MATRIX GENERATORS FOR EXCEPTIONAL GROUPS OF LIE TYPE

R. B. HOWLETT, L. J. RYLANDS, AND D. E. TAYLOR

Abstract. This paper gives a uniform method of constructing generators for finite groups of Lie type with particular emphasis on the exceptional groups. The algorithm constructs matrices for the action of root elements on the lowest dimension representation of an associated Lie algebra. These generators have been implemented in the computer algebra system Magma and this completes the provision of pairs of matrix generators for all finite groups of Lie type.

1. Introduction

Until recently it was impractical to use general purpose computer algebra systems to investigate Chevalley groups except for those of small rank over small fields. But computer algebra systems (such as Magma (Bosma *et al.* 1997) and GAP (Schönert *et al.* 1994)) now have the power to deal with some aspects of all finite groups of Lie type. A natural way to represent these groups is via matrices over the defining field. Thus, for computational purposes, there is a need to provide matrix generators for these groups. This has been done for the classical groups (Taylor 1987, Rylands and Taylor 1998) and now it remains to extend this to all finite groups of Lie type.

It is the purpose of the present paper to give a uniform method of constructing generators for groups of Lie type with particular emphasis on the exceptional groups. The constructions described here could be carried out within any computer algebra system and, in particular, have been implemented in Magma. This completes the determination of matrix generators for all groups of Lie type, including the twisted groups of Steinberg, Suzuki and Ree (and the Tits group).

The Lie algebras and related Chevalley groups of types A_n, B_n, C_n and D_n can be identified with classical groups (Carter (1972), §11.3), and in Taylor (1987) and Rylands and Taylor (1998) this identification was used to translate the generators given by Steinberg (1962) to matrix forms.

The constructions in this paper rely on an investigation of the root systems of Lie algebras, providing a uniform approach and avoiding case by case discussions of non-associative algebras. In each case (except E_8) we obtain the lowest dimensional module for the Lie algebra via an embedding in a Lie algebra of higher rank.

2. Modules

In this section we prove two theorems about Lie algebras and root systems for use in the remainder of the paper. For notation and general facts about Lie algebras see Carter (1972) or Humphreys (1972).

Date: 24 June 1999.

Let $\mathcal{L}$ denote a complex semisimple Lie algebra with root system Φ, fundamental roots Δ, Cartan subalgebra H and Cartan decomposition $\mathcal{L} = H \oplus \bigoplus_{\alpha\in\Phi} \mathcal{L}_\alpha$. For each $\alpha \in \Phi$ choose $e_\alpha \in \mathcal{L}_\alpha$ so that $\{ e_\alpha \mid \alpha \in \Phi \}$ together with the elements $h_\alpha = [e_\alpha\, e_{-\alpha}]$ for $\alpha \in \Delta$ forms a Chevalley basis for $\mathcal{L}$ (Carter (1972), Theorem 4.2.1). In particular, $\{ h_\alpha \mid \alpha \in \Delta \}$ is a basis for H, Φ is a subset of the dual space of H and $[h\, e_\beta] = \beta(h)$ for all $h \in H$. We let Φ^+ denote the set of positive roots with respect to Δ and put $\Phi^- = \{ -\alpha \mid \alpha \in \Phi^+ \}$. The *height* of a root is the sum of its coefficients when expressed as a sum of fundamental roots.

Let κ denote the Killing form on the dual of H. Then $\langle \alpha, \beta \rangle = 2\kappa(\alpha,\beta)/\kappa(\beta,\beta)$ is linear in the first variable and if $\Delta = \{\alpha_1, \ldots, \alpha_\ell\}$, the $i\,j$-th entry of the Cartan matrix is $\langle \alpha_i, \alpha_j \rangle$.

When $\alpha + \beta \in \Phi$, write $c_{\alpha,\beta}$ for the structure constant given by $[e_\alpha\, e_\beta] = c_{\alpha,\beta}\, e_{\alpha+\beta}$. For convenience, define $c_{\alpha,\beta}$ to be 0 when $\alpha + \beta$ is neither 0 nor a root.

As usual, the adjoint action of $\mathcal{L}$ on itself is defined by $(\operatorname{ad} x)y = [x\, y]$.

Theorem 1. *Let $\mathcal{L}$ be a semisimple Lie algebra with root system Φ and fundamental roots Δ. Given a subset Δ_1 of Δ, let Φ_1 be the root system generated by Δ_1 and let $\mathcal{L}_1$ be the corresponding Lie subalgebra of $\mathcal{L}$. For $\gamma \in \Phi \setminus \Phi_1$, let*

$$X = \{ \alpha \in \Phi \mid \alpha - \gamma \text{ is in the span of } \Delta_1 \}.$$

Then the subspace V of $\mathcal{L}$ spanned by the e_α where $\alpha \in X$ is an $\mathcal{L}_1$-module of dimension $|X|$.

Proof. The restriction of the adjoint action of $\mathcal{L}$ to $\mathcal{L}_1$ allows us to view $\mathcal{L}$ as an $\mathcal{L}_1$-module. For $\alpha \in \Phi_1$ and $\beta \in X$ it is clear that $\alpha + \beta - \gamma$ is a linear combination of elements of Δ_1. Therefore, if $\alpha + \beta \in \Phi$, then $\alpha + \beta \in X$ and hence $\operatorname{ad}(e_\alpha)e_\beta \in V$. To complete the proof that V is an $\mathcal{L}_1$-submodule of $\mathcal{L}$ we note that we cannot have $\alpha + \beta = 0$, otherwise $-\gamma$ would belong to the span of Δ_1, contrary to the choice of γ. □

Beginning with a Dynkin diagram for $\mathcal{L}_1$ and a finite field $\mathbb{F}$, we give an algorithmic construction of an $\mathcal{L}_1$-module V and of the matrices representing the action of $\exp(t \operatorname{ad}(e_\alpha))$ on V (with respect to the basis indexed by X of Theorem 1), where $\alpha \in \Phi_1$ and $t \in \mathbb{F}$.

In each case we label the fundamental roots with lower case letters $a, b, c, \ldots$. This provides a natural total order $\prec$ on Δ and we suppose that $\Delta \setminus \Delta_1 = \{\omega\}$ where ω is the last element of Δ. Let V be the $\mathcal{L}_1$-module corresponding to $\gamma = \omega$. We see from the proof of Theorem 1 that X consists of the roots in which the coefficient of ω is 1 when expressed as a linear combination of fundamental roots; in particular, $X \subseteq \Phi^+$. The Dynkin diagram is conveniently described by its Cartan matrix and, given this information, the algorithm of Jacobson (1962), p. 122 (and sketched in §11.1 of Humphreys (1972)) constructs the positive roots of Φ such that roots of equal height are ordered lexicographically. We shall write $\alpha \prec \beta$ to indicate that α comes before β in this order.

To obtain upper triangular matrices for the linear transformations $\operatorname{ad}(e_\alpha)$ when α is positive, we order X, and hence the basis $\{ e_\alpha \mid \alpha \in X \}$ of V, according to the reverse of Jacobson's ordering. Given $\alpha \in \Phi_1$, the matrix of the restriction of $\operatorname{ad}(e_\alpha)$ to V has

$c_{\alpha,\beta}$ in the row indexed by $\alpha+\beta$ and the column indexed by β, whenever $\alpha+\beta$ is a root.

The assumption that we are working with a Chevalley basis for $\mathcal{L}$ means that the $c_{\alpha,\beta}$ are determined up to a sign. In fact $c_{\alpha,\beta} = \pm(r+1)$ where r is the greatest integer such that $\beta - r\alpha$ is a root. In order to determine the sign we follow the method of Carter (1972), §4.2. For each positive root γ which is not a fundamental root we choose the least fundamental root α (in the total ordering $\prec$) such that $\beta = \gamma - \alpha$ is a root. In the terminology of Carter, (α, β) is an extraspecial pair. The signs of the structure constants $c_{\alpha,\beta}$ for extraspecial pairs (α,β) may be chosen arbitrarily and then all other structure constants are uniquely determined.

Given the ordered set of positive roots it is a straightforward matter to determine the extraspecial pairs. Then for roots α and β ($\alpha+\beta \neq 0$) we may use the following algorithm (derived from Carter (1972), Theorem 4.1.2) to determine the $c_{\alpha,\beta}$ recursively, given that we take $c_{\alpha,\beta}$ to be positive whenever (α,β) is an extraspecial pair. The Killing form on the dual of the Cartan subalgebra of $\mathcal{L}$ is completely determined by the Cartan matrix; namely

$$\begin{aligned} \kappa(\alpha_i,\alpha_j) &= \frac{4t_{ij}}{t_{ii}t_{jj}}, \quad \text{where} \\ t_{ij} &= \sum_{\alpha\in\Phi} \langle\, \alpha, \alpha_i \,\rangle \langle\, \alpha, \alpha_j \,\rangle. \end{aligned}$$

Step 1. *$\alpha+\beta$ is not a root.*
In this case $c_{\alpha,\beta} = 0$ and from now on we may suppose that $\alpha+\beta$ is a root.

