April 16, 2015

GAUSSIAN ELIMINATION IN SYMPLECTIC AND SPLIT ORTHOGONAL GROUPS

SUSHIL BHUNIA, AYAN MAHALANOBIS AND ANUPAM SINGH

IISER Pune, Dr. Homi Bhabha Road, Pashan, Pune 411008, INDIA.

ABSTRACT. This paper studies an algorithm similar to that of Gaussian elimination in symplectic and split orthogonal groups. We discuss two applications of this algorithm in computational group theory. One computes the spinor norm and the other computes the double coset decomposition with respect to Siegel maximal parabolic subgroup.

1. INTRODUCTION

This paper is about Gaussian elimination in symplectic and split orthogonal groups in odd characteristic in their natural representations as matrices of size greater than 3. We consider a field to be of odd characteristic, if it is either of characteristic zero or a odd prime. Examples of such fields are \( \mathbb{C}, \mathbb{R}, \mathbb{Q} \) or finite fields \( \mathbb{F}_q \) of odd characteristics. Gaussian elimination (also known as row-column operations and Gauss-Jordan elimination) went through many versions at different periods of history. It appeared in print as chapter eight in a Chinese mathematical text called, “The nine chapters of the mathematical art”. It is believed, a part of that book was written as early as 150 BCE. Gauss made significant contributions to this algorithm along with many great mathematicians like John von Neumann and Alan Turing. This algorithm is referred to as Gaussian elimination as a tribute to a true legend in mathematics. For historical perspective of this algorithm we refer to a nice work by Grcar [7].

Gaussian elimination in general linear groups consist of two objects:

- **a**: Define elementary matrices.
- **b**: Define elementary row-column operations.

Using these two steps, one can reduce any element of the general linear group to a diagonal matrix with at most one non-identity element in the diagonal.

In the same spirit as above, we define elementary matrices and elementary operations for split orthogonal and symplectic groups over a field of odd characteristic (see Section 3). The main object in this paper is an algorithm very similar to Gaussian elimination in symplectic and split orthogonal groups. This algorithm yields to the following theorem and has two important applications.

**Theorem A.** Let \( k \) be a field of odd characteristic. Then the following holds:

1. Every element of the split orthogonal group \( O(d,k) \) can be written as a product of elementary matrices and a diagonal matrix. Furthermore, the diagonal matrix is of the form \( \text{diag}(1, \ldots, 1, \lambda, 1, \ldots, 1, \lambda^{-1}), \lambda \in k^\times \).
2. Every element of the symplectic group \( Sp(2l,k) \) can be written as a product of elementary matrices.

---

*E-mail address: sushilbhunia@gmail.com, ayan.mahalanobis@gmail.com, anupamk18@gmail.com.*

2010 Mathematics Subject Classification. 20H20, 68W30.

This work is supported by a SERB research grant.
This theorem has a surprising corollary. One can think of the $\lambda$ defined above for orthogonal groups as a map from the orthogonal group to $k^\times$. It follows that:

**Corollary B.** *In an orthogonal group, the image of $\lambda$ in $k^\times/k^\times_2$ is the spinor norm.*

Since the commutator subgroup of the orthogonal group is the kernel of the spinor norm restricted to special orthogonal group, the above corollary is a membership test for the commutator subgroup in the orthogonal group. In other words, an element $g$ in the special orthogonal group belongs to the commutator subgroup if and only if the $\lambda$ it produces in the Gaussian elimination algorithm is a square in the field, see Equation 2.3.

**Application 1:** Compute the spinor norm for orthogonal groups, see Section 5.2.

**Application 2:** Compute the double coset decomposition with respect to Siegel maximal parabolic subgroup, see Section 6.

The greatness of Gaussian elimination, and its true novelty, comes from the fact that it can turn a theoretical proof into an algorithm. We now have an efficient solution to the word problem in symplectic and orthogonal groups with the given set of generators. The need for such an algorithm was well articulated by Seress [14]:

The classical group can also be recognized constructively; the output is not only a proof that $G$ is a classical group, but every element of $G$ can be expressed effectively in terms of the given generating set.

This project is now known as the constructive group recognition project. This is one of the major forces in computational group theory and has evolved quite a bit [1, 6, 10, 11] over the last decade.

