J. Symbolic Computation (1998) **25**, 351–360

Matrix Generators for the Orthogonal Groups

L. J. RYLANDS[†] AND D. E. TAYLOR[‡]

Department of Mathematics, University of Western Sydney, Nepean, Australia
School of Mathematics and Statistics, University of Sydney, Australia

In 1962 Steinberg gave pairs of generators for all finite simple groups of Lie type. In this paper, for each finite orthogonal group we provide a pair of matrices which generate its derived group: the matrices correspond to Steinberg's generators modulo the centre. These generators have been implemented in the computer algebra system MAGMA and this completes the provision of pairs of generators in MAGMA for all (perfect) finite classical groups.

1. Introduction

Generators for the groups $SL(l,q)$, $Sp(2m,q)$, $U(l,q)$ and $Sz(q)$ have been available in computer algebra systems for some time (Taylor, 1987; Schönert *et al.*, 1994; Bosma, *et al.*, 1997). Until recently it has only been practical to work with these groups for small dimensions and small fields. This covered small orthogonal groups (but not in their natural representation) because the orthogonal groups up to dimension 6 are isomorphic to other linear groups. For a complete description of the isomorphisms see Chapters 11 and 12 in Taylor (1992).

However, recent advances in computing speed and memory, as well as better algorithms, make it possible to work with larger groups. Hence there has been an increasing need for matrix generators for the orthogonal groups, particularly in dimensions beyond 6. This demand comes from several sources. For example, those working directly with orthogonal groups as well as those wishing to test new linear group recognition algorithms (Niemeyer and Praeger, 1998; Celler and Leedham-Green, 1997) now need generators for all classical groups. The recent paper by Ishibashi and Earnest (1994a, b) provides generators for $O(l,q)$, but not for $SO(l,q)$ nor its derived group $\Omega(l,q)$. The matrices of Ishibashi and Earnest have been implemented in GAP by Celler (1994, ogroup.g.3.4, GAP library).

In 1962 Steinberg gave pairs of generators for all finite simple groups of Lie type. Steinberg's generators are given in terms of root elements and generators for the Weyl group. In this paper we describe the corresponding generators for the finite orthogonal groups

[†] E-mail: `l.rylands@nepean.uws.edu.au`
[‡] E-mail: `D.Taylor@maths.usyd.edu.au`

0747–7171/98/030351 + 10 $25.00/0 sy970180

$\Omega(l,q)$. These generators are presented as matrices and are equal to Steinberg's generators modulo the centre of the group. The purpose is to provide explicit constructions for the orthogonal groups which can be used within computer algebra packages such as MAGMA (Bosma *et al.*, 1997) or GAP (Schönert *et al.*, 1994). Our methods are easily adapted to provide generators for $SO(l,q)$ and $O(l,q)$.

In the first part of the paper we outline the (well known) connection between the orthogonal groups and the Chevalley groups of types B_m, D_m and ${}^2D_m$ via their Lie algebras. This leads directly to the construction of the matrix generators in terms of root elements and the BN-pair structure.

2. Preliminaries

There are three families of finite orthogonal groups and, except for a few small cases, they correspond to Dynkin diagrams of types B_m, D_m and ${}^2D_m$. Steinberg (1962) provided generators for the Chevalley groups in terms of root elements and it is our intention to lift his generators to the corresponding matrix groups. As a general reference see Humphreys (1972), particularly Sections 8 and 25.2.

We begin by reviewing the connection between orthogonal groups defined by quadratic forms and Chevalley groups defined in terms of simple Lie algebras of types B_m and D_m.

A quadratic form on a vector space V over a field $\mathbb{F}$ is a function $Q : V \to \mathbb{F}$ such that $Q(av) = a^2Q(v)$ and $\beta(u,v) = Q(u+v) - Q(u) - Q(v)$ is bilinear. It is non-degenerate if $Q(v) \neq 0$ for all nonzero elements v of the radical of β. For details see Taylor (1992). If the characteristic of $\mathbb{F}$ is not 2, β is a non-degenerate symmetric bilinear form and uniquely determines Q. If the characteristic of $\mathbb{F}$ is 2 then β is an alternating form and the dimension of its radical is either 1 or 0.

It is always possible to write V as an orthogonal direct sum

$$V = L_1 \perp L_2 \perp \ldots \perp L_m \perp W$$

where $L_i = \langle e_i, f_i \rangle$, $Q(e_i) = Q(f_i) = 0$, $\beta(e_i, f_i) = 1$ and W is a subspace with no singular vectors. If $\mathbb{F}$ is finite, the dimension of W is 0, 1 or 2. If $\mathbb{F}$ is algebraically closed (e.g., $\mathbb{C}$) the dimension of W is 0 or 1. The integer m is the Witt index of Q and we let l be the dimension of V.