Step 2. height$(\alpha) >$ height(β).
Then $c_{\alpha,\beta} = -c_{\beta,\alpha}$ and now we may suppose that height$(\alpha) \leq$ height(β).

Step 3. *α is negative.*

Step 3a. *β is negative.*
Then $c_{\alpha,\beta} = c_{-\beta,-\alpha}$.

Step 3b. *β is positive.*
If $\xi = \alpha+\beta$ is negative, then $c_{\alpha,\beta} = \dfrac{\kappa(\xi,\xi)c_{\beta,-\xi}}{\kappa(\alpha,\alpha)}$, whereas if ξ is positive, then $c_{\alpha,\beta} = \dfrac{\kappa(\xi,\xi)c_{-\alpha,\xi}}{\kappa(\beta,\beta)}$. Return to Step 2.

Step 4. *α is positive.*
Let (ε,η) be the extraspecial pair for $\alpha+\beta$ so that $\alpha+\beta = \varepsilon+\eta$. If $\varepsilon = \alpha$, then $c_{\alpha,\beta} = r+1$, where r is the greatest integer such that $\beta - r\alpha$ is a root. If $\varepsilon = \beta$, then $c_{\alpha,\beta} = -1$. Otherwise,

$$c_{\alpha,\beta} = \frac{\kappa(\alpha+\beta,\alpha+\beta)}{r+1}\left(\frac{c_{-\varepsilon,\beta}c_{-\eta,\alpha}}{\kappa(\beta-\varepsilon,\beta-\varepsilon)} - \frac{c_{-\varepsilon,\alpha}c_{-\eta,\beta}}{\kappa(\alpha-\varepsilon,\alpha-\varepsilon)}\right),$$

where r is the greatest integer such that $\eta - r\varepsilon$ is a root.

The same choice of structure constants is made in Gilkey and Seitz (1988).

For the case in which all elements of Φ have the same length a considerable improvement to the algorithm can be obtained via the following theorem. Furthermore, in this case, $\mathrm{ad}(e_{-\alpha})e_{\alpha+\beta} = c_{-\alpha,\alpha+\beta}e_\beta = c_{\alpha,\beta}e_\beta$ (see STEP 3B above) and so the matrix of $\mathrm{ad}(e_{-\alpha})|_V$ is the transpose of the matrix of $\mathrm{ad}(e_\alpha)|_V$.

Theorem 2. *Given that Φ is a root system with fundamental roots Δ where Φ^+ is totally ordered by $\prec$ (as above), suppose that all roots have the same length and that the structure constants are determined by the algorithm just described. Then for $\alpha \in \Delta$ and $\beta \in \Phi$ such that $\alpha + \beta \in \Phi$ where the expression for β as a sum of fundamental roots involves some $\omega \succ \alpha$, we have*

$$c_{\alpha,\beta} = \begin{cases} 1 & \text{if } \beta \in \Phi^+ \\ -1 & \text{if } \beta \in \Phi^-. \end{cases}$$

Proof. Suppose at first that $\beta \in \Phi^+$ so that $\alpha + \beta \in \Phi^+$. All roots have the same length and so the α-chain through β is $\beta, \alpha+\beta$. By Carter (1972), §4.2 this forces $c_{\alpha,\beta}$ to be ± 1.

Because α is positive, we determine $c_{\alpha,\beta}$ via STEP 4 of the algorithm. If (ε, η) is the extraspecial pair for $\alpha + \beta$, then $\alpha + \beta = \varepsilon + \eta$ and $\eta - \varepsilon$ is not a root. Because $\varepsilon \preceq \alpha$, it is not possible to have $\varepsilon = \beta$ whereas if $\varepsilon = \alpha$, then $c_{\alpha,\beta} = 1$ and in this case we have finished. Thus we may suppose that $\varepsilon \prec \alpha$. Then $c_{\alpha,\beta} = c_{-\varepsilon,\beta}c_{-\eta,\alpha}$ since $\alpha - \varepsilon$ is not a root and therefore $c_{-\varepsilon,\alpha} = 0$. Now $c_{\alpha,\beta} \neq 0$ and therefore $c_{-\varepsilon,\beta} \neq 0$, whence $\delta = \beta - \varepsilon = \eta - \alpha$ is a (positive) root which involves $\omega \succ \varepsilon$. Thus STEP 3B of the algorithm shows that $c_{-\varepsilon,\beta} = c_{\varepsilon,\delta} = 1$ by induction. Again using STEP 3B we have $c_{-\eta,\alpha} = c_{\alpha,\delta} = 1$ by induction. It follows that $c_{\alpha,\beta} = 1$.

It remains to consider the case in which $\beta \in \Phi^-$ and $\alpha + \beta \in \Phi$. Then $-\alpha - \beta \in \Phi^+$ and, as in STEP 3 of the algorithm, we have $c_{\alpha,\beta} = -c_{\alpha,-\alpha-\beta}$ and the result follows from the case already dealt with. □

Corollary 1. *Suppose that Φ, Φ_1, Δ, Δ_1 and X are as above with $\Delta \setminus \Delta_1 = \{\omega\}$. If all roots have the same length, then $c_{\alpha,\beta} = 1$ for all $\alpha \in \Delta_1$, $\beta \in X$ such that $\alpha + \beta \in X$.*

3. LIE ALGEBRAS AND GROUPS OF TYPES E_6, E_7, E_8, F_4 AND G_2

The Weyl character formula shows that the smallest degree of a non-trivial (irreducible) representation of the complex Lie algebra of type G_2, F_4, E_6, E_7 and E_8 is respectively 7, 26, 27, 56 and 248 (Tits (1967), pp. 41–50). Theorem 1 enables us to write down representations of the Lie algebras of types E_6 and E_7 of degrees 27 and 56 respectively whereas the dimension of the adjoint representation of E_8 is 248.

In order to obtain representations of minimal degree for the Lie algebras of types G_2 and F_4 we realize them as the fixed points of graph automorphisms of D_4 and E_6 respectively (see § 3.4). The modules for the Lie algebras of types D_4 and E_6 obtained from Theorem 1 via the inclusions $D_4 \subseteq D_5$ and $E_6 \subseteq E_7$ restrict to modules for G_2 and F_4 of dimensions 8 and 27 respectively. In both cases there is an invariant submodule of codimension 1 affording representations of dimensions 7 and 26 respectively. It turns out that all the representations considered so far are subrepresentations of the adjoint representation of E_8.

The use of a Chevalley basis in our construction of the modules means that each module comes equipped with a $\mathbb{Z}$-form, and therefore the usual Chevalley construction (Carter 1972, Chapter 4) yields matrix groups over all fields. In general the group so constructed is a central extension of the simple group. Steinberg (1962) has given pairs of generators for the simple groups, and hence we obtain pairs of generators for the central extensions.

In most cases the representations obtained are irreducible. However, when the Lie algebra has type G_2 or F_4 and the field has characteristic 2 or 3 respectively, there is a submodule of dimension 1 whose quotient is an irreducible module of dimension 6 or 25, respectively.

For the remainder of the paper we shall consider a simple Lie algebra $\mathcal{L}$ and a representation $\phi : \mathcal{L} \to \mathfrak{gl}(\ell, \mathbb{C})$ of $\mathcal{L}$ by $\ell \times \ell$ matrices. For each $e_\alpha \in \mathcal{L}_\alpha$ the matrix $\phi(e_\alpha)$ will have integer entries and be the restriction of $\mathrm{ad}(e_\alpha)$ to a suitable module, hence nilpotent. Moreover, for any field $\mathbb{F}$ and $\xi \in \mathbb{F}$ the sum

$$x_\alpha(\xi) = \exp(\xi\phi(e_\alpha)) = 1 + \xi\phi(e_\alpha) + \frac{\xi^2}{2!}\phi(e_\alpha)^2 + \cdots$$

will be finite (it will never have more than 3 terms) and defined over $\mathbb{F}$. The Chevalley group associated with $\mathcal{L}$, ϕ and the field $\mathbb{F}_q$ of order q is

$$G_\phi(q) = \langle\, x_\alpha(\xi) \mid \xi \in \mathbb{F}_q,\ \alpha \in \Phi \,\rangle.$$

In what follows we let I denote the identity matrix and $E_{i,j}$ denote the elementary matrix with 1 in the ij-th position and 0's elsewhere; ξ will be always be an element of the relevant field.