We describe the project very briefly, for more see [1, 11]. Let $\langle X \rangle = G \subseteq \text{GL}(d, q)$ be a classical group generated by a generating set $X$ presented in its natural representation. There are standard generators $S$ already defined for these groups. First part of the constructive group recognition algorithm is to write every element of $S$ as a word in $X$. This algorithm is probabilistic in nature and requires one to solve the discrete logarithm problem in the underlying field, [11, Theorem 1.1]. Once this is done, the next step is to write every element $g \in G$ as a word in $S$. Since every element in $S$ is a word in $X$, every element in $G$ is ultimately written as a word in $X$ and the constructive recognition is done.

Our algorithm fits in the last leg of this process. Instead of the standard generators, we use elementary matrices and we solve the word problem in $G$. Our algorithm is fast and straightforward to understand compared to the one used by the standard generators [1, Section 5]. Furthermore obvious applications, like an algorithm to find the spinor norm or an algorithm for the double coset decomposition suggests some naturalness in our algorithm.

In this paper we work with a fixed basis and the corresponding matrix of bilinear form denoted as $\beta$ (see Equations 2.1 & 2.2). A split orthogonal or symplectic group could have many conjugates in the general linear group which are obtained by choosing different basis for the bilinear form. We do not address the conjugacy problem in this paper, which could be important for certain problems in computational group theory. The bilinear form that we use and the generators that we define have its roots in the abstract root system of a semisimple Lie algebra and Chevalley groups defined by Chevalley and Steinberg [4, 15]. However we assume no knowledge of Lie theory or Chevalley groups in this paper.

2. ORTHOGONAL AND SYMPLECTIC GROUPS

We begin with a brief introduction of orthogonal and symplectic groups. We follow Carter [2], Taylor [16] and Grove [8] in our introduction. In this section, we fix some notations which will be used throughout this paper. We denote the transpose of a matrix $X$ by $^TX$. 


Let $V$ be a vector space of dimension $d$ over a field $k$ of odd characteristic. Let $\beta : V \times V \to k$ be a bilinear form. By fixing a basis of $V$ we can associate a matrix to $\beta$. We shall abuse the notation slightly and denote the matrix of the bilinear form by $\beta$ itself. Thus $\beta(x,y) = T_x \beta y$ where $x, y$ are column vectors. We will work with non-degenerate bilinear forms, which implies, $\det \beta \neq 0$. A symmetric or skew-symmetric bilinear form $\beta$ satisfies $\beta = T \beta$ or $\beta = -T \beta$ respectively.

**Definition 2.1** (Orthogonal Groups). A square matrix $X$ of size $d$ is called orthogonal if $T X \beta X = \beta$ where $\beta$ is symmetric. The set of orthogonal matrices form the orthogonal group.

In this paper, we deal with the split orthogonal group defined by one particular bilinear form defined in Equations 2.1 & 2.2. So any mention of orthogonal group means this one particular orthogonal group, unless stated otherwise.

**Definition 2.2** (Symplectic Group). A square matrix $X$ of size $d$ is called symplectic if $T X \beta X = \beta$ where $\beta$ is skew-symmetric. The set of symplectic matrices form the symplectic group.

In this paper, we deal with the symplectic group defined by the bilinear form defined by Equation 2.2. So any mention of symplectic group means this one particular symplectic group, unless stated otherwise. We write the dimension of $V$ as $d$ where $d = 2l + 1$ or $d = 2l$ and $l \geq 1$. In the case $\beta$ is symmetric we define the corresponding quadratic form $Q : V \to k$ by $Q(v) = \frac{1}{2} \beta(v,v)$.

Up to equivalence, there is an unique non-degenerate skew-symmetric bilinear form over $k$. Furthermore a skew-symmetric bilinear form exists only in even dimension. We fix a basis of $V$ as $\{ e_1, \ldots, e_l, e_{-1}, \ldots, e_{-l} \}$ so that the matrix $\beta$ is:

$$
\beta = \begin{pmatrix} 0 & I_l \\
-I_l & 0 \end{pmatrix}.
$$

The symplectic group with this $\beta$ is denoted as $\text{Sp}(2l,k)$.

Up to equivalence, there is a unique non-degenerate symmetric bilinear form of maximal Witt index over $k$. This is also called the split form. We fix a basis $\{ e_0, e_1, \ldots, e_l, e_{-1}, \ldots, e_{-l} \}$ for odd dimension and $\{ e_1, \ldots, e_l, e_{-1}, \ldots, e_{-l} \}$ for even dimension so that the matrix $\beta$ is:

$$
\beta = \begin{cases} 
\begin{pmatrix} 2 & 0 & 0 \\
0 & 0 & I_l \\
0 & I_l & 0 \end{pmatrix} & \text{when } d = 2l + 1 \\
\begin{pmatrix} 0 & I_l \\
I_l & 0 \end{pmatrix} & \text{when } d = 2l.
\end{cases}
$$