In describing the groups and Lie algebras associated with a quadratic form Q we shall write matrices with respect to the ordered basis

$$e_1, e_2, \ldots, e_m, w_1, \ldots, w_k, f_m, \ldots, f_1$$

where $w_1, \ldots, w_k$ is a basis of W to be chosen later. We use J to denote the matrix of β with respect to this basis.

In the case $\mathbb{F} = \mathbb{C}$, the complex Lie algebra $\mathcal{L}$ of Q consists of all $l \times l$ matrices X such that $X^tJ + JX = 0$ with Lie product $[xy] = xy - yx$.

Over the complex numbers there is just one non-degenerate quadratic form in each dimension. If $l = 2m$, we have

$$J = \begin{pmatrix} & & & 1 \\ & & \iddots & \\ & 1 & & \\ 1 & & & \end{pmatrix}$$

and $\mathcal{L}$ is of type D_m. If $l = 2m+1$, we may take $W = \langle w \rangle$, where $Q(w) = 1$ (hence

$\beta(w,w)=2$),

$$J=\begin{pmatrix} & & & & & & 1\\ & & & & & \cdot^{\cdot^{\cdot}} & \\ & & & & 1 & & \\ & & & 2 & & & \\ & & 1 & & & & \\ & \cdot^{\cdot^{\cdot}} & & & & & \\ 1 & & & & & & \end{pmatrix}$$

and $\mathcal{L}$ is of type B_m.

In type D_m the diagonal matrices of $\mathcal{L}$ have the form

$$h=\operatorname{diag}(\lambda_1,\lambda_2,\dots,\lambda_m,-\lambda_m,\dots,-\lambda_1)$$

and in type B_m they have the form

$$h=\operatorname{diag}(\lambda_1,\lambda_2,\dots,\lambda_m,0,-\lambda_m,\dots,-\lambda_1).$$

In both cases the set H of these matrices is a Cartan subalgebra.

The root space of $\alpha\in H^*$ is $\mathcal{L}_\alpha=\{x\in\mathcal{L}\mid[hx]=\alpha(h)x\}$ and the set Φ of nonzero α such that $\mathcal{L}_\alpha\neq 0$ is the root system of H. For $\alpha\in\Phi$, $\dim L_\alpha=1$ and we have the Cartan decomposition $\mathcal{L}=H\oplus\bigoplus_{\alpha\in\Phi}\mathcal{L}_\alpha$.

The real vector space spanned by the roots may be identified with the Euclidean space $\mathbb{R}^m$ with orthonormal basis $\varepsilon_1,\dots,\varepsilon_m$ given by $\varepsilon_i(h)=\lambda_i$, where h is defined as above.

For each $\alpha\in\Phi$ there is a unique element $h_\alpha\in H$ such that $\alpha(h_\alpha)=2$ and $h_\alpha\in[\mathcal{L}_\alpha\mathcal{L}_{-\alpha}]$. We shall choose a set of fundamental roots $\Delta=\{\alpha_1,\alpha_2,\dots,\alpha_m\}$ and elements $x_\alpha\in\mathcal{L}_\alpha$, for $\alpha\in\Phi$, such that $\{x_\alpha,h_{\alpha_i}\mid\alpha\in\Phi,1\le i\le m\}$ forms a Chevalley basis for $\mathcal{L}$. That is, $[x_\alpha x_{-\alpha}]=h_\alpha$ and for $\alpha,\beta,\alpha+\beta\in\Phi$, $[x_\alpha x_\beta]=c_{\alpha,\beta}x_{\alpha+\beta}$, where $c_{\alpha,\beta}=-c_{-\alpha,-\beta}\in\mathbb{Z}$.

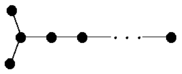
Let E_{ij} be the $l\times l$ matrix with 1 in the i,j-th position and 0 elsewhere; also let i' denote $l+1-i$.

2.1. CASE 1. TYPE D_m ($l=2m$, $m>1$)

The set of roots is $\Phi=\{\pm(\varepsilon_i\pm\varepsilon_j)\mid 1\le i<j\le m\}$. As fundamental roots for D_m we take

$$\alpha_1=\varepsilon_{m-1}+\varepsilon_m,\alpha_2=\varepsilon_{m-1}-\varepsilon_m,\dots,\alpha_m=\varepsilon_1-\varepsilon_2$$

corresponding to the Dynkin diagram



The set of positive roots is $\{\varepsilon_i\pm\varepsilon_j\mid i<j\}$.