Following Carter (1972), §6.4, for each positive root α we take

$$\begin{aligned} n_\alpha(\xi) &= x_\alpha(\xi)x_{-\alpha}(-\xi^{-1})x_\alpha(\xi) \quad \text{and} \\ h_{\alpha,\xi} &= n_\alpha(\xi)n_\alpha(-1). \end{aligned}$$

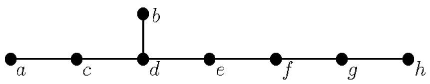
Then $h_{\alpha,\xi}$ satisfies

$$h_{\alpha,\xi}x_\beta(\nu)h_{\alpha,\xi}^{-1} = x_\beta(\xi^{\langle \beta,\alpha \rangle}\nu)$$

for all $\nu \in \mathbb{F}_q^\times$ and $\beta \in \Phi$ and so may be identified with the element h in Theorem 3.4 of Steinberg (1962). In each case the matrix $h_{\alpha,\xi}$ will be diagonal.

Finally, n will always be a product (in some order) of the $n_\alpha(1)$ where $\alpha \in \Delta$; that is, it will correspond to a Coxeter element of the Weyl group.

3.1. E_8. Label the fundamental roots as indicated in the diagram



The degree of the smallest representation is 248. This is the dimension of the Lie algebra of type E_8, and so the Chevalley construction for the field $\mathbb{F}_q$ produces the (simple) adjoint group $E_8(q)$.

In this case, for $e \in \mathcal{L}$, $\phi(e)$ is the matrix of $\mathrm{ad}(e)$ with respect to the Chevalley basis. The Lie algebra is generated by the matrices $\phi(e_\alpha)$, where $\pm\alpha \in \{a, b, \ldots, h\}$. Each matrix has at most 61 of its $61,504$ entries non-zero but this is still too large to be given here. However, Theorem 2 and the fact that $\phi(e_{-\alpha})$ is almost the transpose of $\phi(e_\alpha)$ allows these matrices to be computed rapidly. From these we get generators for the group $E_8(q)$:

$$x_\alpha(\xi) \;=\; I + \xi\phi(e_\alpha) + \frac{1}{2}\xi^2\phi(e_\alpha)^2 \quad \text{for } \pm\,\alpha \in \{a, b, \dots, h\},$$

where $\xi \in \mathbb{F}_q$. Using these elements we have

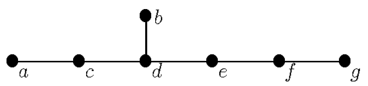
$$\begin{aligned} n_\alpha(\xi) &= x_\alpha(\xi)x_{-\alpha}(-\xi^{-1})x_\alpha(\xi) \quad \text{for } \alpha \in \{a, b, \dots, h\},\\ n &= n_h(1)n_g(1)n_f(1)n_e(1)n_d(1)n_c(1)n_b(1)n_a(1) \quad \text{and}\\ h_{h,\xi} &= n_h(\xi)n_h(-1). \end{aligned}$$

It follows from Steinberg (1962), Theorem 3.11 that $E_8(q)$ is generated by

$$\begin{cases} h_{h,\mu} \text{ and } x_h(1)n & \text{for } q > 3\\ x_h(1) \text{ and } n & \text{for } q \le 3, \end{cases}$$

where μ is a primitive element of $\mathbb{F}_q$.

3.2. E_7. The Dynkin diagram for E_7 is



labelled to be consistent with the diagram of type E_8. We use Theorem 1 with $\Delta_1 = \Delta(E_7)$, $\Delta = \Delta(E_8)$ and $\gamma = h$ to construct a representation space V of dimension 56 of the Lie algebra of type E_7. The basis for V is $\{\, e_\alpha \mid \alpha \in X \,\}$ with X defined and ordered as in §2 (so that $X = \{2a{+}3b{+}4c{+}6d{+}5e{+}4f{+}3g{+}h, \dots, f{+}g{+}h, g{+}h, h\}$). The ordering ensures that the matrix $\phi(e_\alpha)$ of $\mathrm{ad}(e_\alpha)|_V$ is upper triangular for each root $\alpha \in \Phi^+(E_7)$. By Corollary 1, for all $\alpha \in \Delta_1$, every nonzero entry of $\phi(e_\alpha)$ is 1.

Since $\phi(e_{-\alpha})$ is the transpose of $\phi(e_\alpha)$ for any root α, the following elements and their transposes generate the Lie algebra:

$$\begin{aligned}
\phi(e_a) &= E_{7,8} + E_{9,10} + E_{11,12} + E_{13,15} + E_{16,18} + E_{19,22} + E_{35,38}\\
&\qquad + E_{39,41} + E_{42,44} + E_{45,46} + E_{47,48} + E_{49,50},\\
\phi(e_b) &= E_{5,6} + E_{7,9} + E_{8,10} + E_{20,23} + E_{24,26} + E_{27,29} + E_{28,30}\\
&\qquad + E_{31,33} + E_{34,37} + E_{47,49} + E_{48,50} + E_{51,52},\\
\phi(e_c) &= E_{5,7} + E_{6,9} + E_{12,14} + E_{15,17} + E_{18,21} + E_{22,25} + E_{32,35}\\
&\qquad + E_{36,39} + E_{40,42} + E_{43,45} + E_{48,51} + E_{50,52},\\
\phi(e_d) &= E_{4,5} + E_{9,11} + E_{10,12} + E_{17,20} + E_{21,24} + E_{25,28} + E_{29,32}\\
&\qquad + E_{33,36} + E_{37,40} + E_{45,47} + E_{46,48} + E_{52,53},\\
\phi(e_e) &= E_{3,4} + E_{11,13} + E_{12,15} + E_{14,17} + E_{24,27} + E_{26,29} + E_{28,31}\\
&\qquad + E_{30,33} + E_{40,43} + E_{42,45} + E_{44,46} + E_{53,54},\\
\phi(e_f) &= E_{2,3} + E_{13,16} + E_{15,18} + E_{17,21} + E_{20,24} + E_{23,26} + E_{31,34}\\
&\qquad + E_{33,37} + E_{36,40} + E_{39,42} + E_{41,44} + E_{54,55} \quad \text{and}\\
\phi(e_g) &= E_{1,2} + E_{16,19} + E_{18,22} + E_{21,25} + E_{24,28} + E_{26,30} + E_{27,31}\\
&\qquad + E_{29,33} + E_{32,36} + E_{35,39} + E_{38,41} + E_{55,56}.
\end{aligned}$$

The matrix group $G_\phi(q)$ is generated by the elements $x_\alpha(\xi) = I + \xi\phi(e_\alpha)$ (as $\phi(e_\alpha)^2 = 0$) for $\pm\alpha \in \{a, b, \ldots, g\}$ and $\xi \in \mathbb{F}_q$.

In general we have $n_\alpha(\xi) = x_\alpha(\xi)x_{-\alpha}(-\xi^{-1})x_\alpha(\xi)$ and $h_{\alpha,\xi} = n_\alpha(\xi)n_\alpha(-1)$. The centre of $G_\phi(q)$ is generated by $h_{b,-1}h_{e,-1}h_{g,-1} = -I$ and thus $G_\phi(q)$ is $2E_7(q)$ (the central extension of the simple group $E_7(q)$ by a group of order 2) when q is odd or $E_7(q)$ when q is a power of 2.

The diagonal matrix $h_{g,\xi}$ has its ith diagonal entry equal to

$$\begin{cases} \xi & \text{if } i = 1, 16, 18, 21, 24, 26, 27, 29, 32, 35, 38 \text{ or } 55, \\ \xi^{-1} & \text{if } i = 2, 19, 22, 25, 28, 30, 31, 33, 36, 39, 41 \text{ or } 56, \\ 1 & \text{otherwise.} \end{cases}$$

A Coxeter element is the matrix $n = n_g(1)n_f(1)n_e(1)n_d(1)n_c(1)n_b(1)n_a(1)$. Its nonzero entries are equal to 1 for the indices

$$\begin{gathered} (1,10),(9,12),(10,14),(11,15),(12,17),(13,18),(14,23),(15,21),(16,22), \\ (17,26),(18,25),(19,5),(20,29),(21,30),(22,7),(23,38),(24,33),(26,41), \\ (27,37),(29,44),(32,46),(35,50),(38,52),(39,32),(41,35),(42,36),(44,39), \\ (45,40),(46,42),(47,43),(48,45),(51,49),(52,53),(53,54),(54,55),(55,56) \end{gathered}$$

and -1 for

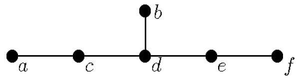
$$\begin{gathered} (2,1),(3,2),(4,3),(5,4),(6,8),(7,6),(8,9),(25,11),(28,13),(30,20),(31,16), \\ (33,24),(34,19),(36,27),(37,28),(40,31),(43,34),(49,48),(50,51),(56,47). \end{gathered}$$

It follows from Steinberg (1962), Theorem 3.11 that $G_\phi(q)$ is generated by

$$\begin{cases} h_{g,\mu} \text{ and } x_g(1)n & \text{for } q > 3 \\ x_g(1) \text{ and } n & \text{for } q \leq 3, \end{cases}$$

where μ is a primitive element of $\mathbb{F}_q$.

