,j} \) for \( 3 \leq i, j \leq 5 \), which means that \( \mathfrak{g}_0 \cong \mathfrak{sl}_3(\mathbb{C}) \oplus \mathfrak{t}_2 \) (where \( \mathfrak{t}_2 \) denotes the subalgebra spanned by \( h_1, h_2 \)). Furthermore, \( \mathfrak{g}_1 \) is spanned by \( e_{1,2}, e_{2,3}, e_{2,4}, e_{2,5}, e_{3,1}, e_{4,1} \) and \( e_{5,1} \). Finally, \( \mathfrak{g}_2 \) is spanned by \( e_{1,3}, e_{1,4}, e_{1,5}, e_{2,1}, e_{3,2}, e_{4,2} \) and \( e_{5,2} \).

Following [24], a Cartan subspace of \( \mathfrak{g}_1 \) is defined to be a maximal subspace consisting of commuting semisimple elements. Vinberg (24, Theorem 1) showed that all Cartan subspaces are conjugate under \( G_0 \), and their dimension is called the rank of \( \mathfrak{g}_1 \) (or rather of the pair \((G_0, \mathfrak{g}_1)\), or of the \( \theta \)-representation afforded by \( G_0 \) and \( \mathfrak{g}_1 \)). In particular, it follows that every semisimple orbit has a point in a fixed Cartan subspace \( \mathfrak{c} \subset \mathfrak{g}_1 \). Moreover, two elements of \( \mathfrak{c} \) lie in the same \( G_0 \)-orbit if and only if they are conjugate under the little Weyl group \( W_\mathfrak{c} = N_{G_0}(\mathfrak{c})/Z_{G_0}(\mathfrak{c}) \).

Vinberg also showed that \( W_\mathfrak{c} \) is a complex reflection group. By the Chevalley-Shephard-Todd theorem this implies that the ring of invariants \( \mathbb{C}[\mathfrak{c}]^{W_\mathfrak{c}} \) is freely generated by \( r \) fundamental invariants, where \( r \) is the rank of \( \mathfrak{g}_1 \). Moreover, by [24, §4], different semisimple orbits are separated by the polynomial invariants of \( W_\mathfrak{c} \) on \( \mathfrak{c} \). This means that two elements of \( \mathfrak{c} \) lie in different \( W_\mathfrak{c} \)-orbits (and hence in different \( G_0 \)-orbits) if and only if there is at least one fundamental invariant taking different values on these elements.

For this reason we consider the classification of the semisimple orbits to be complete if we have a Cartan subspace, generators of the corresponding little Weyl group, and its fundamental invariants. Fortunately there are algorithms to compute the fundamental invariants of \( W_\mathfrak{c} \), given generators of this group (cf. [3, 22]). (We remark that it is much harder to obtain the invariants of \( G_0 \) acting on \( \mathfrak{g}_1 \); see [2] for an example in type \( E_6 \).) Therefore, the problems that we consider in this paper
are given a semisimple Lie algebra $\mathfrak{g}$ over $\mathbb{C}$ and a finite order automorphism $\theta$ of it, to

- find a Cartan subspace $c$ of $\mathfrak{g}_1$,
- find generators for the little Weyl group $W_c = N_{G_0}(c)/Z_{G_0}(c)$.

For a given $\theta$-group it is possible to try and solve these problems using ad-hoc arguments; we refer to [4], [17], [26] for examples of this. In this paper we develop a more systematic approach using computational techniques. We remark that for all $\theta$-groups, the isomorphism type of $W_c$ is known (combine [24], [14], [15], [19]). Our algorithms go beyond finding the isomorphism type, in the sense that they construct a basis of a Cartan subspace $c$, and generators of the little Weyl group $W_c$, given as matrices with respect to the given basis of $c$.

For this we first need to say a bit about our computational setup. We assume that $\mathfrak{g}$ is given by a multiplication table relative to a Chevalley basis. Then all structure constants in the multiplication table are integers. For different Chevalley bases these structure constants have the same absolute value, so can differ only by their signs. Hence constructing a multiplication table is equivalent to obtaining a valid choice for the signs. This way of constructing a semisimple Lie algebra was first proposed by Tits ([23]). A simpler method is given in the book by Kac ([12], see also [5]). The conjugacy classes (in $\text{Aut}(\mathfrak{g})$) of the finite order automorphisms of $\mathfrak{g}$ have been classified by Kac ([11], see also [7]) in terms of so-called Kac diagrams ([11], see also [25], [7], [18]). Since a Kac diagram is an affine Dynkin diagram where the nodes are labeled by non-negative integers satisfying precise conditions, it is quite straightforward to enumerate all Kac diagrams that yield an automorphism of $\mathfrak{g}$ of a fixed order $m$. From the Kac diagram of an automorphism $\theta$ of order $m$ it is straightforward to compute the matrix of $\theta$ relative to the given basis of $\mathfrak{g}$ (this follows directly from the description of the finite order automorphisms as, for example, given in [7], Chapter X, Theorem 5.15, see also the next section). For this we need to work over the field $\mathbb{Q}(\omega)$, where $\omega$ is a primitive $m$-th root of unity. Then by linear algebra we can construct bases of $\mathfrak{g}_0$ and $\mathfrak{g}_1$. If $\theta$ is an inner automorphism then $\mathfrak{g}_0$ and $\mathfrak{g}_1$ are spanned by root spaces of $\mathfrak{g}$. So, although the matrix of $\theta$ has coefficients in $\mathbb{Q}(\omega)$, the spaces $\mathfrak{g}_0$, $\mathfrak{g}_1$ are defined over $\mathbb{Q}$. In fact, this also happens for outer automorphisms, except for some cases in type $D_4$.

In Section 3 we give a method for constructing a Cartan subspace in $\mathfrak{g}_1$. It is based on the following observations: If $\mathfrak{g}_1$ contains semisimple elements, then the set of non-nilpotent elements is dense in $\mathfrak{g}_1$; so by trying random elements we quickly find a non-nilpotent element, and after computing its Jordan decomposition, a semisimple element. We compute the centraliser of this semisimple element, and reduce the problem to finding a Cartan subspace in there. On the other hand, if $\mathfrak{g}_1$ only contains nilpotent elements, then it has a dense $G_0$-orbit. We can check this by also trying random elements, and computing the dimension of their orbits. So the algorithm uses random choices; however, this does not affect the correctness of the output. It only influences the running time. At the end of Section 3 we give some running times of the algorithm with some sample inputs, obtained with an implementation of the algorithm in the computer algebra system MAGMA ([1]).

In Section 4 we describe methods to compute generators of the little Weyl group $W_c$. First we construct an approximation $C_c$, i.e., a finite group containing $W_c$ as a subgroup. Then we work with explicit elements of $G$ in order to check whether for a given $a \in C_c$ there is a $g \in N_{G_0}(c)$ that projects to $a$. In order to check whether
a given \( g \in G \) lies in \( G_0 \) we need \( G \) to be simply connected. So if \( g \) is of type \( E_8 \) we can take \( G \) to be the automorphism group of \( g \). For other types we consider a suitable representation \( \rho \) of \( g \), and let \( G \) be the connected algebraic group with Lie algebra \( \rho(g) \).

Finally, in the last section we comment on our implementation of the algorithms of Section 4 in MAGMA. Also we discuss how the algorithm behaves in practice, by giving some timings on sample inputs, and other data relevant to the performance of the algorithm. At the end of the section we describe the output of our algorithms for one \( \theta \)-group arising from the Lie algebra of type \( E_6 \).

We do not give estimates for the complexity of our algorithms. It is likely that the algorithm for computing a Cartan subspace runs in polynomial time. However, this algorithm uses random choices, so in order to prove polynomiality we need some estimate on the expected number of random choices that are carried out, but we do not have such an estimate; although in practice very few choices are needed and the algorithm appears to run in time polynomial in \( \dim g \). Regarding the algorithm for obtaining generators of the little Weyl group the problems are even greater. In that algorithm it is sometimes necessary to work over extensions of \( \mathbb{Q} \), but we have no bounds on the degree of the extension needed.

The MAGMA code implementing the algorithms described here is available on the website: http://www.science.unitn.it/degraaf/w0.html

2. Preliminaries

Here we briefly recall some notions regarding semisimple Lie algebras, and their automorphisms. For more detailed accounts we refer to standard works in the literature, such as [9], [10], [25].