The elements $h_i=h_{\alpha_i}$ of the Chevalley basis are

$$\begin{aligned} h_1&=E_{m-1,m-1}+E_{mm}-E_{m'm'}-E_{(m-1)',(m-1)'} && \text{and}\\ h_k&=E_{m+1-k,m+1-k}-E_{m+2-k,m+2-k}\\ &\quad+E_{(m+2-k)',(m+2-k)'}-E_{(m+1-k)',(m+1-k)'} && k=2,\dots,m.\end{aligned}$$

Then $\{h_i\mid 1\le i\le m\}$ is a basis for H.

Now define a map $\mu : \Phi \to \mathcal{L}$ such that $\mu(\alpha)$ spans $\mathcal{L}_\alpha$ by

$$\begin{aligned} \mu(\varepsilon_i - \varepsilon_j) &= E_{ij} - E_{j'i'} && i \neq j \\ \mu(\varepsilon_i + \varepsilon_j) &= -E_{ij'} + E_{ji'} && i < j \\ \mu(-\varepsilon_i - \varepsilon_j) &= E_{i'j} - E_{j'i} && i < j. \end{aligned}$$

The set $\mu(\Phi)$ completes the Chevalley basis as is shown by the easy but tedious calculation that for all $\alpha, \beta \in \Phi$

$$[\mu(\alpha)\mu(\beta)] = \begin{cases} \pm(r+1)\mu(\alpha+\beta) & \alpha+\beta \in \Phi \\ h_\alpha & \alpha+\beta = 0 \\ 0 & \alpha+\beta \notin \Phi \cup \{0\} \end{cases}$$

where $\beta - r\alpha, \ldots, \beta + q\alpha$ is the α-string through β (Humphreys, 1972, §8.4). Thus the Chevalley basis for $\mathcal{L}$ is

$$\{\mu(\alpha) \mid \alpha \in \Phi\} \cup \{h_i \mid 1 \leq i \leq m\}.$$

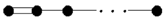
If α is a positive root then $\mu(\alpha)$ is an upper triangular matrix.

2.2. CASE 2. TYPE B_m ($l = 2m+1$)

The set of roots is $\Phi = \{\pm\varepsilon_i, \pm(\varepsilon_i \pm \varepsilon_j) \mid 1 \leq i < j \leq m\}$. As fundamental roots for B_m we take

$$\alpha_1 = \varepsilon_m, \alpha_2 = \varepsilon_{m-1} - \varepsilon_m, \alpha_3 = \varepsilon_{m-2} - \varepsilon_{m-1}, \ldots, \alpha_m = \varepsilon_1 - \varepsilon_2$$

corresponding to the Dynkin diagram



The positive roots are all ε_i, $\varepsilon_i + \varepsilon_j$ and $\varepsilon_i - \varepsilon_j$ $(i < j)$.

The elements $h_i = h_{\alpha_i}$ of the Chevalley basis are

$$\begin{aligned} h_1 &= 2E_{mm} - 2E_{m'm'} \qquad \text{and} \\ h_k &= E_{m+1-k,m+1-k} - E_{m+2-k,m+2-k} \\ &\quad + E_{(m+2-k)',(m+2-k)'} - E_{(m+1-k)',(m+1-k)'} \qquad k = 2, \ldots, m. \end{aligned}$$

Then $\{h_i \mid 1 \leq i \leq m\}$ is a basis for H.

Now define a map $\mu : \Phi \to \mathcal{L}$ such that $\mu(\alpha)$ spans $\mathcal{L}_\alpha$ by

$$\begin{aligned} \mu(\varepsilon_i - \varepsilon_j) &= E_{ij} - E_{j'i'} && i \neq j \\ \mu(\varepsilon_i + \varepsilon_j) &= -E_{ij'} + E_{ji'} && i < j \\ \mu(-\varepsilon_i - \varepsilon_j) &= E_{i'j} - E_{j'i} && i < j \\ \mu(\varepsilon_i) &= 2E_{i,m+1} - E_{m+1,i'} \\ \mu(-\varepsilon_i) &= -2E_{i',m+1} + E_{m+1,i}. \end{aligned}$$

The set $\mu(\Phi)$ completes the Chevalley basis as is shown by the easy but tedious calculation that for all $\alpha, \beta \in \Phi$

$$[\mu(\alpha)\mu(\beta)] = \begin{cases} \pm(r+1)\mu(\alpha+\beta) & \alpha+\beta \in \Phi \\ h_\alpha & \alpha+\beta = 0 \\ 0 & \alpha+\beta \notin \Phi \cup \{0\}. \end{cases}$$

Thus the Chevalley basis for $\mathcal{L}$ is

$$\{\mu(\alpha) \mid \alpha \in \Phi\} \cup \{h_i \mid 1 \leq i \leq m\}.$$

If α is a positive root then $\mu(\alpha)$ is an upper triangular matrix.