3.3. E_6. The Dynkin diagram for E_6 is



labelled to be consistent with the diagram of type E_7. We use Theorem 1 with $\Delta_1 = \Delta(E_6)$, $\Delta = \Delta(E_7)$ and $\gamma = g$ to construct a representation space V of dimension 27 of the Lie algebra of type E_6. The basis of V is indexed by X and ordered as in §2, that is, $X = \{2a+2b+3c+4d+3e+2f+g, \ldots, e+f+g, f+g, g\}$. This choice of ordering means that for $\alpha \in \Delta_1$ the matrix $\phi(e_\alpha)$ of $\mathrm{ad}(e_\alpha)|_V$ is upper triangular. (Note that there are two 27-dimensional representations of the Lie algebra of type E_6; one is the contragredient of the other.) By Corollary 1 the nonzero entries of the matrices are 1 and a straightforward calculation produces the following 27×27 matrices:

$$\begin{aligned}
\phi(e_a) &= E_{1,2} + E_{11,13} + E_{14,16} + E_{17,18} + E_{19,20} + E_{21,22},\\
\phi(e_b) &= E_{4,5} + E_{6,7} + E_{8,10} + E_{19,21} + E_{20,22} + E_{23,24},\\
\phi(e_c) &= E_{2,3} + E_{9,11} + E_{12,14} + E_{15,17} + E_{20,23} + E_{22,24},\\
\phi(e_d) &= E_{3,4} + E_{7,9} + E_{10,12} + E_{17,19} + E_{18,20} + E_{24,25},\\
\phi(e_e) &= E_{4,6} + E_{5,7} + E_{12,15} + E_{14,17} + E_{16,18} + E_{25,26} \quad \text{and}\\
\phi(e_f) &= E_{6,8} + E_{7,10} + E_{9,12} + E_{11,14} + E_{13,16} + E_{26,27}.
\end{aligned}$$

The matrix $\phi(e_{-\alpha})$ is the transpose of $\phi(e_\alpha)$ and the Lie algebra of type E_6 is generated by the $\phi(e_\alpha)$ for $\pm\alpha \in \{a, \dots, f\}$.

The matrix group $G_\phi(q)$ is generated by the elements $x_\alpha(\xi) = \exp(\xi\phi(e_\alpha)) = I + \xi\phi(e_\alpha)$ for $\pm\alpha \in \{a, b, \dots, f\}$ and $\xi \in \mathbb{F}_q$.

If $q \equiv 1 \bmod 3$, the field $\mathbb{F}_q$ contains an element ω of order 3 and the centre of $G_\phi(q)$ is generated by the scalar matrix $h_{a,\omega^2} h_{c,\omega} h_{e,\omega^2} h_{f,\omega}$ of order 3. Thus when $q \equiv 1 \bmod 3$, the group $G_\phi(q)$ is $3E_6(q)$ (the central extension of the simple group $E_6(q)$ by a group of order 3); otherwise it is the simple group $E_6(q)$.

The diagonal matrix $h_{a,\xi}$ has its ith diagonal entry equal to

$$\begin{cases} \xi & \text{if } i = 1, 11, 14, 17, 19 \text{ or } 21\\ \xi^{-1} & \text{if } i = 2, 13, 16, 18, 20 \text{ or } 22\\ 1 & \text{otherwise.}\end{cases}$$

A Coxeter element is given by $n = n_a(1)n_c(1)n_d(1)n_e(1)n_f(1)n_b(1)$; it has nonzero entries equal to 1 for indices

$$\begin{gathered}(1,10), (7,12), (9,14), (10,15), (11,16), (12,17), (14,18), (15,21), (17,22),\\ (18,9), (19,24), (20,11), (21,27), (22,19), (23,13), (24,20), (25,23)\end{gathered}$$

and -1 for

$$(2,1), (3,2), (4,3), (5,8), (6,5), (8,7), (13,4), (16,6), (26,25), (27,26).$$

It follows from Steinberg (1962), Theorem 3.11 that $G_\phi(q)$ is generated by

$$\begin{cases} h_{a,\mu} \text{ and } x_a(1)n & \text{for } q > 3\\ x_a(1) \text{ and } n & \text{for } q = 2 \text{ or } 3,\end{cases}$$

where μ is a primitive element of $\mathbb{F}_q$.

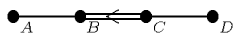
3.4. **The fixed points of a graph automorphism.** Suppose that all the roots of the simple Lie algebra $\mathcal{L}$ have the same length and that σ is an automorphism of the Dynkin diagram of $\mathcal{L}$. Then σ determines a linear transformation of the Cartan subalgebra (and its dual) which permutes the fundamental roots Δ and fixes the full root system Φ. In fact this permutation of Φ, which we also denote by σ, extends to an automorphism of $\mathcal{L}$ such that, in the notation of §2, $h_\alpha{}^\sigma = h_{\alpha^\sigma}$ and $e_\alpha{}^\sigma = \pm e_{\alpha^\sigma}$ (Carter 1972, Proposition 12.2.3).

Let $\mathcal{L}^\sigma$ be the subalgebra of fixed points of σ. In the cases of interest to us, namely D_4 and E_6, $\mathcal{L}^\sigma$ is a simple Lie algebra of type G_2 or F_4, respectively.

For each $e \in \mathcal{L}$ let $\tilde{e}$ be the sum of the elements in the $\langle \sigma \rangle$-orbit of e. Then for $h \in H$ such that $h^\sigma = h$ and for $\alpha \in \Phi$ we have $[h\, \tilde{e}_\alpha] = \alpha(h)\tilde{e}_\alpha$. Thus the roots of $\mathcal{L}^\sigma$ are the restrictions to $H^\sigma = H \cap \mathcal{L}^\sigma$ of the roots of $\mathcal{L}$. Also, for $\alpha \in \Delta$ we have $\tilde{h}_\alpha = [\tilde{e}_\alpha\, \tilde{e}_{-\alpha}]$.

For types D_4 and E_6 and $\alpha \in \Delta$ such that $\alpha \neq \alpha^\sigma$ we have $\langle \alpha, \alpha^\sigma \rangle = 0$. Thus $\alpha(\tilde{h}_\alpha) = 2$ and it follows that a Chevalley basis for $\mathcal{L}^\sigma$ can be obtained by taking elements $\tilde{e}$, where e runs through a set of representatives for the orbits of the group $\langle -1, \sigma \rangle$ on a Chevalley basis of $\mathcal{L}$. We label the fundamental roots of $\mathcal{L}^\sigma$ as $A, B, \dots$. If A is the restriction of the root a, we choose $e_A = \tilde{e}_a$, and so on. The remaining elements of the Chevalley basis are determined by $e_A, e_B, \dots$ up to a sign and we choose the signs to agree with the algorithm of §2. The Cartan matrix of $\mathcal{L}^\sigma$ can be obtained from the Cartan matrix of $\mathcal{L}$ by taking, for each pair of representatives of the $\langle \sigma \rangle$-orbits on Δ, the sum of the entries in the row of α corresponding to the columns indexed by the elements in the $\langle \sigma \rangle$-orbit of β.

3.5. F_4. We begin with the complex Lie algebra $\mathcal{L}$ of type E_6 given in §3.3 and with its Dynkin diagram as given there. In this case the graph automorphism has order 2. The restrictions of a, c, d and b to H^σ are the fundamental roots A, B, C and D of $\mathcal{L}^\sigma$, and we have $e_A = \tilde{e}_a = e_a + e_f$, $e_B = \tilde{e}_c = e_c + e_e$, $e_C = \tilde{e}_d = e_d$ and $e_D = \tilde{e}_b = e_b$. Since $\begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$ is the Cartan matrix of $\mathcal{L}$, the Cartan matrix of $\mathcal{L}^\sigma$ with respect to the ordering A, B, C, D is $\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -2 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$ and therefore its Dynkin diagram is



of type F_4.