The orthogonal group corresponding to this form is a split orthogonal group. In this paper, we will simply call it the orthogonal group and this group will be denoted by $O(d,k)$. If we need to emphasize parity of the dimension, we will write $O(2l+1,k)$ or $O(2l,k)$. We denote by $\Omega(d,k)$ the commutator subgroup of the orthogonal group $O(d,k)$ which is equal to the commutator subgroup of $SO(d,k)$. There is a well known exact sequence

$$
1 \longrightarrow \Omega(d,k) \longrightarrow SO(d,k) \xrightarrow{\Theta} k^\times / k^{\times 2} \longrightarrow 1
$$

where $\Theta$ is the spinor norm. The spinor norm is defined as $\Theta(g) = \prod_{i=1}^{m} Q(v_i)$ where $g = \rho_{v_1} \cdots \rho_{v_m}$ is written as a product of reflections. Since the group $SO(d,k)$ is of index 2 in $O(d,k)$, we fix a generator for the quotient as $w_l = I - e_{l,1} - e_{-l,-1} - e_{1,-l} - e_{-1,l}$.
3. Elementary Matrices and Elementary Operations

In what follows, the scalar $t$ varies over the field $k$ and $1 \leq i, j \leq l$. Furthermore, $l \geq 2$ which means $d \geq 4$. We define $te_{i,j}$ as the matrix unit with $t$ in the $(i, j)$ position and zero everywhere else. We use $e_{i,j}$ to denote $1e_{i,j}$. We often use the well known identity $e_{i,j}e_{k,l} = \delta_{j,k}e_{i,l}$ where $\delta_{i,j}$ is the Kronecker delta.

3.1. Elementary Matrices for $O(2l,k)$. We index rows by $1, 2, \ldots, l, -1, -2, \ldots, -l$. The elementary matrices are defined as follows:

$$x_{i,j}(t) = I + t(e_{i,j} - e_{.-i},.) \quad \text{for} \quad i \neq j,$$

$$x_{i,-j}(t) = I + t(e_{i,-j} - e_{-.i},.) \quad \text{for} \quad i < j,$$

$$x_{-i,j}(t) = I + t(e_{-i,j} - e_{-.j},i) \quad \text{for} \quad i < j,$$

$$w_l = I - e_{l,l} - e_{-l,-l} - e_{l,-l} - e_{-l,l}$$

and in matrix format

E1: \[
\begin{pmatrix} R & 0 \\
0 & T_R^{-1} \end{pmatrix}
\]
where $R = I + te_{i,j}; i \neq j$

E2: \[
\begin{pmatrix} I & R \\
0 & I \end{pmatrix}
\]
where $R$ is $t(e_{i,j} - e_{j,i})$ for $i < j$

E3: \[
\begin{pmatrix} I & 0 \\
R & I \end{pmatrix}
\]
where $R$ is $t(e_{i,j} - e_{j,i})$ for $i < j$.

The row and column operations:

$$ER1:\ \begin{pmatrix} R & 0 \\
0 & T_R^{-1} \end{pmatrix} \begin{pmatrix} A & B \\
C & D \end{pmatrix} = \begin{pmatrix} RA & RB \\
T_R^{-1}C & T_R^{-1}D \end{pmatrix}$$

$$EC1:\ \begin{pmatrix} A & B \\
C & D \end{pmatrix} \begin{pmatrix} R & 0 \\
0 & T_R^{-1} \end{pmatrix} = \begin{pmatrix} AR & B T_R^{-1} \\
C R & D T_R^{-1} \end{pmatrix}$$

$$ER2:\ \begin{pmatrix} I & R \\
0 & I \end{pmatrix} \begin{pmatrix} A & B \\
C & D \end{pmatrix} = \begin{pmatrix} A + RC & B + RD \\
C & D \end{pmatrix}$$

$$EC2:\ \begin{pmatrix} A & B \\
C & D \end{pmatrix} \begin{pmatrix} I & R \\
0 & I \end{pmatrix} = \begin{pmatrix} A & AR + B \\
C & CR + D \end{pmatrix}$$

$$ER3:\ \begin{pmatrix} I & 0 \\
R & I \end{pmatrix} \begin{pmatrix} A & B \\
C & D \end{pmatrix} = \begin{pmatrix} A & B \\
RA + C & RB + D \end{pmatrix}$$

$$EC3:\ \begin{pmatrix} A & B \\
C & D \end{pmatrix} \begin{pmatrix} I & 0 \\
R & I \end{pmatrix} = \begin{pmatrix} A & BR \\
C + DR & D \end{pmatrix}$$