The matrices of $\frac{1}{k!}\mu(\alpha)^k$, $\alpha \in \Phi$ have integer entries (Humphreys, 1972, §25) and therefore $\exp(t\mu(\alpha))$ may be interpreted over any field. For each prime power q we let $\mathcal{L}(q)$ denote the Lie algebra spanned by $\mu(\Phi)$ over $\mathbb{F}_q$. The algebra $\mathcal{L}(q)$ acts on the vector space $V(q)$ and we shall use the same notation for its basis as for V. The quadratic form Q takes integral values on the integral linear combinations of this basis and so induces a quadratic form $Q(q)$ on $V(q)$. In all cases it remains non-singular.

3. Orthogonal Groups

From now on we work with a fixed finite field $\mathbb{F}_q$ and abbreviate $\mathcal{L}(q)$, $V(q)$ and $Q(q)$ to $\mathcal{L}$, V and Q. The group of all non-singular linear transformations of V which preserve Q is the orthogonal group $O(V,Q)$; the intersection of the kernels of the spinor norm and the Dickson invariant is $\Omega(V,Q)$. When $l = 2m$ and Q is a form of (maximal) Witt index m we denote this group by $\Omega^+(l,q)$ ($\mathcal{L}$ has type D_m in this case). When $l = 2m+1$ and the Witt index of Q is m we denote it by $\Omega^0(l,q)$ ($\mathcal{L}$ has type B_m). When $l = 2m$ and the Witt index of Q is $m-1$ we denote it by $\Omega^-(l,q)$ (see Section 5). We also denote the groups $\Omega^+(l,q)$, $\Omega^0(l,q)$ and $\Omega^-(l,q)$, by $\Omega^\epsilon(l,q)$ for $\epsilon = 1, 0, -1$. Except for $\Omega^+(4,2)$, $\Omega(V,Q)$ is the derived group of $O(V,Q)$ (Theorems 11.45 and 11.51, Taylor, 1992).

For $l \geq 3$, the groups $\Omega^\epsilon(l,q)$ are closely related to the Chevalley groups of adjoint type of the Lie algebra $\mathcal{L}$ of the previous section. The groups that do not arise as Chevalley groups are considered later.

The previous section describes a representation $\phi : \mathcal{L} \to \mathfrak{gl}(l,q)$ of $\mathcal{L}$ as $l \times l$ matrices. For each $\mu(\alpha)$ the matrix $\phi(\mu(\alpha))$ is nilpotent, hence the sum

$$\exp(\phi(t\mu(\alpha))) = 1 + t\phi\mu(\alpha) + \frac{t^2}{2!}\phi\mu(\alpha)^2 + \cdots$$

is finite (in fact in our case it has no more than three terms). Let $x_\alpha(t) = \exp(\phi(t\mu(\alpha)))$; then the Chevalley group associated with $\mathcal{L}$ and ϕ over $\mathbb{F}_q$ is

$$G = \langle x_\alpha(t) \mid t \in \mathbb{F}_q,\ \alpha \in \Phi\rangle.$$

The adjoint representation of $\mathcal{L}$ is the map ad : $\mathcal{L} \to \mathrm{End}(\mathcal{L})$ where $\mathrm{ad}(x)y = [xy]$. It is not difficult to show (Carter, 1972; theorem 4.5.1) that $\mathrm{ad}\,\mu(\alpha)$ is nilpotent. Let $\hat{x}_\alpha(t) = \exp(\mathrm{ad}\,\mu(\alpha))$, then (Carter, 1972; theorem 4.5.1)

$$\phi(\hat{x}_\alpha(t).z) = x_\alpha(t)\phi(z)x_\alpha(t)^{-1} \qquad \text{for } z \in \mathcal{L}.$$

Hence the group G is related to the Chevalley group of adjoint type, $\widehat{G} = \langle \hat{x}_\alpha(t) \mid t \in \mathbb{F}_q,\ \alpha \in \Phi\rangle$, by the homomorphism $\theta : G \to \widehat{G}$ where

$$\theta(g).z = \phi^{-1}\left(g\phi(z)g^{-1}\right) \qquad \text{for } z \in \mathcal{L},\ g \in G.$$

By construction $\theta(x_\alpha(t)) = \hat{x}_\alpha(t)$ and therefore θ is onto. Every element in the kernel of θ commutes with the image of $\phi\mu$, and hence the kernel of θ consists of scalar matrices.