Take ϕ to be the representation of dimension 27 for E_6 with representation space V defined in §3.3 and let $v_1, v_2, \dots, v_{27}$ be its basis defined there. We note that $\phi(e_{-X})$ is the transpose of $\phi(e_X)$.

The restriction of ϕ to $\mathcal{L}^\sigma$ is reducible. There is an $\mathcal{L}^\sigma$-invariant subspace U with basis u_i, $i = 1, \dots, 26$, where

$$u_i = \begin{cases} v_i & \text{for } 1 \leq i < 13 \\ v_{13} + v_{14} & \text{for } i = 13 \\ v_{14} + v_{15} & \text{for } i = 14 \\ v_{i+1} & \text{for } 14 < i \leq 26 \end{cases}$$

In characteristic 0 the representation splits into the sum of the (irreducible) 26-dimensional representation on U and the zero representation on $\langle u_0 \rangle$, where $u_0 = v_{13} - v_{14} + v_{15}$. In any characteristic $\langle u_0 \rangle$ is the unique 1-dimensional $\mathcal{L}^\sigma$-submodule of U.

If we let ψ denote the representation of $\mathcal{L}^\sigma$ on U we obtain the following matrix generators for the Lie algebra of type F_4.

$$\begin{aligned}
\psi(e_A) &= E_{1,2} + E_{6,8} + E_{7,10} + E_{9,12} + 2E_{11,13} + E_{11,14} + E_{13,15} \\
&\qquad + E_{16,17} + E_{18,19} + E_{20,21} + E_{25,26}, \\
\psi(e_B) &= E_{2,3} + E_{4,6} + E_{5,7} + E_{9,11} + E_{12,13} + 2E_{12,14} + E_{14,16} \\
&\qquad + E_{15,17} + E_{19,22} + E_{21,23} + E_{24,25}, \\
\psi(e_C) &= E_{3,4} + E_{7,9} + E_{10,12} + E_{16,18} + E_{17,19} + E_{23,24}, \\
\psi(e_D) &= E_{4,5} + E_{6,7} + E_{8,10} + E_{18,20} + E_{19,21} + E_{22,23}, \\
\psi(e_{-A}) &= E_{2,1} + E_{8,6} + E_{10,7} + E_{12,9} + E_{13,11} + 2E_{15,13} + E_{15,14} \\
&\qquad + E_{17,16} + E_{19,18} + E_{21,20} + E_{26,25}, \\
\psi(e_{-B}) &= E_{3,2} + E_{6,4} + E_{7,5} + E_{11,9} + E_{14,12} + E_{16,13} + 2E_{16,14} \\
&\qquad + E_{17,15} + E_{22,19} + E_{23,21} + E_{25,24}, \\
\psi(e_{-C}) &= \psi(e_C)^t \quad \text{and} \\
\psi(e_{-D}) &= \psi(e_D)^t.
\end{aligned}$$

From these we obtain

$$\begin{aligned}
\psi(e_{2B+C}) &= -E_{2,6} - E_{5,11} + E_{10,16} + E_{12,18} - E_{15,22} - E_{21,25} \quad \text{and} \\
\psi(e_{-(2B+C)}) &= \psi(e_{2B+C})^t.
\end{aligned}$$

The group $G_\psi(q)$ is generated by the elements $x_\alpha(\xi) = I + \xi\psi(e_\alpha) + \frac{1}{2}\xi^2\psi(e_\alpha)^2$ for $\pm\alpha \in \{A, B, C, D\}$ and $\xi \in \mathbb{F}_q$. It is isomorphic to the simple group $F_4(q)$.

In particular we have:

$$\begin{aligned}
x_A(1) &= I + \psi(e_A) + \frac{1}{2}\psi(e_A)^2 = I + E_{1,2} + E_{6,8} + E_{7,10} + E_{9,12} + 2E_{11,13} \\
&\qquad + E_{11,14} + E_{13,15} + E_{16,17} + E_{18,19} + E_{20,21} + E_{25,26} + E_{11,15}, \\
x_C(1) &= I + \psi(e_C) = I + E_{3,4} + E_{7,9} + E_{10,12} + E_{16,18} + E_{17,19} + E_{23,24} \quad \text{and} \\
x_{-B}(1) &= I + \psi(e_{-B}) + \frac{1}{2}\psi(e_{-B})^2 = I + E_{3,2} + E_{6,4} + E_{7,5} + E_{11,9} + E_{14,12} \\
&\qquad + E_{16,12} + E_{16,13} + 2E_{16,14} + E_{17,15} + E_{22,19} + E_{23,21} + E_{25,24}.
\end{aligned}$$

The ith diagonal entry of $h_{A,\xi} = n_A(\xi)n_A(-1)$ is equal to

$$\begin{cases}
\xi & \text{if } i = 1, 6, 7, 9, 16, 18, 20 \text{ or } 25 \\
\xi^{-1} & \text{if } i = 2, 8, 10, 12, 17, 19, 21 \text{ or } 26 \\
\xi^2 & \text{if } i = 11 \\
\xi^{-2} & \text{if } i = 15 \\
1 & \text{otherwise}
\end{cases}$$

and the ith diagonal entry of $h_{2B+C,\xi}$ is equal to

$$\begin{cases}
\xi & \text{if } i = 2, 5, 10, 12, 15 \text{ or } 21 \\
\xi^{-1} & \text{if } i = 6, 11, 16, 18, 22 \text{ or } 25 \\
1 & \text{otherwise.}
\end{cases}$$

The Coxeter element $n = n_A(1)n_B(1)n_C(1)n_D(1)$ has nonzero entries equal to 1 for indices

$$(1,5),(4,7),(5,9),(6,10),(7,12),(9,20),(11,21),(13,14),(18,23),(19,16),$$
$$(20,24),(21,18),(22,17),(23,19),(24,25),(25,26),(26,22)$$

and -1 for

$$(2,1),(3,2),(8,3),(10,4),(12,11),(14,13),(14,14),(15,6),(16,15),(17,8).$$

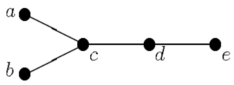
It follows from Steinberg (1962), Theorems 3.11 and 3.14 that $F_4(q)$ is generated by

$$\begin{cases} h_{A,\mu} \text{ and } x_A(1)n & \text{for } q \text{ odd and } q > 3 \\ x_A(1) \text{ and } n & \text{for } q = 3 \\ h_{2B+C,\mu} \text{ and } x_C(1)x_{-B}(1)n & \text{for } q \text{ even and } q > 2 \\ x_C(1)x_{-B}(1) \text{ and } n & \text{for } q = 2, \end{cases}$$

where μ is a primitive element of $\mathbb{F}_q$.

Except when $\mathbb{F}_q$ has characteristic 3 this representation of $F_4(q)$ is irreducible. In characteristic 3 we have $u_0 = u_{13} + u_{14} \in U$ and the quotient $U/\langle u_0 \rangle$ affords an irreducible representation of $F_4(q)$ of dimension 25.

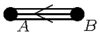
3.6. G_2. Let a, b, c, d and e be the fundamental roots for the root system of type D_5 as shown in the Dynkin diagram:



The root system of type D_5 has 20 positive roots and that of D_4 has 12. The ordering given in §2 for the roots in $\Phi^+(D_5) \setminus \Phi^+(D_4)$ is $a+b+2c+2d+e$, $a+b+2c+d+e$, $a+b+c+d+e$, $b+c+d+e$, $a+c+d+e$, $c+d+e$, $d+e$, e. Applying the methods of §2 gives an 8-dimensional representation ϕ of the Lie algebra $\mathcal{L}$ of type D_4 such that

$$\begin{aligned} \phi(e_a) &= E_{3,4} + E_{5,6}, \\ \phi(e_b) &= E_{3,5} + E_{4,6}, \\ \phi(e_c) &= E_{2,3} + E_{6,7}, \\ \phi(e_d) &= E_{1,2} + E_{7,8} \end{aligned}$$

and where $\phi(e_{-\alpha})$ is the transpose of $\phi(e_\alpha)$ for all $\alpha \in \Delta$.

We regard the Lie algebra of type G_2 as the subalgebra of fixed points $\mathcal{L}^\sigma$ of the diagram automorphism σ of order three of $\mathcal{L}$. The restrictions of a and c to H^σ are the fundamental roots A and B for $\mathcal{L}^\sigma$ and we have $e_A = \tilde{e}_a = e_a + e_b + e_d$ and $e_B = \tilde{e}_c = e_c$. The Cartan matrix of $\mathcal{L}$ is $\begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$ and the considerations of §3.4 show that the Cartan matrix for $\mathcal{L}^\sigma$ is $\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$ and hence its Dynkin diagram is of type G_2, namely 
.