3.2. Elementary Matrices for $O(2l+1,k)$. We index rows by $0, 1, \ldots, l, -1, \ldots, -l$. The elementary matrices are:

$$x_{i,j}(t) = I + t(e_{i,j} - e_{.-i},.) \quad \text{for} \quad i \neq j,$$

$$x_{i,-j}(t) = I + t(e_{i,-j} - e_{-.i},i) \quad \text{for} \quad i < j,$$

$$x_{-i,j}(t) = I + t(e_{-i,j} - e_{-.j},i) \quad \text{for} \quad i < j,$$

$$x_{i,0}(t) = I + t(2e_{i,0} - e_{0,-i}) - t^2e_{i,-i},$$

$$x_{0,i}(t) = I + t(-2e_{-i,0} + e_{0,i}) - t^2e_{-i,i}.$$

$$w_l = I - e_{l,l} - e_{-l,-l} - e_{l,-l} - e_{-l,l}.$$
E1: \[
\begin{pmatrix}
1 & 0 & 0 \\
0 & R & 0 \\
0 & 0 & tR^{-1}
\end{pmatrix}
\] where \( R = I + te_{i,j}; \ i \neq j \).

E2: \[
\begin{pmatrix}
0 & I & R \\
0 & 0 & I \\
1 & 0 & 0
\end{pmatrix}
\] where \( R = t(e_{i,j} - e_{j,i}); \ i < j \).

E3: \[
\begin{pmatrix}
0 & I & 0 \\
0 & R & I \\
1 & 0 & 0
\end{pmatrix}
\] where \( R = t(e_{i,j} - e_{j,i}); \ i < j \).

E4a: \[
\begin{pmatrix}
1 & 0 & R \\
0 & I & 0 \\
-2R & I & -TRR
\end{pmatrix}
\] where \( R = te_i \)

E4b: \[
\begin{pmatrix}
1 & R & 0 \\
0 & I & 0 \\
-2R & -TRR & I
\end{pmatrix}
\] where \( R = te_i \)

Here \( e_i \) is the row vector with 1 at \( i \)th place and zero elsewhere.

3.3. **Elementary operations for \( O(2l+1) \).** Let \( g = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \) be a \((2l+1) \times (2l+1)\) matrix where \( A, B, C, D \) are \( l \times l \) matrices. The matrices \( X = (X_1, X_2, \ldots, X_l), Y = (Y_1, Y_2, \ldots, Y_l), E = T(E_1, E_2, \ldots, E_l) \) and \( F = T(F_1, F_2, \ldots, F_l) \). Let \( \alpha \in k \). Let us note the effect of multiplication by elementary matrices from above:

\[ ER1: \begin{pmatrix} 1 & 0 & 0 \\ 0 & R & 0 \\ 0 & 0 & tR^{-1} \end{pmatrix} \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ RE & RA & RB \\ T^{-1} & T^{-1}C & T^{-1}D \end{pmatrix} \]

\[ EC1: \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & R & 0 \\ 0 & 0 & tR^{-1} \end{pmatrix} = \begin{pmatrix} \alpha & XR & YTR^{-1} \\ E & AR & BTR^{-1} \\ F & CR & DTR^{-1} \end{pmatrix} \]

\[ ER2: \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & R \\ 0 & 0 & I \end{pmatrix} \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ E+RF & A+RC & B+RD \\ F & C & D \end{pmatrix} \]

\[ EC2: \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & R \\ 0 & 0 & I \end{pmatrix} = \begin{pmatrix} \alpha & XR+Y \\ E & A & AR+B \\ F & C & CR+D \end{pmatrix} \]

\[ ER3: \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ 0 & R & I \end{pmatrix} \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ RE+F & RA+C & RB+D \end{pmatrix} \]

\[ EC3: \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ 0 & R & I \end{pmatrix} = \begin{pmatrix} \alpha & X+YR & Y \\ E & A & BR+B \\ F & C+DR & D \end{pmatrix} \]

For E4 we only write the equations that we need later.

- Let the matrix \( g \) has \( C = \text{diag}(d_1, \ldots, d_l) \).

\[ ER4: \left((I + te_{0,-i} - 2te_{i,0} - t^2e_{i,-i})g\right)_{i,i} = X_i + td_i \]
There are three kinds of elementary matrices.