Let \( g \) be a semisimple Lie algebra over \( \mathbb{C} \), with fixed Cartan subalgebra \( \mathfrak{h} \). Let \( \Phi \subset \mathfrak{h}^\ast \) denote the root system of \( g \), and let \( \Delta = \{ \alpha_1, \ldots, \alpha_l \} \) be a fixed basis of it. For \( \alpha \in \Phi \),

\[
g_\alpha = \{ x \in g \mid [h, x] = \alpha(h)x \text{ for } h \in \mathfrak{h} \}
\]

denotes the corresponding root space.

The Killing form \( \kappa \) of \( g \) is non-degenerate. Hence we get a bijection \( \mathfrak{h}^\ast \to \mathfrak{h} \), \( \mu \mapsto \hat{\mu} \), where \( \kappa(h, \hat{\mu}) = \mu(h) \) for all \( h \in \mathfrak{h} \). Using this bijection, \( \kappa \) induces a non-degenerate bilinear form \( (\ , \ ) \) on \( \mathfrak{h}^\ast \). For \( \mu \in \mathfrak{h}^\ast \) we set

\[
\mu^\vee = \frac{2\hat{\mu}}{(\mu, \mu)} \in \mathfrak{h}.
\]

Let \( G \) be a connected algebraic group with Lie algebra \( g \). Then the Weyl group of \( g \) is \( N_G(\mathfrak{h})/Z_G(\mathfrak{h}) \). This group is isomorphic to the Weyl group \( W \) of the root system \( \Phi \); a reflection \( s_\alpha \) acts on \( \mathfrak{h} \) by \( s_\alpha(h) = h - \alpha(h)\hat{\alpha}^\vee \).

We use canonical sets of generators of \( g \) (cf. [10]), which correspond to bases of \( \Phi \). A canonical set of generators corresponding to the basis \( \Delta \) consists of elements \( x_1, \ldots, x_l, y_1, \ldots, y_l, h_1, \ldots, h_l \), where \( x_i \in g_{\alpha_i}, y_i \in g_{-\alpha_i} \), the \( h_i \in \mathfrak{h} \) form a basis of \( \mathfrak{h} \) and

\[
[h_i, h_j] = 0,
[x_i, y_j] = \delta_{ij} h_i,
[h_i, x_j] = \langle \alpha_j, \alpha_i^\vee \rangle x_j,
[h_i, y_j] = -\langle \alpha_j, \alpha_i^\vee \rangle y_j.
\]
In particular, this means that $h_i = \alpha_i^\vee$. For the proof of the following lemma we refer to [5], Section 5.11.

**Lemma 2.1.** Let $\{\tilde{\alpha}_1, \ldots, \tilde{\alpha}_l\}$ be a basis of $\Phi$. Let $1 \leq i \leq l$ and let $\tilde{x}_i$ be a non-zero element of $\mathfrak{g}_{\tilde{\alpha}_i}$. Then there exists a non-zero $\tilde{y}_i \in \mathfrak{g}_{-\tilde{\alpha}_i}$ such that, by setting $\tilde{h}_i = [\tilde{x}_i, \tilde{y}_i]$, we have $[\tilde{h}_i, \tilde{x}_i] = 2\tilde{x}_i$. Moreover, the $\tilde{x}_i, \tilde{y}_i, \tilde{h}_i$ for $1 \leq i \leq l$ form a canonical generating set of $\mathfrak{g}$.

We note that we can find the $\tilde{y}_i$ as in the lemma by solving a set of linear equations. Hence the lemma provides an algorithm for finding a canonical generating set, given a basis of $\Phi$.

An automorphism of $\mathfrak{g}$ can be described by giving the images of the elements of a canonical generating set. Conversely, given any canonical generating set, $x'_i, y'_i$ and $h'_i$ with the same commutation relations as above, then the map sending $x_i$ to $x'_i$, $y_i$ to $y'_i$, $h_i$ to $h'_i$ is an automorphism of $\mathfrak{g}$.

The conjugacy classes of the finite order automorphisms of $\mathfrak{g}$ are parametrised by Kac diagrams. Here we briefly indicate what a Kac diagram is, and how to construct it. For a much more detailed description we refer to [25], Chapter 3, [7], Section X.5, or [18]. Let $\alpha_0$ denote the lowest root of $\Phi$. Then the Dynkin diagram of the roots $\alpha_0, \ldots, \alpha_l$ is called the extended Dynkin diagram of $\Phi$ (or of $\mathfrak{g}$). Let $n_i \in \mathbb{Z}$ be such that $\alpha_0 = -\sum_{i=0}^l n_i \alpha_i$ and set $n_0 = 1$. Let $s_0, \ldots, s_l$ be non-negative integers with $\gcd(s_0, \ldots, s_l) = 1$, and let $m = \sum_{i=0}^l n_i s_i$. Let $\omega \in \mathbb{C}$ be a primitive $m$-th root of unity. Let $x_0$ be a non-zero element of $\mathfrak{g}_{\alpha_0}$. Then $x_0, \ldots, x_l$ generate $\mathfrak{g}$. Moreover, $x_i \mapsto \omega^{s_i} x_i \ (0 \leq i \leq l)$ defines an automorphism of $\mathfrak{g}$ of order $m$. The Kac diagram of this automorphism is the extended Dynkin diagram with labels $s_0, \ldots, s_l$. In terms of the canonical generating set the automorphism is given by $x_i \mapsto \omega^{s_i} x_i, y_i \mapsto \omega^{-s_i} y_i, h_i \mapsto h_i (1 \leq i \leq l)$.

Now we describe how an element of the Weyl group can be lifted to an automorphism of $\mathfrak{g}$. Let $w \in W$; then

$$w(h_i) = w(\alpha_i^\vee) = w(\alpha_i)^\vee.$$ 

Let $x'_i$ be a non-zero element of $\mathfrak{g}_{w(\alpha_i)}$, and let $y'_i \in \mathfrak{g}_{-w(\alpha_i)}$ be such that $[[x'_i, y'_i], x'_i] = 2x'_i$. Set $h'_i = [x'_i, y'_i]$. Then by Lemma 2.1 the $x'_i, y'_i, h'_i$ form a canonical generating set of $\mathfrak{g}$. Hence the map sending $x_i \mapsto x'_i, y_i \mapsto y'_i, h_i \mapsto h'_i$ extends to an automorphism $\sigma_w$ of $\mathfrak{g}$. Moreover, $h'_i = w(\alpha_i)^\vee = w(\alpha_i^\vee) = w(h_i)$. Hence $\sigma_w$ is an automorphism of $\mathfrak{g}$, stabilising $\mathfrak{h}$, and such that its restriction to $\mathfrak{h}$ coincides with $w$.

Now let $\sigma$ be an automorphism of $\mathfrak{g}$, stabilising $\mathfrak{h}$, and such that its restriction to $\mathfrak{h}$ is the identity. Then $\sigma(h_i) = h_i$. Moreover, the $\sigma(x_i), \sigma(y_i)$ lie in $\mathfrak{g}_{\alpha_i}, \mathfrak{g}_{-\alpha_i}$, respectively. So $\sigma(x_i) = \lambda_i x_i, \sigma(y_i) = \mu_i y_i$. Since $[x_i, y_i] = h_i$ we get that $\lambda_i \mu_i = 1$. Conversely, if we take arbitrary $\lambda_i \in \mathbb{C}, \lambda_i \neq 0$, and set $\mu_i = \frac{1}{\lambda_i}$, then the $h_i, \lambda_i x_i, \mu_i y_i$ form a canonical generating set of $\mathfrak{g}$. So we get a corresponding automorphism of $\mathfrak{g}$, that is the identity on $\mathfrak{h}$. This gives us an explicit description of those automorphisms that are the identity on $\mathfrak{h}$. They depend on $l$ non-zero parameters.
3. Constructing a Cartan subspace

In this section we let \( \mathfrak{g} \) be a reductive Lie algebra with a \( \mathbb{Z}/m\mathbb{Z} \)-grading, \( \mathfrak{g} = \bigoplus_{i=0}^{m-1} \mathfrak{g}_i \). A Cartan subspace of \( \mathfrak{g}_1 \) is a maximal subspace consisting of semisimple commuting elements. Here we describe an algorithm for computing such a Cartan subspace.

In the algorithm we need to compute the Jordan decomposition of elements of semisimple Lie algebras. This can be done as follows. Let \( x \in \mathfrak{s} \), with \( \mathfrak{s} \) a semisimple Lie algebra. Compute the Jordan decomposition of the adjoint map \( \text{ad}_x = S + N \), with \( S \) semisimple and \( N \) nilpotent. Then there are unique \( x_s, x_n \in \mathfrak{s} \) such that \( S = \text{ad}_x x_s \) and \( N = \text{ad}_x x_n \). Moreover, we can find these elements by solving systems of linear equations. Furthermore, the Jordan decomposition of \( x \) is \( x = x_s + x_n \).