Given a singular vector u and $v \in \langle u\rangle^\perp$ we define a Siegel transformation to be a map

$\rho_{u,v} \in \Omega(V)$ such that

$$\rho_{u,v}(x) = x + \beta(x,v)u - \beta(x,u)v - Q(v)\beta(x,u)u.$$

The $\rho_{u,v}$ generate $\Omega(V)$ (Taylor, 1992; Theorem 11.46). For each root α, $x_\alpha(t)$ is a Siegel transformation. For example when $\alpha = \varepsilon_i - \varepsilon_j$, $x_\alpha(t) = \rho_{te_i,f_j} = I + t(E_{ij} - E_{j'i'})$ and when $\alpha = \varepsilon_i$, $x_\alpha(t) = \rho_{te_i,w} = I + t(2E_{i,m+1} - E_{m+1,i'}) - t^2 E_{ii'}$.

This proves:

THEOREM 3.1. *For* $\epsilon = 0, 1$, $G = \Omega^\epsilon(l,q)$ *and the kernel of* θ *has order* 1 *or* 2.

4. Generators for $\Omega^+(l,q)$ and $\Omega^0(l,q)$

In this section ξ will be a generator of the group $\mathbb{F}_q^\times$. For each positive root α there exists an element $h_{\alpha,\xi}$ such that $h_{\alpha,\xi} x_\beta(k) h_{\alpha,\xi}^{-1} = x_\beta(\xi^{2\frac{(\beta,\alpha)}{(\alpha,\alpha)}} k)$ for all $k \in \mathbb{F}_q^\times$ and $\beta \in \Phi$ (Steinberg, 1962; Theorem 3.4); in what follows a diagonal matrix will suffice, and it is easy to check that it satisfies the conditions.

As in Steinberg (1962; Theorem 3.7), for each $\alpha \in \Phi^+$, $n_\alpha = x_\alpha(1)x_{-\alpha}(-1)x_\alpha(1)$. Write n_i for n_{α_i}.

We are now ready to give matrices for Steinberg's generators for the groups $\Omega^\epsilon(l,q)$ for $\epsilon = 0, 1$.

4.1. TYPE D_m $(l = 2m)$ m EVEN $m > 3$

In this case

$$\begin{aligned} x_{\alpha_1}(1) &= I + \phi\mu(\alpha_1) = I - E_{m-1,m'} + E_{m,(m-1)'}, \\ x_{-\alpha_1}(1) &= I + \phi\mu(-\alpha_1) = I + E_{(m-1)',m} - E_{m',m-1}, \\ x_{\alpha_3}(1) &= I + \phi\mu(\alpha_3) = I + E_{m-2,m-1} - E_{(m-1)',(m-2)'}. \end{aligned}$$

The matrix $(n^{(1)}_{jk})$ of $n_1 = x_{\alpha_1}(1)x_{-\alpha_1}(-1)x_{\alpha_1}(1)$ has 1s on the diagonal and 0s elsewhere except

$$n^{(1)}_{jk} = \begin{cases} 0 & j = k = m-1,\ m,\ m' \text{ or } (m-1)' \\ -1 & (j,k) = (m-1, m') \text{ or } ((m-1)', m) \\ 1 & (j,k) = (m, (m-1)') \text{ or } (m', m-1). \end{cases}$$

For $i = 2, \ldots, m$, $n_i = (n^{(i)}_{jk})$ has 1s on the diagonal and 0's elsewhere except

$$n^{(i)}_{jk} = \begin{cases} 0 & j = k = m+1-i,\ m+2-i,\ (m+2-i)' \text{ or } (m+1-i)' \\ -1 & (j,k) = (m+2-i, m+1-i) \\ -1 & (j,k) = ((m+2-i)', (m+1-i)') \\ 1 & (j,k) = (m+1-i, m+2-i) \\ 1 & (j,k) = ((m+1-i)', (m+2-i)'). \end{cases}$$

The matrix (n_{jk}) of $n = n_1 n_2 \ldots n_m$ has nonzero entries

$$n_{jk} = \begin{cases} (-1)^m & (j,k) = ((m-1)', 1) \text{ or } (m-1, 1') \\ 1 & (j,k) = (m, m') \text{ or } (m', m) \\ 1 & (j,k) = (i, i+1) \text{ or } (i', (i+1)') \text{ for } i = 1, \ldots, m-2. \end{cases}$$

The matrix (h_{jk}) of $h_{\alpha_2,\xi}$ is the identity except that $h_{m-1,m-1} = h_{m',m'} = \xi$ and $h_{m,m} = h_{(m-1)',(m-1)'} = \xi^{-1}$.