- Let the matrix \( g = \text{diag}(d_1, \ldots, d_l) \).

\[
ER4 :\quad [(I + te_{0,i} - 2te_{i,0} - t^2e_{i,-i})g]_{0,i} = X_i + td_i
\]

\[
EC4 :\quad [g(I + te_{0,i} - 2te_{i,0} - t^2e_{i,-i})]_{i,0} = E_i - 2td_i.
\]

3.4. **Elementary Matrices for \( \text{Sp}(2l, k) \).**

Let \( x_{i,j}(t) = I + t(e_{i,j} - e_{-j,-i}) \) for \( i \neq j \),

\[x_{i,-j}(t) = I + t(e_{i,-j} + e_{j,-i}) \text{ for } i < j,\]

\[x_{-i,j}(t) = I + t(e_{-i,j} + e_{-j,i}) \text{ for } i < j,\]

\[x_{i,-i}(t) = I + te_{i,-i},\]

\[x_{-i,i}(t) = I + te_{-i,i}.\]

There are three kinds of elementary matrices.

- **E1:** \(
\begin{pmatrix}
R & 0 \\
0 & T_R^{-1}
\end{pmatrix}
\) where \( R = I + te_{i,j}; i \neq j \).

- **E2:** \(
\begin{pmatrix}
I & R \\
0 & I
\end{pmatrix}
\) where \( R \) is either \( t(e_{i,j} + e_{j,i}); i < j \) or \( te_{i,i}. \)

- **E3:** \(
\begin{pmatrix}
I & 0 \\
R & I
\end{pmatrix}
\) where \( R \) is either \( t(e_{i,j} + e_{j,i}); i < j \) or \( te_{i,i}. \)

3.5. **Elementary Operations for \( \text{Sp}(2l, k) \).** Let \( g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \) be a \( 2l \times 2l \) matrix written in block form of size \( l \times l \). Then the row and column operations are as follows:

- **ER1:** \(
\begin{pmatrix}
R & 0 \\
0 & T_R^{-1}
\end{pmatrix}
\begin{pmatrix}
A & B \\
C & D
\end{pmatrix} = \begin{pmatrix}
RA & RB \\
T_R^{-1}C & T_R^{-1}D
\end{pmatrix}
\)

- **EC1:** \(
\begin{pmatrix}
A & B \\
C & D
\end{pmatrix}
\begin{pmatrix}
R & 0 \\
0 & T_R^{-1}
\end{pmatrix} = \begin{pmatrix}
AR & B^TR^{-1} \\
C & D^TR^{-1}
\end{pmatrix}
\)

- **ER2:** \(
\begin{pmatrix}
I & R \\
0 & I
\end{pmatrix}
\begin{pmatrix}
A & B \\
C & D
\end{pmatrix} = \begin{pmatrix}
A + RC & B + RD \\
C & D
\end{pmatrix}
\)

- **EC2:** \(
\begin{pmatrix}
A & B \\
C & D
\end{pmatrix}
\begin{pmatrix}
I & R \\
0 & I
\end{pmatrix} = \begin{pmatrix}
A & AR + B \\
C & CR + D
\end{pmatrix}
\)

- **ER3:** \(
\begin{pmatrix}
I & 0 \\
R & I
\end{pmatrix}
\begin{pmatrix}
A & B \\
C & D
\end{pmatrix} = \begin{pmatrix}
A & B \\
RA + C & RB + D
\end{pmatrix}
\)

- **EC3:** \(
\begin{pmatrix}
A & B \\
C & D
\end{pmatrix}
\begin{pmatrix}
I & 0 \\
R & I
\end{pmatrix} = \begin{pmatrix}
A + BR & B \\
C + DR & D
\end{pmatrix}
\)

**Remark:** In the case of orthogonal group we note that the left multiplication by \( w_j \) interchanges \( l^\text{th} \) row with \( -l^\text{th} \) row while multiplying both by \(-1\).
4. Gaussian Elimination in Orthogonal and Symplectic Groups

Recall the field $k$ is of odd characteristic. Cohen, Murray and Taylor [5] proposed a generalized row-column operations, using a representation of Chevalley groups. The key idea there was to bring down an element to a maximal parabolic subgroup and repeat the process inductively. The emphasis there was to represent generators as symbols so that it takes less memory to store. Here we use the natural matrix representation of these groups. Thus our study needs no background in Chevalley groups and is easy to understand and implement.

4.1. Gaussian Elimination for $Sp(2l,k)$ and $O(2l,k)$. The algorithm is as follows.

Step 1: **Input**: A matrix $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ which belongs to $Sp(2l,k)$ or $O(2l,k)$.