Next we give the algorithm for computing a Cartan subspace. In the algorithm a parameter \( R \) is used. It is a positive integer, fixed throughout. The behaviour of the algorithm depends on it. For the explanation of the algorithm we refer to the proof of Proposition \( \ref{prop:cartan} \).

**Algorithm 1.** Input: a reductive \( \mathbb{Z}/m\mathbb{Z} \)-graded Lie algebra \( \mathfrak{g} \). Output: a Cartan subspace of \( \mathfrak{g}_1 \).

1. Let \( \mathfrak{s} = [\mathfrak{g}, \mathfrak{g}] \) and let \( \mathfrak{r} \) be the centre of \( \mathfrak{g} \). Let \( \mathfrak{s}_1 = \mathfrak{s} \cap \mathfrak{g}_1 \).
2. If \( \mathfrak{s}_1 = 0 \) then return \( \mathfrak{g}_1 \).
3. Let \( x_1, \ldots, x_m \) be a basis of \( \mathfrak{s}_1 \), and set \( x = \sum_{i=1}^{m} c_i x_i \), where the \( c_i \) are drawn randomly uniformly and independently from the set \( \Omega = \{0, \ldots, R\} \).
4. If \( x \) is not nilpotent, then execute Step 4(a). Otherwise execute Step 4(b).
   a. \( (x \text{ not nilpotent}) \) Compute the Jordan decomposition \( x = x_s + x_n \). Let \( \tilde{\mathfrak{g}} \) be the centraliser of \( x_s \) in \( \mathfrak{g} \). Return the output of the algorithm when applied recursively to \( \tilde{\mathfrak{g}} \), with the grading induced by the grading of \( \mathfrak{g} \).
   b. \( (x \text{ is nilpotent}) \) Set \( \mathfrak{s}_0 = \mathfrak{s} \cap \mathfrak{g}_0 \). Compute \([\mathfrak{s}_0, x] \); if the dimension of this space is equal to the dimension of \( \mathfrak{s}_1 \), then return \( \mathfrak{g}_1 \cap \mathfrak{r} \). Otherwise return to Step 3.

**Proposition 3.1.** If Algorithm 1 terminates, then it returns a Cartan subspace of \( \mathfrak{g}_1 \). Moreover, the probability that the algorithm terminates tends to 1 as \( R \) tends to \( \infty \).

**Proof.** The first statement is shown by induction on the dimension of \( \mathfrak{g} \), the induction hypothesis being that the statement is true for all reductive graded Lie algebras of dimension less than \( \dim \mathfrak{g} \).

We note that since \( \mathfrak{g} \) is reductive, \( \mathfrak{g} = \mathfrak{s} \oplus \mathfrak{r} \), with \( \mathfrak{s} \) semisimple. Let \( \theta \) be the automorphism corresponding to the grading of \( \mathfrak{g} \), i.e., \( \theta(x) = \omega^m x \) for \( x \in \mathfrak{g}_i \), where \( \omega \) is a primitive \( m \)-th root of unity. Then \( \theta \) stabilises \( \mathfrak{s} \) and \( \mathfrak{r} \). Hence \( \mathfrak{s} \) is also graded, where the grading is induced by the grading of \( \mathfrak{g} \). Furthermore, \( \mathfrak{g}_1 = (\mathfrak{g}_1 \cap \mathfrak{s}) \oplus (\mathfrak{g}_1 \cap \mathfrak{r}) \). Note that \( \mathfrak{g}_1 \cap \mathfrak{r} \) is always contained in a Cartan subspace. So if \( \mathfrak{g}_1 \cap \mathfrak{s} = 0 \), then \( \mathfrak{g}_1 \cap \mathfrak{r} \) and hence \( \mathfrak{g}_1 \) is a Cartan subspace of \( \mathfrak{g}_1 \).

If the \( x \) found in Step 3 is not nilpotent, then its semisimple part, \( x_s \), also lies in \( \mathfrak{s} \). Therefore, its centraliser, \( \tilde{\mathfrak{g}} \), is strictly contained in \( \mathfrak{g} \). Furthermore, it is reductive as \( x_s \) is semisimple. Hence by induction the algorithm, with input \( \tilde{\mathfrak{g}} \), computes a Cartan subspace, \( \mathfrak{c} \) of \( \tilde{\mathfrak{g}}_1 \). Then \( \mathfrak{c} \) is a Cartan subspace of \( \mathfrak{g} \). Indeed, \( x_s \) is contained in a Cartan subspace \( \mathfrak{c}' \) of \( \mathfrak{g}_1 \). But \( \mathfrak{c}' \) is also contained in \( \tilde{\mathfrak{g}} \). Now \( x_s \) is an eigenvector of \( \theta \), so it is also an eigenvector of \( \theta^{-1} \). This implies that \( \tilde{\mathfrak{g}} \).
is $\theta$-stable. Therefore, $\tilde{g}_1 = g_1 \cap \tilde{g}$. Now $y \in \tilde{g}$ is semisimple as an element of $\tilde{g}$ if and only if it is semisimple as an element of $g$. It follows that $c'$ is a maximal commutative subspace of $\tilde{g}$, consisting of semisimple elements. In other words, it is a Cartan subspace of $\tilde{g}_1$. So $c'$ is $G_0$-conjugate to $c$ (where $G_0$ is the subgroup of $G$ corresponding to $\tilde{g}_0$). Hence $c$ is a Cartan subspace of $g_1$.

If, on the other hand, $x$ is nilpotent, then $[s_0, x]$ is the tangent space to the orbit $S_0 \cdot x$, where $S_0 \subset G_0$ is the group corresponding to $s_0$. If the dimension of this orbit equals the dimension of $s_1$, then $s_1$ contains an open nilpotent orbit (namely $S_0 \cdot x$). This implies that $s_1$ consists entirely of nilpotent elements. Indeed, the set of non-nilpotent elements in $s_1$ is open. If it is non-empty, then it has to have a non-empty intersection with the open nilpotent orbit, which is not possible. Hence in this case $g_1 \cap r$ is a Cartan subspace of $g_1$.

Now we turn to the question of termination. If the algorithm does not terminate, then the algorithm enters an infinite loop in steps 3 to 5. This means that the element found in Step 3 is always nilpotent. But for large $R$ that means that $s_1$ consists of nilpotent elements, as the set of non-nilpotent elements is open (and therefore dense, when non-empty). By [24], §2.6, this implies that $s_1$ has an open nilpotent orbit. Again for large $R$ that means that at some point a random $x$ is found that lies in the open nilpotent orbit. But that contradicts the assumption that we have an infinite loop.

**Remark 3.2.** Proposition 3 holds that the algorithm works when $R$ is large enough. In practice however, it turns out that it is enough to take a small $R$. In our implementation we have used $R = 2$, and hence $\Omega = \{0, 1\}$. On some occasions this makes it necessary to perform more iterations; but the upside of this approach is that the coefficients of the elements involved are much nicer. Of course, with such a small $R$ it is not guaranteed that the algorithm terminates. This can be remedied by increasing $R$ if, after a few rounds of the iteration, no “good” element has been found (i.e., a semisimple element, or a nilpotent element lying in a dense orbit).

**Remark 3.3.** Algorithm 1 may not work for reductive Lie algebras in characteristic $p > 0$. However, using some results of Levy ([14]) it is possible to formulate a variant of the algorithm that also works in characteristic $p > 2$. Levy proved ([14], Lemma 1.12) that the following are equivalent:

- $g_1$ contains no non-central semisimple elements.
- $g_1 = s \oplus n$, where $s$ and $n$ are the sets of semisimple and nilpotent elements of $g_1$, respectively, and $s \subset \mathfrak{z}(g)$ (the centre of $g$).

Moreover, suppose that $g_1$ has non-central semisimple elements. Let $x \in g_1$ be a randomly chosen element, with Jordan decomposition $x = x_s + x_n$. Then from [14], Lemma 2.16, it follows that $x_s$ is non-central with high probability.

We proceed as follows. Let $x$ be a randomly chosen element of $g_1$, with Jordan decomposition $x = x_s + x_n$. If $x_s$ is non-central, then we construct $\tilde{g}$ as in Algorithm 1 and apply the algorithm to $\tilde{g}$. If $x_s$ is central, then we compute the Jordan decomposition of all basis elements of $g_1$. Let $s$, $n$ be the subspaces spanned by all semisimple and nilpotent parts, respectively. If $g_1 = s \oplus n$ and $s$ is contained in the centre of $g$, and all elements of $n$ are nilpotent, then the output is $s$. If one of these conditions is not satisfied, then we choose another random element, and repeat the process.
If the characteristic is small, then the set $\Omega$ used in the algorithm may be too small. In that case one can replace $\Omega$ by a finite field of characteristic $p$, of at least $R$ elements.