The restriction of ϕ to $\mathcal{L}^\sigma$ gives an 8-dimensional representation V of G_2 with basis $v_1, \ldots, v_8$. This representation is reducible and there is an $\mathcal{L}^\sigma$-invariant submodule U with basis u_i, $i = 1, \ldots, 7$, where

$$u_i = \begin{cases} v_i & \text{for } 1 \le i < 4 \\ v_4 + v_5 & \text{for } i = 4 \\ v_{i+1} & \text{for } 4 < i \le 7 \end{cases}$$

In characteristic 0, we have $V = U \oplus \langle u_0 \rangle$ as $\mathcal{L}^\sigma$-modules, where $u_0 = -v_4 + v_5$. In any characteristic, $\langle u_0 \rangle$ is the unique 1-dimensional $\mathcal{L}^\sigma$-submodule of V.

Let ψ denote the restriction of ϕ to $\mathcal{L}^\sigma$ with respect to the basis u_i of U. We have

$$\begin{aligned} \psi(e_A) &= E_{1,2} + 2E_{3,4} + E_{4,5} + E_{6,7}, \\ \psi(e_{-A}) &= E_{2,1} + E_{4,3} + 2E_{5,4} + E_{7,6}, \\ \psi(e_B) &= E_{2,3} + E_{5,6}, \\ \psi(e_{-B}) &= E_{3,2} + E_{6,5} \end{aligned}$$

and later we shall need

$$\begin{aligned} \psi(e_{A+B}) &= E_{1,3} - 2E_{2,4} + E_{4,6} - E_{5,7}, \\ \psi(e_{-A-B}) &= -E_{3,1} + E_{4,2} - 2E_{6,4} + E_{7,5}, \\ \psi(e_{2A+B}) &= -2E_{1,4} + E_{2,5} + E_{3,6} - E_{4,7} \quad \text{and} \\ \psi(e_{-2A-B}) &= -E_{4,1} + E_{5,2} + E_{6,3} - 2E_{7,4}. \end{aligned}$$

The group $G_\psi(q)$ is generated by the elements $x_\alpha(\xi) = I + \xi\psi(e_\alpha) + \frac{1}{2}\xi^2\psi(e_\alpha)^2$ for $\pm\alpha \in \{A, B\}$ and $\xi \in \mathbb{F}_q$; it is isomorphic to $G_2(q)$.

In particular we have

$$\begin{aligned} x_A(\xi) &= I + \xi E_{1,2} + 2\xi E_{3,4} + \xi E_{4,5} + \xi E_{6,7} + \xi^2 E_{3,5}, \\ x_{-A}(\xi) &= I + \xi E_{2,1} + \xi E_{4,3} + 2\xi E_{5,4} + \xi E_{7,6} + \xi^2 E_{5,3}, \\ x_B(\xi) &= I + \xi e_B = I + \xi E_{2,3} + \xi E_{5,6}, \\ x_{-B}(\xi) &= I + \xi e_{-B} = I + \xi E_{3,2} + \xi E_{6,5}, \\ n &= n_A(1)n_B(1) = E_{1,3} - E_{2,1} + E_{3,6} - E_{4,4} - E_{5,2} + E_{6,7} + E_{7,5}, \\ h_{A,\xi} &= \xi E_{1,1} + \xi^{-1}E_{2,2} + \xi^2 E_{3,3} + E_{4,4} + \xi^{-2}E_{5,5} + \xi E_{6,6} + \xi^{-1}E_{7,7}, \\ h_{B,\xi} &= E_{1,1} + \xi E_{2,2} + \xi^{-1}E_{3,3} + E_{4,4} + \xi E_{5,5} + \xi^{-1}E_{6,6} + E_{7,7} \quad \text{and} \\ h_{2A+B,\xi} &= \xi^2 E_{1,1} + \xi E_{2,2} + \xi E_{3,3} + E_{4,4} + \xi^{-1}E_{5,5} + \xi^{-1}E_{6,6} + \xi^{-2}E_{7,7}. \end{aligned}$$

It follows from Steinberg (1962), Theorems 3.11 and 3.14 that $G_2(q)$ is generated by

$$\begin{cases} h_{2A+B,\mu} \text{ and } x_B(1)x_{-A}(1)n & \text{for } q \equiv 0 \bmod 3 \\ h_{A,\mu} \text{ and } x_A(1)n & \text{for } q \not\equiv 0 \bmod 3 \text{ and } q \ne 2 \\ x_A(1) \text{ and } n & \text{for } q = 2, \end{cases}$$

where μ is a primitive element of $\mathbb{F}_q$.

Except for characteristic 2 this representation of $G_2(q)$ is irreducible. In characteristic 2 the subspace spanned by the fourth basis element is fixed, and so by taking the quotient an irreducible representation of dimension 6 is obtained.

4. The twisted groups

This section deals with the twisted groups ${}^2B_2$, ${}^3D_4$, ${}^2E_6$, ${}^2F_4$ and ${}^2G_2$. Each twisted group ${}^kG(q)$ is generated by fixed points of an automorphism of $G(q^k)$ or $G(q)$ of order k which arises from a field automorphism and an automorphism of order k of the underlying graph of the Dynkin diagram. In the case of a single root length, the twisted group ${}^kG(q)$ is a subgroup of $G(q^k)$ and the field automorphism is the Frobenius map. On the other hand, when there is more than one root length, a power of the field automorphism is the Frobenius map over the prime field. A consequence of this is that ${}^kG(q)$ is defined only for some values of q, and is a subgroup of $G(q)$. See Chapters 13 and 14 of Carter (1972) for the definition and a discussion of these groups.

For $\xi \in \mathbb{F}_q$ write ξ^σ for the image of ξ under the field automorphism, for $\alpha \in \Phi$ write $\overline{\alpha}$ for the image of α under the map on Φ corresponding to the graph automorphism and write $\overline{x}$ for the image of x under the associated group automorphism.

Except for ${}^2B_2(2)$, ${}^2F_4(2)$ and ${}^2G_2(3)$, the twisted groups are simple (Steinberg (1967), p. 186 and Carter (1972), Chapter 14).

4.1. **The groups ${}^2B_2$.** The Dynkin diagrams of types B_2 and C_2 are the same ($\underset{a}{\bullet}\!\Rightarrow\!\underset{b}{\bullet}$) and the underlying graph has an automorphism of order 2. When the order q of the field is an odd power of 2 there is a field automorphism which, when combined with the graph automorphism, induces an automorphism of the group $B_2(q)$. The group ${}^2B_2(q)$ of fixed points is also known as a Suzuki group. They were first described in Suzuki (1960) and then interpreted as twisted groups of Lie type by Ree (Tits 1960). Thus in this section $\mathbb{F}_q$ will denote the field of order $q = 2^{2m+1}$ and σ will be the automorphism of $\mathbb{F}_q$ such that $\xi^\sigma = \xi^{2^m}$; that is, $2\sigma^2 = 1$. This field automorphism combined with the graph automorphism extends to an automorphism of the group given by $\overline{x_X(\xi)} = \begin{cases} x_{\overline{X}}(\xi^\sigma) & X \text{ a long root} \\ x_{\overline{X}}(\xi^{2\sigma}) & X \text{ a short root} \end{cases}$.

Even though we refer to the groups as ${}^2B_2(q)$, we use the four dimensional (symplectic) representation obtained from the embedding of C_2 in C_3. The following elements of ${}^2B_2(q)$ will be needed:

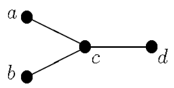
$$\begin{aligned} x &= x_a(1)x_b(1)x_{a+2b}(1) = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \\ n &= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \\ h(\xi) &= h_a(\xi)\overline{h_a(\xi)} = h_a(\xi)h_b(\xi^\sigma) \\ &= \operatorname{diag}(\xi^\sigma, \xi^{-\sigma+1}, \xi^{\sigma-1}, \xi^{-\sigma}). \end{aligned}$$

It follows from Steinberg (1962), Theorem 4.1 that ${}^2B_2(q)$ is generated by

$$\begin{cases} h(\mu) \text{ and } xn & \text{for } q > 2 \\ x \text{ and } n & \text{for } q = 2 \end{cases}$$

where μ is a primitive element of $\mathbb{F}_q$.

4.2. **The groups $^3D_4$.** The simple group $^3D_4(q)$ is a subgroup of the orthogonal group $\Omega^+(8,q^3)$, which we identify with the Chevalley group of type D_4 over F_{q^3}. It is defined in terms of an automorphism of $\Omega^+(8,q^3)$ of order 3 which arises from the diagram automorphism of order 3 and the Frobenius map of order 3.