**Output**: The matrix $g_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ is one of the following kind:

a: The matrix $C_1$ is a diagonal matrix $\text{diag}(1,\ldots,1,\lambda)$ with $\lambda \neq 0$ and $A_1$ is $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & a_{22} \end{pmatrix}$ where $A_{11}$ is symmetric when $g$ is in $Sp(2l,k)$ and skew-symmetric when $g$ is in $O(2l,k)$ and is of size $l - 1$. Furthermore, $A_{12} = \lambda^T A_{21}$ when $g$ is in $Sp(2l,k)$ and $A_{12} = -\lambda^T A_{21}$, $a_{22} = 0$ when $g$ is in $O(2l,k)$.

b: The matrix $C_1$ is a diagonal matrix $\text{diag}(1,\ldots,1,0,\ldots,0)$ with number of 1s equal to $m$ and $A_1$ is of the form $\begin{pmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{pmatrix}$ where $A_{11}$ is an $m \times m$ symmetric matrix when $g$ is in $Sp(2l,k)$ and skew-symmetric when $g$ is in $O(2l,k)$.

**Justification**: Observe the effect of ER1 and EC1 on the block $C$. This amounts to Gaussian elimination on a $l \times l$ matrix. Thus we can reduce $C$ to a diagonal matrix and Corollary 4.2 makes sure that $A$ has required form.

Step 2: **Input**: matrix $g_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$.

**Output**: matrix $g_1 = \begin{pmatrix} A_2 & B_2 \\ 0 & T_{A_2^{-1}} \end{pmatrix}$; $A_2$ is a diagonal matrix $\text{diag}(1,\ldots,1,\lambda)$.

**Justification**: Observe the effect of ER2. It changes $A_1$ by $A_1 + RC_1$. Using Lemma 4.5 we can make the matrix $A_1$ the zero matrix in the first case and $A_{11}$ the zero matrix in the second case. After that we make use of Lemma 4.6 to interchange the rows so that we get zero matrix at the place of $C_1$. If required use ER1 and EC1 to make $A_1$ a diagonal matrix. The Lemma 4.4 ensures that $D_1$ becomes $T_{A_2^{-1}}$.

Step 3: **Input**: matrix $g_2 = \begin{pmatrix} A_2 & B_2 \\ 0 & T_{A_2^{-1}} \end{pmatrix}$; $A_2$ is a diagonal matrix $\text{diag}(1,\ldots,1,\lambda)$.

**Output**: Matrix $g_3 = \begin{pmatrix} A_2 & 0 \\ 0 & T_{A_2^{-1}} \end{pmatrix}$; $A_2$ is diagonal matrix $\text{diag}(1,\ldots,1,\lambda)$.

**Justification**: Using Corollary 4.3 we see that the matrix $B_2$ has certain form. We can use ER2 to make the matrix $B_2$ a zero matrix because of Lemma 4.5.

The algorithm terminates here for $O(2l,k)$. However for $Sp(2l,k)$ there is one more step.

Step 4: **Input**: matrix $g_3 = \text{diag}(1,\ldots,1,\lambda,1,\ldots,1,\lambda^{-1})$.

**Output**: Identity matrix

**Justification**: This can be written as a product of elementary matrices by the first part of Lemma 4.7.

4.2. Gaussian Elimination for $O(2l+1,k)$. An overview of the algorithm is as follows:
Step 1: **Input:** matrix $g = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix}$ which belongs to $O(2l + 1, k)$;

**Output:** matrix $g_1 = \begin{pmatrix} \alpha & X_1 & Y_1 \\ E_1 & A_1 & B_1 \\ F_1 & C_1 & D_1 \end{pmatrix}$ of one of the following kind:

- a: The matrix $C_1$ is a diagonal matrix $\text{diag}(1, \ldots, 1, \lambda)$ with $\lambda \neq 0$.
- b: The matrix $C_1$ is a diagonal matrix $\text{diag}(1, \ldots, 1, 0, \ldots, 0)$ with number of 1s equal to $m$ and $m < l$.