**Example 3.4.** Let $\mathfrak{g}$ and $\theta$ be as in Example 1.2. Consider the element $u = e_{1,2} + e_{2,3} + e_{3,1} \in \mathfrak{g}_1$. Its minimum polynomial is $x^4 - x$, and therefore $u$ is semisimple. The centraliser of $u$ in $\mathfrak{g}$, $\mathfrak{g}_u$, is spanned by $e_4, e_5, e_6, h_4, h_1 + 2h_2 + 3h_3$, $u, e_{1,3} + e_{2,1} + e_{3,2}$. Here the first four elements lie in $\mathfrak{g}_0$, and the last two in $\mathfrak{g}_1$ and $\mathfrak{g}_2$, respectively. We have that $\mathfrak{g}_u = \mathfrak{s} \oplus \mathfrak{r}$, where $\mathfrak{s}$ is spanned by $e_4, e_5, h_4$. We see that $\mathfrak{s}$ is contained in $\mathfrak{g}_0$. So a Cartan subspace of $\mathfrak{g}_u$, and hence of $\mathfrak{g}$, is $\mathfrak{g}_1 \cap \mathfrak{r}$, which is spanned by $u$. In particular, the rank of $\mathfrak{g}_1$ is 1.

We have implemented the algorithm in the computer algebra system MAGMA ([1]). In Table 1 we give the running times on some sample inputs. The timings have been obtained on a 3.16 GHz processor.

<table>
<thead>
<tr>
<th>Type</th>
<th>Kac diagram</th>
<th>Rank</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_6$</td>
<td>eeuee</td>
<td>3</td>
<td>1.1</td>
</tr>
<tr>
<td>$E_7$</td>
<td>eeuee</td>
<td>3</td>
<td>5.8</td>
</tr>
<tr>
<td>$E_8$</td>
<td>eeuee</td>
<td>4</td>
<td>56.3</td>
</tr>
<tr>
<td>$D_8$</td>
<td>eueee</td>
<td>4</td>
<td>3.9</td>
</tr>
</tbody>
</table>

We see that the running times increase rather sharply with the dimension of the Lie algebra. The data given here suggests that the running time behaves like $c(\dim \mathfrak{g})^{3.4}$, where $c$ is a constant. This is no surprise, as the algorithm mainly deals with matrices of adjoint maps $\text{ad}_g x$, so $\dim \mathfrak{g}$ should be the main parameter influencing the running time.

4. The little Weyl group

Here we let $\mathfrak{g}$ be a simple Lie algebra over $\mathbb{C}$, with a finite order automorphism $\theta$. We let $G$ be a simply connected algebraic group with Lie algebra $\mathfrak{g}$. Then there exists an automorphism $\hat{\theta}$ of $G$, with differential equal to $\theta$. Also, $G_0$ (which is defined to be the connected algebraic subgroup of $G$ with Lie algebra $\mathfrak{g}_0$) is equal to $G^\theta = \{ g \in G \mid \hat{\theta}(g) = g \}$ ([24], §2).

Let $\mathfrak{c}$ be a Cartan subspace of $\mathfrak{g}_1$. In this section we consider the problem of computing the little Weyl group, $W_\mathfrak{c} = N_{G_0}(\mathfrak{c})/Z_{G_0}(\mathfrak{c})$. According to a theorem of Vinberg this group is generated by complex reflections that act on the space $\mathfrak{c}$. We
want to find a set of complex reflections, given by their matrices with respect to a fixed basis of \( \mathfrak{c} \), that generate \( W_\mathfrak{c} \). We divide this section into several subsections.

4.1. **Approximating \( W_\mathfrak{c} \) from above.** In this subsection we describe an algorithm to construct a finite subgroup of \( \text{GL}(\mathfrak{c}) \) containing \( W_\mathfrak{c} \). This is based on the construction of a \( \theta \)-stable Cartan subalgebra, due to Levy ([14]).

Let \( \mathfrak{t} \) be the unique minimal algebraic torus in \( \mathfrak{g} \) containing \( \mathfrak{c} \). Throughout we set \( \mathfrak{s} = \mathfrak{z}_0(\mathfrak{c}) \) (the centraliser of \( \mathfrak{c} \) in \( \mathfrak{g} \)). Then \( \mathfrak{s} \) is a reductive subalgebra. Moreover, it is \( \theta \)-stable and hence graded, \( \mathfrak{s}_k = \mathfrak{s} \cap \mathfrak{g}_k \).

**Lemma 4.1.** Let \( \mathfrak{z}(\mathfrak{s}) \) denote the centre of \( \mathfrak{s} \). Then

\[
\mathfrak{t} = \bigoplus_{\gcd(k,m)=1} \mathfrak{g}_k \cap \mathfrak{z}(\mathfrak{s}).
\]

**Proof.** By [24], §3.1 we have \( \mathfrak{t} = \bigoplus_{\gcd(k,m)=1} \mathfrak{t} \cap \mathfrak{g}_k \). Since \( \mathfrak{s} \) is reductive, its centre consists of semisimple elements. Hence \( \mathfrak{z}(\mathfrak{s}) \) is an algebraic torus containing \( \mathfrak{c} \). Therefore it contains \( \mathfrak{t} \). So the left-hand side is contained in the right-hand side.

For the converse, let \( k \) be such that \( \gcd(k,m) = 1 \). Then \( \mathfrak{g}_1 \) and \( \mathfrak{g}_k \) have the same rank (which is the dimension of a maximal commutative subspace consisting of semisimple elements). Indeed: in [24], §3.1 it is shown that \( \text{rank}(\mathfrak{g}_1) \leq \text{rank}(\mathfrak{g}_k) \), but the same arguments, starting with \( \mathfrak{g}_k \) instead of \( \mathfrak{g}_1 \), show the reverse inequality. This implies that the right-hand side cannot be strictly bigger than the left-hand side (as, by [24], §3.1, all \( \mathfrak{t} \cap \mathfrak{g}_k \) have the same dimension).

The next lemma, as well as Proposition 4.3 are taken from [14].

**Lemma 4.2.** Let \( \mathfrak{t}_0 \) be a Cartan subalgebra of \( \mathfrak{s}_0 \). Then \( \mathfrak{h} = \mathfrak{z}_0(\mathfrak{t}_0 + \mathfrak{t}) \) is a \( \theta \)-stable Cartan subalgebra of \( \mathfrak{g} \) containing \( \mathfrak{c} \).

**Proof.** We have that \( \mathfrak{t}_0, \mathfrak{t} \) are \( \theta \)-stable; hence this holds for \( \mathfrak{h} \) as well. Let \( \mathfrak{h}' \) be a Cartan subalgebra of \( \mathfrak{g} \) containing \( \mathfrak{c} \). Then it contains \( \mathfrak{t} \) as well. Also, \( \mathfrak{h}' \subset \mathfrak{s} \), and hence \( \mathfrak{h}' \) is a Cartan subalgebra of \( \mathfrak{s} \). But by [7], Chapter X, Lemma 5.3, \( \mathfrak{s}_0 \) contains a regular element of \( \mathfrak{s} \) (i.e., an element of which the centraliser is a Cartan subalgebra of \( \mathfrak{s} \)). So \( \mathfrak{h}' \) is \( S \)-conjugate to \( \mathfrak{z}_s(\mathfrak{t}_0) \) (here \( S \) is the connected subgroup of \( G \) with Lie algebra \( \mathfrak{s} \)). In particular, also \( \mathfrak{z}_s(\mathfrak{t}_0) \) is a Cartan subalgebra of \( \mathfrak{g} \). But \( \mathfrak{z}_s(\mathfrak{t}_0) \) is equal to \( \mathfrak{z}_\mathfrak{t}(\mathfrak{t}_0 + \mathfrak{t}) \). (Note that a semisimple element of \( \mathfrak{g} \) that centralises \( \mathfrak{c} \) has to centralise \( \mathfrak{t} \) as well.) It is clear that \( \mathfrak{h} \) contains \( \mathfrak{c} \).