For $\xi \in \mathbb{F}_{q^3}$ the Frobenius map sends ξ to ξ^q. The group automorphism is given by $x_\alpha(\xi) = x_{\overline{\alpha}}(\xi^q)$.

We begin with the 8-dimensional representation of the Lie algebra of type D_4 given in §3.6. From the matrices $\phi(e_\alpha)$, $\pm\alpha \in \{a,b,c,d\}$, we obtain the following elements of the Chevalley group of type D_4.

$$\begin{aligned}
x_a(\xi) &= I + \xi E_{3,4} + \xi E_{5,6},\\
x_b(\xi) &= I + \xi E_{3,5} + \xi E_{4,6},\\
x_c(\xi) &= I + \xi E_{2,3} + \xi E_{6,7},\\
x_d(\xi) &= I + \xi E_{1,2} + \xi E_{7,8}
\end{aligned}$$

and $x_{-\alpha}(\xi) = x_\alpha(\xi)^t$ for $\alpha \in \{a,b,c,d\}$. From these elements we derive

$$\begin{aligned}
n_a(\xi) &= E_{1,1} + E_{2,2} + \xi E_{3,4} - \xi^{-1}E_{4,3} + \xi E_{5,6} - \xi^{-1}E_{6,5} + E_{7,7} + E_{8,8},\\
n_b(\xi) &= E_{1,1} + E_{2,2} + \xi E_{3,5} + \xi E_{4,6} - \xi^{-1}E_{5,3} - \xi^{-1}E_{6,4} + E_{7,7} + E_{8,8},\\
n_c(\xi) &= E_{1,1} + \xi E_{2,3} - \xi^{-1}E_{3,2} + E_{4,4} + E_{5,5} + \xi E_{6,7} - \xi^{-1}E_{7,6} + E_{8,8},\\
n_d(\xi) &= \xi E_{1,2} - \xi^{-1}E_{2,1} + E_{3,3} + E_{4,4} + E_{5,5} + E_{6,6} + \xi E_{7,8} - \xi^{-1}E_{8,7},\\
h_{a,\xi} &= \mathrm{diag}(1,1,\xi,\xi^{-1},\xi,\xi^{-1},1,1),\\
h_{b,\xi} &= \mathrm{diag}(1,1,\xi,\xi,\xi^{-1},\xi^{-1},1,1),\\
h_{c,\xi} &= \mathrm{diag}(1,\xi,\xi^{-1},1,1,\xi,\xi^{-1},1) \quad \text{and}\\
h_{d,\xi} &= \mathrm{diag}(\xi,\xi^{-1},1,1,1,1,\xi,\xi^{-1}).
\end{aligned}$$

We take $x_R(\xi) = x_a(\xi)x_b(\xi^\sigma)x_d(\xi^{\sigma^2})$ for $\xi \in \mathbb{F}_{q^3}$ and $x_c(\eta)$ for $\eta \in \mathbb{F}_q$ to be the fundamental root elements for the group $^3D_4(q)$. Then we have

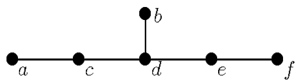
$$\begin{aligned}
x_R(1) &= I + E_{1,2} + E_{3,4} + E_{3,5} + E_{3,6} + E_{4,6} + E_{5,6} + E_{7,8},\\
n_R(1) &= x_R(1)x_{-R}(-1)x_R(1) = n_a(1)n_b(1)n_d(1)\\
&= E_{1,2} - E_{2,1} + E_{3,6} - E_{4,5} - E_{5,4} + E_{6,3} + E_{7,8} - E_{8,7},\\
n &= n_R(1)n_c(1) = E_{1,3} - E_{2,1} + E_{3,7} - E_{4,5} - E_{5,4} - E_{6,2} + E_{7,8} + E_{8,6} \quad \text{and}\\
h_R(\xi) &= h_{a,\xi}h_{b,\xi^\sigma}h_{d,\xi^{\sigma^2}} = \mathrm{diag}(\xi^{\sigma^2},\xi^{-\sigma^2},\xi^{\sigma+1},\xi^{\sigma-1},\xi^{-\sigma+1},\xi^{-\sigma-1},\xi^{\sigma^2},\xi^{-\sigma^2}).
\end{aligned}$$

It follows from Steinberg (1962), Theorem 4.1 that $^3D_4(q)$ is generated by

$$h_R(\mu) \text{ and } x_R(1)n$$

where μ is a primitive element of the field $\mathbb{F}_{q^3}$.

4.3. **The groups** $^2E_6$**.** Label the fundamental roots as in §3.3:



The diagram automorphism of order 2, combined with the Frobenius map $\xi \mapsto \xi^\sigma = \xi^q$ of the field F_{q^2}, gives rise to an automorphism $g \mapsto \overline{g}$ of the group $G_\phi(q^2)$ of type E_6 (defined in §3.3) such that $\overline{x_\alpha(\xi)} = x_{\overline{\alpha}}(\xi^\sigma)$. The fixed points of this automorphism form the group $\overline{G}_\phi(q)$ of type $^2E_6$. If 3 divides $q+1$ and if ω is an element of order 3 in $\mathbb{F}_{q^2}$, then $h_{a,\omega^2}h_{f,\omega}h_{c,\omega}h_{e,\omega^2}$ is an element of order 3 in the centre of $\overline{G}_\phi(q)$. In this case $\overline{G}_\phi(q)$ is the central extension $3\,{}^2E_6(q)$ of the twisted simple group $^2E_6(q)$; otherwise it is the simple group $^2E_6(q)$ itself.

As fundamental root elements for the group $\overline{G}_\phi(q)$ we take $x_R(\xi) = x_a(\xi)x_f(\xi^\sigma)$ and $x_S(\xi) = x_c(\xi)x_e(\xi^\sigma)$ for $\xi \in \mathbb{F}_{q^2}$ and $x_d(\eta)$ and $x_b(\eta)$ for $\eta \in \mathbb{F}_q$. Then

$$\begin{aligned} x_R(1) &= I + E_{1,2} + E_{6,8} + E_{7,10} + E_{9,12} + E_{11,13} + E_{11,14} + E_{11,16} + E_{13,16} \\ &\qquad + E_{14,16} + E_{17,18} + E_{19,20} + E_{21,22} + E_{26,27}, \quad \text{and} \\ x_S(1) &= I + E_{2,3} + E_{4,6} + E_{5,7} + E_{9,11} + E_{12,14} + E_{12,15} + E_{12,17} + E_{14,17} \\ &\qquad + E_{15,17} + E_{16,18} + E_{20,23} + E_{22,24} + E_{25,26}. \end{aligned}$$

From these elements and similar expressions for $x_{-R}(1)$ and $x_{-S}(1)$ we derive $n_R(1) = x_R(1)x_{-R}(-1)x_R(1)$ and $n_S(1) = x_S(1)x_{-S}(-1)x_S(1)$.

Then a Coxeter element is given by $n = n_R(1)n_S(1)n_d(1)n_b(1)$; it has nonzero entries equal to 1 for indices

$$\begin{gathered} (1,5),(4,7),(5,9),(6,10),(7,12),(9,21),(11,22),(13,15),(19,24),(20,17), \\ (21,25),(22,19),(23,18),(24,20),(25,26),(26,27),(27,23) \end{gathered}$$

and -1 for

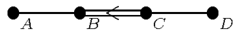
$$(2,1),(3,2),(8,3),(10,4),(12,11),(14,13),(15,14),(16,6),(17,16),(18,8).$$

The diagonal matrix $h_R(\xi) = h_{a,\xi}h_{f,\xi^\sigma}$ has its ith diagonal entry equal to

$$\begin{cases} \xi & i = 1, 17, 19 \text{ or } 21 \\ \xi^{-1} & i = 2, 18, 20 \text{ or } 22 \\ \xi^{\sigma} & i = 6, 7, 9 \text{ or } 26 \\ \xi^{-\sigma} & i = 8, 10, 12 \text{ or } 27 \\ \xi^{\sigma+1} & i = 11 \\ \xi^{\sigma-1} & i = 13 \\ \xi^{-\sigma+1} & i = 14 \\ \xi^{-\sigma-1} & i = 16 \\ 1 & \text{otherwise.} \end{cases}$$

By Steinberg (1962), Theorem 4.1 $^2E_6(q)$ is generated by $h_R(\mu)$ and $x_R(1)n$ where μ is a primitive element of $\mathbb{F}_{q^2}$.