**Justification:** Using ER1 and EC1 we do the classical Gaussian elimination on a $l \times l$ matrix $C$.

Step 2: **Input:** matrix $g_1 = \begin{pmatrix} \alpha & X_1 & Y_1 \\ E_1 & A_1 & B_1 \\ F_1 & C_1 & D_1 \end{pmatrix}$;

**Output:** matrix $g_2 = \begin{pmatrix} \alpha_2 & X_2 & Y_2 \\ E_2 & A_2 & B_2 \\ F_2 & C_2 & D_2 \end{pmatrix}$ of one of the following kind:

- a: The matrix $C_2$ is $\text{diag}(1, 1, \ldots, 1, \lambda)$ with $\lambda \neq 0$, $X_2 = 0 = F_2$ and $A_2$ is of the form $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & 0 \end{pmatrix}$ where $A_{11}$ is skew-symmetric of size $l - 1$ and $A_{12} = -\lambda^TA_{21}$.
- b: The matrix $C_2$ is $\text{diag}(1, \ldots, 1, 0, \ldots, 0)$ with number of 1s equal to $m$; $X_2$ and $F_2$ have first $m$ entries 0, and $A_2$ is of the form $\begin{pmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{pmatrix}$ where $A_{11}$ is an $m \times m$ skew-symmetric.

**Justification:** Once we have $C_1$ in diagonal form we use ER4 and EC4 to change $X_1$ and $F_1$ in the required form. Then Lemma 4.8 makes sure that $A_1$ has required form.

Step 3: **Input:** matrix $g_2 = \begin{pmatrix} \alpha_2 & X_2 & Y_2 \\ E_2 & A_2 & B_2 \\ F_2 & C_2 & D_2 \end{pmatrix}$;

**Output:**

- a: matrix $g_3 = \begin{pmatrix} \alpha_3 & 0 & Y_3 \\ E_3 & 0 & B_3 \\ 0 & C_3 & D_3 \end{pmatrix}$ where $C_3$ is $\text{diag}(1, 1, \ldots, 1, \lambda)$.
- b: matrix $g_3 = \begin{pmatrix} \alpha_3 & X_3 & Y_3 \\ E_3 & A_3 & B_3 \\ F_3 & C_3 & D_3 \end{pmatrix}$ where $C_3$ is $\text{diag}(1, \ldots, 1, 0, \ldots, 0)$ with number of 1s equal to $m$; $X_3$ and $F_3$ have first $m$ entries 0, and $A_3$ is of the form $\begin{pmatrix} 0 & 0 \\ A_{21} & A_{22} \end{pmatrix}$.

**Justification:** Observe the effect of ER2 and the Lemma 4.5 ensures the required form.

Step 4: **Input:** $g_3 = \begin{pmatrix} \alpha_3 & X_3 & Y_3 \\ E_3 & A_3 & B_3 \\ F_3 & C_3 & D_3 \end{pmatrix}$;

**Output:** $g_4 = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & A_4 & B_4 \\ 0 & 0 & A_4^{-1} \end{pmatrix}$ with $A_4$ diagonal matrix $\text{diag}(1, \ldots, 1, \lambda)$.

**Justification:** In the first case, interchange rows $i$ and $-i$ for all $1 \leq i \leq l$. Now the matrix is in the form so that we can apply Lemma 4.10 and get the required result. In the second case we interchange $i$ with $-i$ for $1 \leq i \leq m$. This will make $C_3 = 0$. Then
if needed we use ER1 and EC1 on $A_3$ to make it diagonal. The Lemma 4.9 ensures that $A_3$ has full rank. Further we can use ER4 and EC4 to make $X_3 = 0$ and $E_3 = 0$. The Lemma 4.10 gives the required form.

Step 5: Input: $g_4 = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & A_4 & B_4 \\ 0 & 0 & A_4^{-1} \end{pmatrix}$ with $A_4 = \text{diag}(1, \ldots, 1, \lambda)$.

Output: $g_5 = \text{diag}(1, 1, \ldots, 1, \lambda, 1, \ldots, 1, \lambda^{-1})$.

Justification: Lemma 4.10 ensures that $B_4$ is of certain kind. We can use ER2 to make $B_4 = 0$. If need we use Lemma 4.6 to make the first diagonal entry 1.

Proof of the Theorem A. (a) Let $g \in O(d, k)$. Using the above algorithm we can reduce $g$ to a diagonal matrix.

(b) If $g \in \text{Sp}(2l, k)$ using above algorithm we can reduce $g$ to the identity. Thus $g$ is a product of elementary matrices. $

4.3. Time-complexity of the above algorithm. We establish that the worst case time-complexity of the above algorithm is $\mathcal{O}(l^3)$.

In Step 1, we make $C$ a diagonal matrix by row-column operations. That has complexity $\mathcal{O}(l^3)$.

In Step 2, $A_1 + RC_1$ is two field multiplications and two additions. In the worst case, it has to be done $l^2$ times and so the complexity is $\mathcal{O}(l^2)$.

Step 3 is similar to Step 2 above and has complexity $\mathcal{O}(l^2)$.

Step 4 has only a few steps that is independent of $l$.