Let \( \mathfrak{h} \) be as in the previous lemma. Let \( W = \text{N}_G(\mathfrak{h})/\text{Z}_G(\mathfrak{h}) \) be the corresponding Weyl group. Since \( \mathfrak{h} \) is \( \theta \)-stable we can consider the centraliser \( W^\theta \) of \( \theta \) in \( W \). Let \( w \in W^\theta \) and \( x \in \mathfrak{c} \). Then \( w(x) \in \mathfrak{h} \cap \mathfrak{g}_1 = \mathfrak{c} \). So \( w \) stabilises \( \mathfrak{c} \), and we get a map

\[
\pi : W^\theta \to \text{GL}(\mathfrak{c})
\]

by restriction, \( \pi(w) = w|_\mathfrak{c} \). Throughout we set \( \mathcal{C}_\mathfrak{c} = \pi(W^\theta) \).

**Proposition 4.3.** \( W_\mathfrak{c} \subset \mathcal{C}_\mathfrak{c} \).

**Proof.** Let \( a \in W_\mathfrak{c} \), and let \( g \in \text{N}_{G_0}(\mathfrak{c}) \) be a representative of it. Set \( L = \text{Z}_G(t) \), which is a subgroup of \( G \) with Lie algebra \( \mathfrak{l} = \mathfrak{z}_0(\mathfrak{t}) \). Now \( g(t) \) is an algebraic torus of \( \mathfrak{g} \) containing \( \mathfrak{c} \); hence \( g(t) = t \). This implies that \( g^{-1}Lg = L \), and \( g(l) = l \).

Furthermore, \( \mathfrak{l} \) is \( \theta \)-stable, hence it is graded, and \( \mathfrak{l}_0 \) contains \( \mathfrak{t}_0 \). Hence \( \mathfrak{l}_0 \) is a Cartan subalgebra of \( \mathfrak{l}_0 \). Since \( g \) lies in \( G_0 = \mathcal{G}^\theta \), it leaves the grading invariant,
and hence \( g(t_0) \) is a Cartan subalgebra of \( L_0 \). So there is an \( h \in L_0 \subset G_0 \) with \( hg(t_0) = t_0 \) (where \( L_0 \) denotes the connected subgroup of \( G \) with Lie algebra \( L_0 \)).

Since \( h \in L \) also \( hg(t) = t \). But \( h \) is the centraliser of \( t_0 + t \). It follows that \( hg(h) = h \). Also, \( hg \in G_0 \subset G^\theta \), hence \( (hg)|_h \in W^\theta \). Moreover, \( (hg)|_c = g|_c \) as \( h \in L \). So if we write \( w = (hg)|_h \), then \( \pi(w) = a \). □

Let \( \Phi \) be the root system of \( g \) with respect to \( h \). Let \( \Delta = \{ \alpha_1, \ldots, \alpha_l \} \) be a fixed basis of \( \Phi \). Then \( W \) is isomorphic to the Weyl group of \( \Phi \), which is generated by the simple reflections \( s_i = s_{\alpha_i} \). Such a reflection acts on \( h \) by \( s_i(h) = h - \alpha_i(h)\alpha_i^\vee \). Now an element of \( W \) permutes the set \( \{ \alpha^\vee \mid \alpha \in \Phi \} \). This yields a faithful permutation representation of \( W \). Also, \( \theta \) permutes the \( \alpha^\vee \), and hence we can compute a generating set of \( W^\theta \) by using permutation group algorithms (see [8, 20]).

We summarise our findings in the following algorithm.

**Algorithm 2.** Input: a simple \( \mathbb{Z}/m\mathbb{Z} \)-graded Lie algebra \( g \), and a Cartan subspace \( c \) of \( g_1 \).

**Output:** generators of \( C_c \).

\[
\begin{align*}
1 & \text{ Set } s = \mathfrak{z}_0(c) \text{ and } t = \bigoplus_{\gcd(k,m)=1} \mathfrak{g}_k \cap \mathfrak{z}(s). \\
2 & \text{ Compute a Cartan subalgebra } t_0 \text{ of } \mathfrak{z}_0 \text{ and set } \mathfrak{h} = \mathfrak{z}_0(t_0 + t). \\
3 & \text{ Compute the root system } \Phi \text{ of } g \text{ with respect to } \mathfrak{h}. \text{ Set } X = \{ \alpha^\vee \mid \alpha \in \Phi \}. \\
4 & \text{ Compute the permutation action of the generators of } W, \text{ and of } \theta, \text{ on } X. \\
5 & \text{ Using the permutations computed in the previous step, compute generators of } W^\theta. \\
6 & \text{ For each generator of } W^\theta \text{ compute its restriction to } c. \text{ Return the subset of } \text{GL}(c) \text{ so obtained. }
\end{align*}
\]

**Remark 4.4.** This algorithm works verbatim when \( g \) is defined over a field of characteristic \( p > 2 \). In order to prove Lemma 4.4 for that situation one can use [14], Lemma 1.10. Lemma 4.2 and Proposition 4.3 were proved for characteristic \( p > 2 \) in [14].

4.2. **Generators of \( W_c \).** Since we can compute a finite group \( C_c \) containing \( W_c \), the remaining problem is to decide, for a given \( a \in C_c \), whether \( a \in W_c \).

We have the following scheme:

\[
N_G(h) \xrightarrow{\psi} W \supset W^\theta \xrightarrow{\pi} C_c \supset W_c.
\]

(Here \( \psi : N_G(h) \to N_G(h)/Z_G(h) = W \) is the projection.) Let \( a \in C_c \). Then \( a \in W_c \) if and only if there is a \( g \in N_G(h) \) such that

\[
\begin{align*}
\bullet & \psi(g) \in W^\theta \text{ and } \pi(\psi(g)) = a, \\
\bullet & g \in G_0 \text{ or, equivalently, } \hat{\theta}(g) = g.
\end{align*}
\]

So in order to construct the little Weyl group \( W_c \) we need to decide whether, for a given \( a \in C_c \) there exists a \( g \in N_G(h) \) with the above properties. For this we need an explicit realisation of \( G \). How we obtain it depends on \( g \). We consider two cases, to which we devote two separate subsections.

4.2.1. **Simply connected automorphism group.** The first case is when the inner automorphism group of \( g \) is simply connected. This happens when \( g \) is of type \( E_6, F_4, G_2 \). In these cases we take \( G = \text{Aut}(g) \) and identify \( g \) and the Lie algebra of
is not simply connected, which happens when we do not know how to work with automorphisms of \( G \) (see Section 4.2.2).

In these cases \( \theta \in G = \text{Aut}(\mathfrak{g}) \). Hence we can define \( \hat{\theta} \) by \( \hat{\theta}(g) = \theta g \theta^{-1} \). So we can decide whether a given \( g \in G \) lies in \( G_0 \) by checking the condition \( \hat{\theta}(g) = g \).

Let \( a \in C_c \), and \( K_a = \pi^{-1}(a) = \{ w \in W^\theta | \pi(w) = a \} \). (Note that this is a finite set.) Let \( w \in K_a \), and let \( \sigma_w \in G \) be an automorphism of \( \mathfrak{g} \) stabilising \( \mathfrak{h} \), and such that its restriction to \( \mathfrak{h} \) is equal to \( w \). (As seen in Section 2, we can effectively compute \( \sigma_w \).) Then the set of \( g \in N_G(\mathfrak{h}) \) such that \( \psi(g) = w \) is equal to \( \sigma_w Z_G(\mathfrak{h}) \).

Now in Section 2 we have given a description of \( Z_G(\mathfrak{h}) \): we can represent a generic element \( g_0 \) of \( Z_G(\mathfrak{h}) \) by a matrix (which is its matrix relative to a fixed basis of \( \mathfrak{g} \)) depending on \( l \) independent parameters, \( \lambda_1, \ldots, \lambda_l, \mu_1, \ldots, \mu_l \), with \( \lambda_i \mu_i = 1 \). Set \( g = \sigma_w g_0 \), then \( g \in G_0 \) if and only if \( \theta g = g \theta \). This is equivalent to a system of polynomial equations in \( \lambda_i, \mu_i \). Computing a Gröbner basis we can check whether this system has a solution over \( \mathbb{C} \). Here it is important to note that we do not need to solve the equations. If the reduced Gröbner basis is not \( \{1\} \), then the system has a solution, and hence \( a \in W_c \). We perform this for all \( w \in K_a \); if the resulting reduced Gröbner basis is always equal to \( \{1\} \), then \( a \notin W_c \).

In the next algorithm we assume that \( G = \text{Aut}(\mathfrak{g}) \) is simply connected.

**Algorithm 3.** Input: a simple \( \mathbb{Z}/m\mathbb{Z} \)-graded Lie algebra \( \mathfrak{g} \), and a Cartan subspace \( c \) of \( \mathfrak{g}_1 \).