It follows from Steinberg (1962, Theorem 3.13) that $\Omega^+(l,q)$ is generated by

$$\begin{cases} h_{\alpha_2,\xi} \text{ and } x_{-\alpha_1}(1)x_{\alpha_3}(1)n & \text{for } q>2 \\ x_{\alpha_1}(1)x_{\alpha_3}(1) \text{ and } n & \text{for } q=2. \end{cases}$$

4.2. TYPE D_m $(l=2m)$ m ODD $m>2$

It follows from Steinberg (1962, Theorem 3.11) that $\Omega^+(l,q)$ is generated by

$$\begin{cases} h_{\alpha_1,\xi} \text{ and } x_{\alpha_1}(1)n & \text{for } q>3, \\ x_{\alpha_1}(1) \text{ and } n & \text{for } q=2,3 \end{cases}$$

where x_{α_1} and n are as in Section 4.1 and the matrix (h_{jk}) of $h_{\alpha_1,\xi}$ is the identity except that $h_{m-1,m-1}=h_{m,m}=\xi$ and $h_{m',m'}=h_{(m-1)',(m-1)'}=\xi^{-1}$.

4.3. TYPE D_2 $(l=4)$

In this case the group is the central product $SL(2,q)\circ SL(2,q)$. Let p be the characteristic of $\mathbb{F}_q$. We choose elements x (of order p) and z (of order $q+1$) which generate $SL(2,q)$. (See p. 209 of Di Martino and Tamburini (1991) for a discussion of this point.) Since x and z have coprime order, $SL(2,q)\circ SL(2,q)$ is generated by (x,z) and (z,x).

To define z we take the underlying space for $SL(2,q)$ to be the additive group of the field $\mathbb{F}_{q^2}$. Then z is multiplication by $\xi=\zeta^{q-1}$, where ζ is a primitive element of $\mathbb{F}_{q^2}$. The element ξ has order $q+1$ and satisfies a quadratic equation over $\mathbb{F}_q$ whose roots are ξ and $\xi^q=\xi^{-1}$. Thus the minimal polynomial for ξ is X^2-aX+1, where $a=\xi+\xi^{-1}$ and the matrix of z with respect to the basis 1, ξ for $\mathbb{F}_{q^2}$ is $\begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$. Taking $x=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, it follows from Dickson's Theorem (Huppert, 1967; Hauptsatz theorem 8.27) that x and z generate $SL(2,q)$.

In order to represent the elements of $SL(2,q)\circ SL(2,q)$ as 4×4 matrices in $\Omega^+(4,q)$ we use the following construction. The group $SL(2,q)\times SL(2,q)$ acts on the space V of 2×2 matrices M over $\mathbb{F}_q$ such that $(A,B).M=AMB^t$. The determinant of M is a quadratic form of Witt index 2 preserved by this action and the image of $SL(2,q)\times SL(2,q)$ is isomorphic to $SL(2,q)\circ SL(2,q)$ and coincides with $\Omega^+(4,q)$. Using this repesentation $\Omega^+(4,q)$ is generated by the matrices

$$\begin{pmatrix} 0 & -1 & 0 & -1 \\ 1 & a & -1 & a \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & a \end{pmatrix}$$

and

$$\begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ -1 & -1 & a & -a \\ 0 & 1 & 0 & a \end{pmatrix}$$

corresponding to (x,z) and (z,x) respectively, with respect to the basis

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}.$$

4.4. TYPE D_1 $(l = 2)$

In this case $\Omega^+(2, q)$ is the derived group of the full orthogonal group. It is cyclic, of order $\frac{q-1}{2}$ when q is odd and $q - 1$ when q is even. In both cases it is generated by

$$\begin{pmatrix} \xi^2 & 0 \\ 0 & \xi^{-2} \end{pmatrix}.$$

4.5. TYPE B_m $(l = 2m + 1)$ $m \geq 2$

In this case $h = h_{\varepsilon_1+\varepsilon_m,\xi}$ is the identity except that $h_{1,1} = h_{m,m} = \xi$ and $h_{m',m'} = h_{1',1'} = \xi^{-1}$. The matrix $(n_{jk}^{(1)})$ of n_1 has 1s on the diagonal and 0s elsewhere except

$$n_{jk}^{(1)} = \begin{cases} 0 & j = k = m \text{ or } m' \\ -1 & (j,k) = (m, m'),\ (m+1, m+1) \text{ or } (m', m). \end{cases}$$

For $i = 2, \ldots, m$ the matrix $(n_{jk}^{(i)})$ of n_i has 1s on the diagonal and 0s elsewhere except

$$n_{jk}^{(i)} = \begin{cases} 0 & j = k = m+1-i,\ m+2-i,\ (m+2-i)' \text{ or } (m+1-i)' \\ -1 & (j,k) = (m+2-i, m+1-i) \\ -1 & (j,k) = ((m+2-i)', (m+1-i)') \\ 1 & (j,k) = (m+1-i, m+2-i) \\ 1 & (j,k) = ((m+1-i)', (m+2-i)'). \end{cases}$$