4.4. **The groups $^2F_4$ and the Tits group.** The Dynkin diagram of type F_4 is



The underlying graph has an automorphism of order 2. The groups $^2F_4(q)$ were introduced by Ree (1961a) and are defined only when the field has order an odd power of 2. Thus let $\mathbb{F}_q$ be the field of order $q = 2^{2m+1}$. There is an automorphism σ of $\mathbb{F}_q$ such that $\xi^\sigma = \xi^{2^m}$; that is, $2\sigma^2 = 1$. This field automorphism combined with the graph automorphism $X \mapsto \overline{X}$ extends to an automorphism of the group given by

$$\overline{x_X(\xi)} = \begin{cases} x_{\overline{X}}(\xi^\sigma) & X \text{ a long root} \\ x_{\overline{X}}(\xi^{2\sigma}) & X \text{ a short root} \end{cases}.$$

We use the representation and elements given in §3.5. Let $x = x_B(1)x_C(1)x_{2B+C}(1)$; its matrix has 1's on the diagonal and the other nonzero entries are 1 for indices

$$\begin{gathered}(2,3),(2,4),(2,6),(3,4),(4,6),(5,7),(5,9),(5,11),(7,9),(9,11),(10,12),\\(10,16),(10,18),(12,13),(12,16),(14,16),(14,18),(15,17),(15,19),(15,22),\\(16,18),(17,19),(19,22),(21,23),(21,24),(21,25),(23,24),(24,25).\end{gathered}$$

The matrix for

$$\begin{aligned} n = n_{2B+C}(1)n_C(1)n_A(1)n_D(1) &= (n_B(1)n_C(1))^3 n_A(1)n_D(1) = \\ & x_{2B+C}(1)x_C(1)x_{-2B-C}(-1)x_{-C}(-1) \times \\ & \quad x_{2B+C}(1)x_C(1)x_A(1)x_D(1)x_{-A}(-1)x_{-D}(-1)x_A(1)x_D(1) \end{aligned}$$

has nonzero entries equal to 1 for indices

$$\begin{gathered}(1,2),(2,10),(3,5),(4,3),(5,15),(6,1),(7,12),(8,7),(9,8),(10,21),\\(11,4),(12,17),(13,13),(13,14),(14,14),(15,23),(16,9),(17,20),(18,6),\\(19,16),(20,19),(21,26),(22,11),(23,24),(24,22),(25,18),(26,25).\end{gathered}$$

The diagonal matrix $h(\xi) = h_{B,\xi}\overline{h_{B,\xi}} = h_{B,\xi}h_{C,\xi^\sigma}$ has ith diagonal entry

$$\begin{cases} \xi & i = 2, 5, 15 \text{ or } 21 \\ \xi^{-1} & i = 6, 11, 22 \text{ or } 25 \\ \xi^{-\sigma+1} & i = 4, 9, 19 \text{ or } 24 \\ \xi^{\sigma-1} & i = 3, 7, 17 \text{ or } 23 \\ \xi^\sigma & i = 10 \\ \xi^{-\sigma+2} & i = 12 \\ \xi^{\sigma-2} & i = 16 \\ \xi^{-\sigma} & i = 18 \\ 1 & \text{otherwise.} \end{cases}$$

It follows from Steinberg (1962), Theorem 4.1 that $^2F_4(q)$ is generated by

$$\begin{cases} h(\mu) \text{ and } xn & \text{for } q > 2 \\ x \text{ and } n & \text{for } q = 2 \end{cases}$$

where μ is a primitive element of $\mathbb{F}_q$.

The Tits group is the simple group $(^2F_4(2))'$; it has index 2 in $^2F_4(2)$ (Carter 1972, §14.4). The group $(^2F_4(2))'$ is generated by

$$xnx^{-1}n^{-1} \text{ and } n.$$

4.5. **The groups $^2G_2$.** Ree (1961b) describes these groups and gives a matrix representation for them equivalent to the one given here.

Let $q = 3^{2m+1}$ and let σ be the automorphism of $\mathbb{F}_q$ defined by $\xi^\sigma = \xi^{3^m}$ (and so $3\sigma^2 = 1$). The field automorphism σ combined with the graph automorphism $X \mapsto \overline{X}$ (interchanging roots A and B) extends to an automorphism of the group given by $\overline{x_X(\xi)} = \begin{cases} x_{\overline{X}}(\xi^\sigma) & X \text{ a long root} \\ x_{\overline{X}}(\xi^{3\sigma}) & X \text{ a short root} \end{cases}$.

We use the notation from §3.6, but choose different structure constants for the Lie algebra of type G_2 to ensure that the graph automorphism has a nice form (Carter 1972, §12.4). The structure constants are determined by putting $c_{\alpha,\beta} = -(r+1)$ instead of $r+1$ whenever (α, β) is the extraspecial pair for $\alpha+\beta$ in the algorithm in §2. We obtain the following elements of $^2G_2(q)$.

$$\begin{aligned}
x(\xi) &= x_A(\xi^\sigma)x_B(\xi)x_{A+B}(\xi^{\sigma+1})x_{2A+B}(\xi^{2\sigma+1}), \\
x(1) &= \begin{pmatrix} 1&1&0&0&1&2&2 \\ 0&1&1&2&1&0&1 \\ 0&0&1&2&1&0&2 \\ 0&0&0&1&1&0&0 \\ 0&0&0&0&1&1&1 \\ 0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&1 \end{pmatrix}, \\
n' &= (n_A(1)n_B(1))^3 = E_{1,7} - E_{2,6} + E_{3,5} - E_{4,4} + E_{5,3} - E_{6,2} + E_{7,1} \quad \text{and} \\
h(\xi) &= h_A(\xi)\overline{h_A(\xi)} = h_A(\xi)h_B(\xi^{3\sigma}) \\
&= \xi E_{1,1} + \xi^{3\sigma-1}E_{2,2} + \xi^{2-3\sigma}E_{3,3} + E_{4,4} + \xi^{3\sigma-2}E_{5,5} + \xi^{1-3\sigma}E_{6,6} + \xi^{-1}E_{7,7}.
\end{aligned}$$

It follows from Steinberg (1962), Theorem 4.1 that $^2G_2(q)$ is generated by $h(\mu)$ and $x(1)n'$ where μ is a primitive element of $\mathbb{F}_q$.

5. Availability

The generators for all the groups described in this paper have been included in Magma since V2.4.

References

Bosma, W., Cannon, J., Playoust, C. (1997). The Magma algebra system I: The user language. *J. Symbolic Comput.*, 24:235–265.

Carter, R. W. (1972). *Simple Groups of Lie Type.* Wiley-Interscience, New-York.

Gilkey, P. B., Seitz, G. M. (1988). Some representations of exceptional Lie algebras. *Geom. Dedicata*, 25:407–416.

Humphreys, J. E. (1972). *Introduction to Lie Algebras and Representation Theory*, volume 9 of *Graduate Texts in Mathematics.* Springer-Verlag, New York Heidelberg Berlin.

Jacobson, N. (1962). *Lie Algebras*, volume 10 of *Interscience Tracts in Pure and Applied Mathematics.* Interscience, New York.

Ree, R. (1961a). A family of simple groups associated with the simple Lie algebras of type (F_4). *Amer. J. Math.*, 83:401–420.

Ree, R. (1961b). A family of simple groups associated with the simple Lie algebras of type (G_2). *Amer. J. Math.*, 83:432–462.

Rylands, L. J., Taylor, D. E. (1998). Matrix generators for the orthogonal groups. *J. Symbolic Comput.*, 25:351–360.

Schönert, M. *et al.*(1994). *GAP — Groups, Algorithms and Programming.* Lehrstuhl D für Mathematik, RWTH Aachen.

Steinberg, R. (1962). Generators for simple groups. *Canad. J. Math.*, 14:277–283.

Steinberg, R. (1967). *Lectures on Chevalley Groups.* Yale.

Suzuki, M. (1960). A new type of simple groups of finite order. *Proc. Nat. Acad. Sci. U.S.A.*, 46:868–870.

Taylor, D. E. (1987). Pairs of generators for matrix groups I. *The Cayley Bulletin*, 3:76–85. `http://www.maths.usyd.edu.au:8000/u/don`.

Tits, J. (1960). Les groupes simples de Suzuki et Ree. *Séminaire Bourbaki 1960/61*, exp 210.

Tits, J. (1967). *Tabellen zu der einfachen Lie Gruppen und ihren Darstellungen*, volume 40 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin Heidelberg.

School of Mathematics and Statistics, University of Sydney, Australia
E-mail address: `R.Howlett@maths.usyd.edu.au`

School of Science, University of Western Sydney, Nepean, Australia
E-mail address: `L.Rylands@nepean.uws.edu.au`

School of Mathematics and Statistics, University of Sydney, Australia
E-mail address: `D.Taylor@maths.usyd.edu.au`