Output: generators of \( W_c \).

1. Compute generators of \( C_c \) (Algorithm 2).
2. Denote by \( g_0 \) the generic element of \( Z_G(\mathfrak{h}) \), depending on \( l \) independent parameters \( \lambda_1, \ldots, \lambda_l \).
3. Set \( G = \emptyset \).
4. For each \( a \in C_c \) do
   a. Compute \( K_a \).
   b. For each \( w \in K_a \) do
      i. Compute \( \sigma_w \in G \) such that \( \sigma_w |_{\mathfrak{h}} = w \).
      ii. Construct the set \( P \) of polynomial equations equivalent to \( \theta \sigma_w g_0 = \sigma_w g_0 \theta \).
      iii. Compute a reduced Gröbner basis of \( P \). If this is not \( \{1\} \) then add \( a \) to \( G \), and jump to the next element of \( C_c \).

4.2.2. The automorphism group is not simply connected. Now suppose that \( \text{Aut}(\mathfrak{g})^\circ \) is not simply connected, which happens when \( \mathfrak{g} \) is of type \( E_6, E_7 \), or of classical type. We assume that \( \mathfrak{g} \) is of one of these types, but not of type \( D_{2n} \). In Remark 4.16 we indicate what has to be changed for \( \mathfrak{g} \) of type \( D_{2n} \).

We consider a finite dimensional irreducible representation \( \rho: \mathfrak{g} \to \mathfrak{gl}(V) \), and we let \( G \) be the connected subgroup of \( \text{GL}(V) \) with Lie algebra \( \rho(\mathfrak{g}) \). We choose \( \rho \) such that \( G \) is simply connected. Theorem 2.18 of [2] exactly describes the representations that satisfy this condition. For example, for types \( E_6, E_7 \) we can take the smallest dimensional representation, where \( V \) is of dimension 27 and 56 respectively.

Note that \( G \) acts on \( \rho(\mathfrak{g}) \) by automorphisms \( \text{Ad}(\rho)(\rho(x)) = g \rho(x) g^{-1} \). This yields a surjective map \( \varphi: G \to \text{Aut}(\mathfrak{g})^\circ \), with kernel equal to the centre of \( G \). (In type \( E_6, E_7 \), with \( \rho \) as before, this is the group of scalar matrices, with a third,
respectively second, root of unity on the diagonal.) We want to compute generators of $W_c$ along the lines of Algorithm 3, but with the group $G$ instead of $\text{Aut}(g)$. For this we need to solve three problems:

1. Compute an automorphism $\hat{\theta}$ of $G$ with differential $\theta$.
2. Compute a generic element $g_0$ of $Z_G(h)$, depending on $l$ independent parameters.
3. For $w \in W$ compute $g_w \in G$ such that $g_w|_h = w$.

One problem is that we have no way of directly working with elements of $G$. Therefore we consider the larger group

$$\tilde{G} = N_{\text{GL}(V)}(\rho(g)) = \{ g \in \text{GL}(V) \mid g \rho(g) g^{-1} = \rho(g) \}.$$  

We solve the problems outlined above for $\tilde{G}$, and then show that this yields an algorithm for computing generators of $W_c$.

Note that $\tilde{G}$ acts on $g$ by automorphisms; we let $\varphi : \tilde{G} \to \text{Aut}(g)$ be the corresponding map. (Since $G \subset \tilde{G}$ it is justified to use the same symbol $\varphi$.) For $\sigma \in \text{Aut}(g)$ set

$$U_\sigma = \{ u \in \text{End}(V) \mid u \rho(x) = \rho(\sigma(x)) u \text{ for all } x \in g \}.$$  

We have that $u \in U_\sigma$ if and only if $u \rho(x) = \rho(\sigma(x)) u$, for $x$ in a basis of $g$. Therefore, we can compute a basis of $U_\sigma$ by solving a set of linear equations.

**Lemma 4.5.** Let the notation be as above. Set $R = \{ \lambda \cdot I_V \mid \lambda \in \mathbb{C}^* \}$, where $I_V \in \text{End}(V)$ is the identity transformation. Then:

1. $\dim U_\sigma = 1$.
2. $\tilde{G} = GR$.
3. Let $u \in U_\sigma$, $u \neq 0$; then $u \in \tilde{G}$.

**Proof.** We have that $U_\sigma \cap \text{GL}(V)$ is equal to the fibre $\varphi^{-1}(\sigma)$. If we let $\sigma$ be the identity, then this fibre is an algebraic subgroup whose Lie algebra is $\mathfrak{z}_{\text{GL}(V)}(\rho(g))$. Since $\rho$ is irreducible, this is 1-dimensional. Hence, since all fibres are of the same dimension, we get that $U_\sigma$ is 1-dimensional.

It is obvious that $GR \subset \tilde{G}$. For the other inclusion, let $g \in \tilde{G}$. Write $\sigma = \varphi(g)$. Set $R = \{ \lambda \cdot I_V \mid \lambda \in \mathbb{C} \}$. Then, since $\dim U_\sigma = 1$, we have $U_\sigma = gR$. So $\varphi^{-1}(\sigma) = gR$. However, $\varphi^{-1}(\sigma)$ also contains elements of $G$. So there is $h \in G$, $\lambda \in \mathbb{C}^*$ such that $\lambda g = h$. This shows the second point.

For the third statement, let $g \in \varphi^{-1}(\sigma)$. Then $g \neq 0$ and $g \in U_\sigma$, hence $g = \lambda u$ for some non-zero $\lambda \in \mathbb{C}$. This implies $u \in \tilde{G}$. \hfill \Box

Now consider the first problem from above. For this we suppose that $\theta$ is an inner automorphism, i.e., $\theta \in \text{Aut}(g)^0$. Let $\hat{\theta} \in U_\theta$, $\hat{\theta} \neq 0$. By Lemma 4.5 we have $\lambda \hat{\theta} \in G$, for some non-zero scalar $\lambda$, and $\hat{\theta} \rho(x) \hat{\theta}^{-1} = \rho(\theta(x))$ for all $x \in g$. So we can define an automorphism $\hat{\theta}$ of $G$ by $\hat{\theta}(g) = \hat{g} \hat{\theta}^{-1}$. The differential of $\hat{\theta}$ is equal to $\theta$ (after identifying $g$ and $\rho(g)$). So $G_0 = \{ g \in G \mid \hat{\theta} g \hat{\theta}^{-1} = \theta \hat{g} \}$.

Now we deal with the second problem. Let $\sigma_0$ be a generic automorphism of $g$, stabilising $\mathfrak{h}$, such that its restriction to $\mathfrak{h}$ is the identity. As seen before, $\sigma_0$ can be represented (with respect to a fixed basis of $g$) by a matrix whose entries are polynomials in $l$ independent parameters, $\lambda_1, \ldots, \lambda_l, \mu_1, \ldots, \mu_l$, with $\lambda_i \mu_i = 1$. Now we take $\lambda_i$ to be the generators of a rational function field $F$ in $l$ indeterminates, and $\mu_i = \lambda_i^{-1}$. Then we compute a basis vector of the space $U_{\sigma_0}$, by solving a
set of linear equations over $F$. Taking a basis vector of $U_{\sigma_0}$, we get (up to scalar multiples) a generic element of $Z_G(\mathfrak{h})$ (Lemma 4.5). We denote this element by $g_0$.

For the third problem, let $w \in W$ and let $\sigma_w \in \text{Aut}(\mathfrak{g})^0$ be such that it normalises $\mathfrak{h}$ and its restriction to $\mathfrak{h}$ coincides with $w$. Let $g_w$ be a non-zero element of $U_{\sigma_w}$. Then $\lambda g_w \in G$ for some non-zero $\lambda \in \mathbb{C}$ (Lemma 4.5). Furthermore, $g_w \rho(x)g_w^{-1} = \rho(\sigma_w(x))$ for all $x \in \mathfrak{g}$.