Then $n = n_1 n_2 \ldots n_m$ has nonzero entries

$$n_{jk} = \begin{cases} (-1)^m & (j,k) = (m', 1) \text{ or } (m, 1') \\ -1 & (j,k) = (m+1, m+1) \\ 1 & (j,k) = (i, i+1) \text{ or } (i', (i+1)') \text{ for } i = 1, \ldots, m-1. \end{cases}$$

For odd q it follows from Steinberg (1962; Theorem 3.11) that $\Omega^0(l, q)$ is generated by

$$\begin{cases} h \text{ and } x_{\alpha_1}(1)n & \text{for } q > 3 \\ x_{\alpha_1}(1) \text{ and } n & \text{for } q = 3 \end{cases}$$

where $x_{\alpha_1}(1) = I + \phi\mu(\alpha_1) + \frac{1}{2}\phi\mu(\alpha_1)^2 = I + 2E_{m,m+1} - E_{m+1,m'} - E_{m,m'}$.

For q even it follows from Steinberg (1962; Theorem 3.14) that $\Omega^0(l, q)$ is generated by

$$\begin{cases} h \text{ and } x_{\varepsilon_1-\varepsilon_m}(1)x_{-\alpha_1}(1)n & \text{for } q > 2 \\ x_{\varepsilon_1-\varepsilon_m}(1)x_{-\alpha_1}(1) \text{ and } n & \text{for } q = 2 \end{cases}$$

where $x_{\varepsilon_1-\varepsilon_m}(1) = I + E_{1,m} + E_{m',1'}$ and $x_{-\alpha_1}(1) = I + E_{m+1,m} + E_{m',m}$.

4.6. TYPE B_1

The group $\Omega^0(3, q)$ is isomorphic to $PSL(2, q)$ (Taylor, 1992, theorem 11.6). Consequently the Steinberg generators for $PSL(2, q)$ provide generators for $\Omega^0(3, q)$. The group is generated by

$$\begin{cases} nx \text{ and } h & \text{for } q > 3 \\ x \text{ and } n & \text{for } q = 2, 3 \end{cases}$$

where

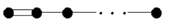
$$n = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \quad x = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ -1 & -2 & 1 \end{pmatrix} \quad \text{and} \quad h = \begin{pmatrix} \xi^{-2} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi^2 \end{pmatrix}.$$

5. Generators for $\Omega^-(l, q)$

The group $\Omega^-(l, q)$ of type ${}^2D_m$ can be considered as a subgroup of the group $G = \Omega^-(l, q^2)$ of type D_{m+1}. Thus $\Omega^-(l, q)$ is a group of $l \times l$ matrices where $l = 2m + 2$.

The Dynkin diagram for type D_{m+1} has an automorphism of order 2: swap roots α_1 and α_2, and leave the other fundamental roots fixed. This extends to an automorphism of the whole root system. Write $\overline{\alpha}$ for the image of α. For ${}^2D_m$ take the roots to be the orbits of this automorphism on the roots for type D_{m+1}. So the roots are

$$\{1, 2\}, \{3\}, \ldots, \{m\}.$$

The Dynkin diagram for ${}^2D_m$ is 

The field $\mathbb{F}_{q^2}$ has an automorphism of order 2 given by $t \to t^q$. Write $\overline{t}$ for the image of t. The map given by $x_\alpha(t) \to x_{\overline{\alpha}}(\overline{t})$ extends to an automorphism of G of order 2. The groups $\Omega^-(l, q)$ are defined in terms of fixed points of this map. See Carter (1972) for details.

Steinberg (1962) gives a pair of generators for $P\Omega^-(l, q)$ in terms of elements of $P\Omega^+(l, q^2)$; we use this to get generators for $\Omega^-(l, q)$ in terms of elements of $\Omega^+(l, q^2)$. However, to get matrices with entries in the correct field ($\mathbb{F}_q$) we follow Carter (1972, p. 271) and change the basis.

Let ν be a generator of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. In type D_{m+1} the quadratic form is $Q(\sum_{i=1}^{m+1}(a_i e_i + b_i f_i)) = \sum_{i=1}^{m+1} a_i b_i$. Take as a new basis $e_1, \ldots, e_m, w_1, w_2, f_m, \ldots, f_1$ where $e_{m+1} = w_1 + \nu w_2$ and $f_{m+1} = -w_1 - \overline{\nu} w_2$. With respect to this new basis the quadratic form is given by $Q'(\sum_{i=1}^{m-1}(a_i e_i + b_i f_i) + c w_1 + d w_2) = \sum_{i=1}^{m-1}(a_i b_i) + (d - \nu c)(d - \overline{\nu} c)/(\nu - \overline{\nu})^2$. Over the field $\mathbb{F}_q$ the quadratic form Q' has Witt index $m - 1$.