Now we describe how the above considerations yield an algorithm to compute generators of $W_\xi$. Consider $a \in C_\xi$, $K_a = \pi^{-1}(a) = \{w \in W^\theta \mid \pi(w) = a\}$, and $w \in K_a$. Let $g_w \in \tilde{G}$ be as above. Let $\lambda \in \mathbb{C}$ be such that $\tilde{g}_w = \lambda g_w$ lies in $G$. Then $\tilde{g}_w Z_G(\mathfrak{h})$ is the set of elements of $G$ that map to $w \in W$. We have $a \in W_\xi$ if and only if $\tilde{g}_w Z_G(\mathfrak{h}) \cap G_0$ is not empty for at least one $w \in K_a$. But $\tilde{g}_w Z_G(\mathfrak{h}) \cap G_0$ is not empty if and only if the polynomial equations that correspond to $\tilde{\theta} g_w g_0 = g_w g_0 \tilde{\theta}$ have a solution over $\mathbb{C}$. Again by Gröbner basis calculations we can check whether these equations have a solution. Performing this for all $w \in K_a$, we can check whether a given $a \in C_\xi$ lies in $W_\xi$. We leave the precise formulation of the algorithm, along the lines of Algorithm 3, to the reader.

Remark 4.6. When $\mathfrak{g}$ is of type $D_{2n}$ then we have to act in a slightly different way, because the corresponding simply connected group $\text{Spin}_{4n}$ has no faithful irreducible representations (cf. [23], §2.10). In this case one can take $\rho$ to be the direct sum of two irreducible representations (for example, with highest weights $\lambda_1$ and $\lambda_2$, where $\lambda_1, \ldots, \lambda_2$ are the fundamental weights). Let $V_1, V_2$ denote the corresponding $\mathfrak{g}$-modules, and $V = V_1 \oplus V_2$. Let $R_1$ (respectively $R_2$) be the set of scalar matrices that are the identity on $V_2$ (respectively, $V_1$). Then $\tilde{G} = GR_1R_2$. Also, the spaces $U_\sigma$ are 2-dimensional. So it is no longer true that a basis element of $U_\sigma$ necessarily lies in $\tilde{G}$. However, by taking different linear combinations of the two basis elements one easily finds an element of $U_\sigma$ that lies in $\tilde{G}$. With this change, one can proceed as for the other types.

4.2.3. Remarks on the algorithm.

Remark 4.7. In the last step of Algorithm 3 of course, one may restrict to $a$ that are complex reflections. Also, once we find a set of $a \in C_\xi$ that do lift to $G_0$, and generate a subgroup of $C_\xi$ of prime index, and at the same time we have found a $b \in C_\xi$ that does not lift to $G_0$, then we can stop.

Remark 4.8. We remark that for the constructions described in this section it is necessary to compute the root system of $\mathfrak{g}$ with respect to $\mathfrak{h}$. However, this Cartan subalgebra may not be split over $\mathbb{Q}$. In fact, that happens quite often. In these cases we have to work over algebraic extensions of $\mathbb{Q}$. Fortunately, MAGMA can handle these well. However, if the degree of the extension increases, then the computations tend to become much more difficult.

Remark 4.9. The automorphism $\theta$ is said to be $N$-regular if $\mathfrak{g}_1$ contains a regular nilpotent element. It is known that, up to conjugacy, there is exactly one $N$-regular inner automorphism of any given order ([16]). Also, Panyushev proved ([16]) that for $N$-regular $\theta$ we have that $W_\xi$ coincides with $C_\xi = \pi(W^\theta)$. Finally, we remark that for the exceptional types the $N$-regular automorphisms have been determined in [6].

Remark 4.10. We note that also Algorithm 3 works in the same way when $\mathfrak{g}$ is defined over a field of characteristic $p > 2$. 
Remark 4.11. Algorithm \( \mathbb{3} \) runs also if \( \text{Aut}(\mathfrak{g})^\circ \) is not simply connected. Moreover, it may very well give the correct output. Indeed, that happens, for example, if the centraliser of \( \theta \) in \( \text{Aut}(\mathfrak{g})^\circ \) is connected, or if \( W_\epsilon = \mathcal{C}_\epsilon \). In fact, it gave the correct output on all examples that we tried.

Remark 4.12. We can compute the degrees of the invariants that generate \( \mathbb{C}[\mathfrak{c}]^{W_\epsilon} \) directly. Indeed, this last ring is isomorphic to \( \mathbb{C}[\mathfrak{g}_1]^{G_0} \) (\cite{24}). The space of homogeneous elements of degree \( k \) of \( \mathbb{C}[\mathfrak{g}_1]^{G_0} \) is isomorphic, as \( G_0 \)-module, to \( \text{Sym}^k(\mathfrak{g}_1) \).

Now in MAGMA there are algorithms implemented for computing the decomposition of this last module into irreducibles, given such a decomposition of \( \mathfrak{g}_1 \). Write \( \mathfrak{g}_0 = \mathfrak{s} \oplus \mathfrak{t} \), where \( \mathfrak{s} \) is semisimple and \( \mathfrak{t} \) a central torus. Then there is an invariant of degree \( k \) if and only if there is a 1-dimensional submodule of \( \text{Sym}^k(\mathfrak{g}_1) \), on which \( \mathfrak{t} \) acts trivially.

Moreover, the product of the degrees of the generating invariants is equal to the order of \( W_\epsilon \) (\cite{13}, Theorem 4.19). So if this product equals the order of \( \mathcal{C}_\epsilon \), then we can conclude \( \mathcal{C}_\epsilon = W_\epsilon \).

This approach works well if the degrees of the generating invariants are relatively small. For higher degrees it becomes difficult to execute, due to the complexity of the algorithm for finding the decomposition of the module \( \text{Sym}^k(\mathfrak{g}_1) \).

5. Implementation and practical experiences

We have implemented the algorithms described in the previous section in the language of the computer algebra system MAGMA. This section has three subsections. The first describes some details of this implementation. The second reports on practical experiences with the implementation. In the third we briefly give an example in type \( E_6 \).

5.1. Implementation. Here we describe the two main problems that we encountered when implementing the algorithm, and how we deal with them.

Let \( \mathfrak{c} \) be a Cartan subspace of \( \mathfrak{g}_1 \), and let \( \mathfrak{h} \) be the Cartan subalgebra computed in Algorithm \( \mathbb{2} \). In Step 3 of that algorithm the adjoint action of \( \mathfrak{h} \) on \( \mathfrak{g} \) needs to be diagonalised. However, in general, the elements of \( \text{ad}_\mathfrak{g} \mathfrak{h} \) are not split over \( \mathbb{Q} \), and for that reason we need to work over an extension of \( \mathbb{Q} \); the larger the degree of that field, the more difficult all subsequent computations become. Furthermore, the Cartan subspace \( \mathfrak{c} \) is found by the randomised Algorithm \( \mathbb{1} \) and different runs produce different Cartan subspaces, which lead to different field extensions. For these reasons we start our program by computing a number (in our implementation it is 10) of Cartan subspaces, and pick the one which leads to the smallest degree field extension of \( \mathbb{Q} \).

The second problem occurs when we are in the situation considered in Section 4.2.2, i.e., \( \text{Aut}(\mathfrak{g})^\circ \) is not simply connected, then one of the main computational problems is computing the lift of an element of \( \text{Aut}(\mathfrak{g})^\circ \) to the group \( \tilde{G} \). Let \( n \) be the dimension of the representation \( \rho : \mathfrak{g} \to \mathfrak{gl}(V) \) and let \( \sigma \in \text{Aut}(\mathfrak{g})^\circ \). Then computing a basis of \( U_\sigma \) by linear equations involves equations in \( n^2 \) unknowns. For larger \( n \) (e.g., \( n = 56 \), as is the case for \( \mathfrak{g} \) of type \( E_7 \)) this becomes very cumbersome indeed. However, in a special case we can do much better. Let \( \tilde{\mathfrak{h}} \) be a Cartan subalgebra of \( \mathfrak{g} \) such that \( \rho(\tilde{\mathfrak{h}}) \) is diagonal, and suppose that \( \sigma(h) = h \) for all \( h \in \mathfrak{h} \). Then a \( \tilde{\sigma} \in U_\sigma \) lies in the subgroup \( \tilde{H} \) of \( \tilde{G} \) with Lie algebra \( \rho(\mathfrak{h}) \oplus \mathfrak{t} \), where \( \mathfrak{t} \) is an abelian Lie algebra consisting of scalar matrices. In particular, \( \tilde{\sigma} \) is a diagonal
matrix. So in this case we can find a basis of $U_\sigma$ by solving a set of linear equations in $n$ unknowns.

Now we construct $\rho$ such that $\rho(h)$ is diagonal, where $h$ is the Cartan subalgebra constructed in Algorithm 2. This implies that for computing the element $g_0$ (see Section 4.2.2) we can use the trick just described. However, we cannot do the same to compute $\tilde{\theta}$, as $\theta$ stabilises a different Cartan subalgebra $\tilde{h}$. We get around this by computing a base change matrix $M$ of $V$ such that, when setting $\tilde{\rho}(x) = M\rho(x)M^{-1}$, we have that $\tilde{\rho}(\tilde{h})$ is diagonal. Then we compute a lift $\tilde{\theta}'$ of $\theta$ using $\tilde{\rho}$, and solving equations in $n$ unknowns. Finally, we set $\tilde{\theta} = M^{-1}\tilde{\theta}'M$.

Let $w \in W$, and let $\sigma_w$ and $g_w$ be as in Section 4.2.2. To compute $g_w$ using equations in $n$ unknowns we need one more step. First we compute a Cartan subalgebra $\tilde{h}$ of $g_0,w = \{x \in g \mid \sigma_w(x) = x\}$. Since $\sigma_w$ is an inner automorphism, this is also a Cartan subalgebra of $g$. We compute the root system of $g$ with respect to $\tilde{h}$, and proceed as in the computation of $\tilde{\theta}$.

**Table 2.** Running times (in seconds) of the algorithm for computing generators of the little Weyl group. The first and second columns have, respectively, the Kac diagram and the order of the automorphism $\theta$. The third column displays the time used to compute lifts to the group $\tilde{G}$. And the fourth column lists the dimension of the representation. (Both of these are not applicable for $g$ of type $E_8$.) The fifth column displays the total time used in Gröbner basis computations. The sixth column has the size of the kernel of the homomorphism $\pi : W^\theta \to C_c$. The seventh column lists the degree of the field extension used in the algorithm. The eighth column has the isomorphism type of $W_c$. The last column has the total time.

| Kac diagram | $|\theta|$ | lift | dim $V$ | GB | $|K|$ | $dF$ | $W_c$ | time |
|-------------|---------|------|--------|----|------|------|-------|-------|
| ![Diagram](#) | 4       | 85   | 27     | 0.03 | 1    | 2    | $G(4,1,2)$ | 91   |
| ![Diagram](#) | 6       | 104  | 27     | 0.05 | 1    | 6    | $G_5$   | 150  |
| ![Diagram](#) | 4       | 379  | 56     | 0.03 | 8    | 2    | $G(4,1,2)$ | 436  |
| ![Diagram](#) | 6       | 495  | 56     | 0.03 | 12   | 2    | $G_5$   | 671  |
| ![Diagram](#) | 3       | $\times$ | $\times$ | 0.0 | 36   | 2    | $G(6,1,2)$ | 94   |
| ![Diagram](#) | 12      | $\times$ | $\times$ | 0.2 | 1    | 12   | $G_{10}$ | 2126 |
| ![Diagram](#) | 4       | 6114 | 144    | 0.02 | 1    | 2    | $G(4,2,4)$ | 6288 |
5.2. **Practical experiences.** Table 2 contains the running time of our implementation on various inputs, consisting of a simple Lie algebra $g$ together with an inner automorphism $\theta$. These timings were obtained on a 3.16 GHz processor.

As in Table 1, we give the Kac diagram of an automorphism by giving the extended Dynkin diagram, where we make some nodes black. A black node means that the corresponding label is 1, otherwise the label is 0.

We describe the isomorphism type of a complex reflection group using the classification of Shephard and Todd ([21]). This means that $W_c$ is either given by a number, denoting its position in the list, or by a symbol of the form $G(m, p, n)$, meaning that it is isomorphic to the intransitive complex reflection group of that type. We refer to the book [13] for details about the Shephard-Todd classification.

On Table 2 we make the following comments:

- When $\text{Aut}(g)^0$ is not simply connected, most time is spent on computing lifts of automorphisms of $g$ to $\tilde{G}$. The main parameter influencing this is $\dim V$. This can be seen when comparing the running time for the last automorphism with the first four.

- However, with the dimensions of the representations being equal, the degree of the field extension is an important parameter influencing the running time, as using a field of higher degree makes all subsequent computations more time consuming. This comes most dramatically to light when comparing the running times in the two examples for $g$ of type $E_8$.

- Despite their theoretical complexity, the Gröbner basis computations do not bear heavily on the running time. For this reason, also the size of $K$, the kernel of $\pi$, does not greatly influence the running time. (Note that, if the size of $K$ is larger, we potentially need to compute more Gröbner bases.)

**Remark 5.1.** With the help of these implementations we have computed the little Weyl groups for $\theta$-groups corresponding to automorphisms of the Lie algebras of exceptional type. We have dealt with all automorphisms of rank $\geq 2$, and with most automorphisms of rank 1. For the outer automorphisms of rank $\geq 2$ of the Lie algebra of type $E_6$, the little Weyl group was in all cases proved to be equal to $C_c$, using the method of Remark 4.12.

In all cases our computation confirmed the isomorphism type of $W_c$ known in the literature (see [24], [16], [15], [19]).

5.3. **An example.** Here we briefly describe an example of a little Weyl group, computed with our programs. Let $g$ be the Lie algebra of type $E_6$, and $\theta$ the automorphism of order 3, with Kac diagram

![Kac diagram](image)

The invariants of this particular $\theta$-representation have been studied in [2]. Here $g_0$ is isomorphic to $\mathfrak{sl}_3(\mathbb{C}) \oplus \mathfrak{sl}_3(\mathbb{C}) \oplus \mathfrak{sl}_3(\mathbb{C})$. As $g_0$-module, $g_1$ is isomorphic to $U \otimes V \otimes W$, where $U, V, W$ are copies of the standard 3-dimensional $\mathfrak{sl}_3$-module. We denote the basis vectors of these modules by $u_i, v_i, w_i$ ($1 \leq i \leq 3$) respectively. Setting $y_1 = e_{2,1}, y_2 = e_{3,2}$ we have $y_1u_1 = u_2, y_2u_2 = u_3$, and the same for the $v$’s and $w$’s. A Cartan subspace $c$ and little Weyl group $W_c$ are computed by our
programs in 44 seconds. After identifying $g_1$ and $U \otimes V \otimes W$ we have that $\mathfrak{c}$ is spanned by

$$A = u_2 \otimes v_1 \otimes w_1 + u_3 \otimes v_2 \otimes w_2 - u_1 \otimes v_3 \otimes w_3,$$

$$B = u_1 \otimes v_2 \otimes w_1 + u_2 \otimes v_3 \otimes w_2 + u_3 \otimes v_1 \otimes w_3,$$

$$C = u_1 \otimes v_1 \otimes w_2 - u_2 \otimes v_2 \otimes w_3 + u_3 \otimes v_3 \otimes w_1,$$

and $W_\mathfrak{c}$ is generated by

$$\begin{pmatrix} \omega & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \frac{1}{\sqrt{3}} \begin{pmatrix} -\omega + 1 & \omega + 2 & -\omega + 1 \\ \omega + 2 & -\omega + 1 & \omega - 1 \\ 2\omega + 1 & -2\omega - 1 & -\omega + 1 \end{pmatrix},$$

where $\omega$ denotes a primitive third root of unity.

The fundamental invariants are computed by MAGMA in 0.3 seconds. They are

$$f_1 = x_1^6 + 10x_1^3x_2^3 - 10x_1^3x_3^2 + x_2^6 + 10x_2^3x_3^2 + x_3^6,$$

$$f_2 = x_1^6x_2^2 + x_1^6x_3^2 + x_1^3x_2^6 - x_1^3x_3^6 - x_2^6x_3^2 - x_2^3x_3^6,$$

$$f_3 = x_1^{12} - 58x_1^9x_2^3 - 58x_1^9x_3^3 - 210x_1^6x_2^6 - 336x_1^6x_3^2x_2^3 - 210x_1^6x_3^2x_3^2 - 58x_1^3x_2^9 +$$

$$336x_1^3x_2^6x_3^3 - 336x_1^3x_2^3x_3^6 + 58x_1^3x_3^2x_2^3 + x_2^{12} - 58x_2^3x_3^9 - 210x_2^6x_3^6 - 58x_2^3x_3^9 + x_3^{12}.$$

So two elements $a_1 A + b_1 B + c_1 C$, $a_2 A + b_2 B + c_2 C$ of $\mathfrak{c}$ are in the same $G_0$ orbit if and only if $f_i(a_1, b_1, c_1) = f_i(a_2, b_2, c_2)$, for $1 \leq i \leq 3$.

Acknowledgements

The authors are grateful to Oksana Yakimova for enlightening discussions, and for her remarks on a previous version of this paper. The authors also thank the anonymous referees for their careful reading of, and helpful comments on a previous version of this paper.

References


DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI TRENTO, ITALY
E-mail address: degraaf@science.unitn.it

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI TRENTO, ITALY
E-mail address: francesco.oriente@tin.it