With this new basis we can now write down Steinberg's generators as $l \times l$ matrices with entries in $\mathbb{F}_q$. The change of basis matrix is

$$S^{-1} = \begin{pmatrix} I_m & & \\ & A & \\ & & I_m \end{pmatrix}$$

where

$$A = \begin{pmatrix} 1 & -1 \\ \nu & -\overline{\nu} \end{pmatrix}.$$

Define h to be

$$S^{-1} h_{1,\nu} h_{2,\overline{\nu}} S = \begin{pmatrix} I_{m-1} & & \\ & B & \\ & & I_{m-1} \end{pmatrix}$$

with

$$B = \begin{pmatrix} \nu\overline{\nu} & & & \\ & -1 & \nu^{-1} + \overline{\nu}^{-1} & \\ & -\nu - \overline{\nu} & 1 + \nu\overline{\nu}^{-1} + \nu^{-1}\overline{\nu} & \\ & & & \nu^{-1}\overline{\nu}^{-1} \end{pmatrix},$$

and x to be

$$S^{-1} x_{\alpha_1}(1) \overline{x_{\alpha_1}(1)} S = S^{-1} x_{\alpha_1}(1) x_{\alpha_2}(1) S = \begin{pmatrix} I_{m-1} & & \\ & C & \\ & & I_{m-1} \end{pmatrix}$$

with

$$C = \begin{pmatrix} 1 & 1 & 0 & 1 \\ & 1 & 0 & 2 \\ & & 1 & \nu + \overline{\nu} \\ & & & 1 \end{pmatrix}.$$

Now $n_R = x_R(1)x_{-R}(-1)x_R(1)$ (R is the new root $\{\alpha_1, \alpha_2\}$). With $n_3, \ldots, n_{m+1}$ as in type D_m (4.1) we calculate $n = n_R n_3 n_4 \ldots n_{m+1}$. The matrix (n_{jk}) of n has nonzero entries

$$n_{jk} = \begin{cases} (-1)^{m-1} & (j,k) = (m',1) \text{ or } (m,1') \\ -1 & (j,k) = (m+1,m+1) \\ -\nu - \overline{\nu} & (j,k) = ((m+1)',m+1) \\ 1 & (j,k) = ((m+1)',(m+1)') \\ 1 & (j,k) = (i,i+1) \text{ or } (i',(i+1)') \text{ for } i = 1,\ldots,m-1. \end{cases}$$

It follows from Steinberg that $\Omega^-(l,q)$ is generated by h and xn for all q.

6. Availability

The generators for $\Omega^\epsilon(l,q)$ described in this paper as well as generators for $SO^\epsilon(l,q)$ and $O^\epsilon(l,q)$ have been included in MAGMA V2.10.

References

Bosma, W., Cannon, J., Playoust, C. (1997). The MAGMA Algebra System I: the user language. *J. Symb. Comput.* **23**.

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

Celler, F., Leedham-Green, C.R. (1997). A non-constructive recognition algorithm for the special linear and other classical groups. *Groups and Computation II, vol. 28, DIMACS*, Providence, RI: Amer. Math. Soc.

Di Martino, L., Tamburini, M.C. (1991). 2-Generation of finite simple groups and some related topics. In A. Barlotti, E. W. Ellers, P. Plauman and K. Strambach (eds), *Generators and Relations in Groups and Geometries.* NATO ASI Series. Dordrecht: Kluwer Academic Publishers, pp 195–234.

Humphreys, J.E. (1972). *Introduction to Lie Algebras and Representation Theory.* New York: Springer Verlag.

Huppert, B. (1967). *Endliche Gruppen I.* Berlin: Springer-Verlag.

Ishibashi, H., Earnest, A.G. (1994a). Two generation of orthogonal groups over finite fields. *J. Algebra* **165**, 164–171.

Ishibashi, H., Earnest, A.G. (1994b). Erratum: Two generation of orthogonal groups over finite fields. *J. Algebra* **170**, 1035.

Niemeyer, A.C., Praeger, C.E. (1998). A recognition algorithm for classical groups over finite fields. *Proc. Lond. Math. Soc.* (in press).

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

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

Taylor, D.E. (1987). Pairs of generators for matrix groups I. *The Cayley Bulletin.*, **3** 76–85.

Taylor, D.E. (1992). *The Geometry of the Classical Groups.* Berlin: Heldermann Verlag.

Originally received 13 September 1996
Accepted 17 April 1997