Then clearly, the time-complexity of our algorithm is $\mathcal{O}(l^3)$.

4.4. Lemmas used in the justification of the Gaussian elimination. To justify the steps of Gaussian algorithm we need several lemmas. Some of these might be well known to experts but we include them here for the convenience of the reader.

Lemma 4.1. Let $Y = \text{diag}(1, \ldots, 1, \lambda, \ldots, \lambda)$ be of size $l$ with number of 1s equal to $m < l$. Let $X$ be a matrix of size $2l$ such that $YX$ is symmetric (skew-symmetric) then $X$ is of the form

\[
\begin{pmatrix}
X_{11} & \lambda^T X_{21} \\
X_{21} & X_{22}
\end{pmatrix}
\]

where $X_{11}$ is symmetric (skew symmetric) and $X_{12} = \lambda^T X_{21}$ ($X_{12} = -\lambda^T X_{21}$).

Furthermore, if $\lambda \neq 0$ then $X_{22}$ is symmetric (skew-symmetric).

Proof. We observe that the matrix $YX = \begin{pmatrix} X_{11} & X_{12} \\ \lambda X_{21} & \lambda X_{22} \end{pmatrix}$. The condition that $YX$ is symmetric implies $X_{11}$ (and $X_{22}$ if $\lambda \neq 0$) is symmetric and $X_{12} = \lambda^T X_{21}$.

Corollary 4.2. Let $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be either in $\text{Sp}(2l, k)$ or $O(2l, k)$.

(1) If $C$ is a diagonal matrix $\text{diag}(1, \ldots, 1, 0, \ldots, 0)$ with number of 1s equal to $m (< l)$ then the matrix $A$ is $\begin{pmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{pmatrix}$ where $A_{11}$ is an $m \times m$ symmetric if $g$ is symplectic and is skew-symmetric if $g$ is orthogonal.

(2) If $C$ is a diagonal matrix $\text{diag}(1, \ldots, 1, \lambda)$ then the matrix $A$ is $\begin{pmatrix} A_{11} & \lambda^T A_{21} \\ A_{21} & A_{22} \end{pmatrix}$ where $A_{11}$ is an $(l-1) \times (l-1)$ symmetric if $g$ is symplectic and $A_{11}$ is skew-symmetric with $A_{22} = 0$ if $g$ is orthogonal.
Proof. We use the condition that \( g \) satisfies \( Tgβg = β \) and get \( CA \) is symmetric (using \( C = TC \) as \( C \) is diagonal) when \( g \) is symplectic and skew-symmetric when \( g \) is orthogonal. The Lemma 4.1 gives the required form for \( A \).

Corollary 4.3. Let \( g = \begin{pmatrix} A & B \\ 0 & A^{-1} \end{pmatrix} \) where \( A = \text{diag}(1, \ldots, 1, \lambda) \) be an element of either \( \text{Sp}(2l, k) \) or \( \text{O}(2l, k) \) then the matrix \( B \) is of the form \( \begin{pmatrix} B_{11} & \pm \lambda^{-1} B_{21} \\ B_{21} & B_{22} \end{pmatrix} \) where \( B_{11} \) is a symmetric matrix of size \( l \) if \( g \) is symplectic and is skew-symmetric along with \( B_{22} = 0 \) if \( g \) is orthogonal.

Proof. Yet again, we use the condition that \( g \) satisfies \( Tgβg = β \) and \( A = TA \) to get \( A^{-1}B \) is symmetric if \( g \) is symplectic and is skew-symmetric if \( g \) is orthogonal. Then Lemma 4.1 gives the required form for \( B \).

Lemma 4.4. Let \( g = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \) \( \in \text{GL}(2l, k) \). Then,

1. the element \( g \) belongs to \( \text{Sp}(2l, k) \) if and only if \( D = T \text{A}^{-1} \) and \( BA = A^{-1}B \) and
2. the element \( g \) belongs to \( \text{O}(2l, k) \) if and only if \( D = T \text{A}^{-1} \) and \( BA = -A^{-1}B \).

Proof. This follows by simple computation using \( Tgβg = β \).

Lemma 4.5. Let \( Y = \text{diag}(1, \ldots, 1, \lambda) \) be of size \( l \) where \( \lambda \neq 0 \) and \( X = (x_{ij}) \) be a matrix such that \( XY \) is symmetric (skew-symmetric). Then \( X = (R_{l} + R_{l} + \ldots)Y \) where each \( R_{m} \) is of the form \( t(e_{i,j} + e_{j,i}) \) for some \( i < j \) or of the form \( te_{i,i} \) for some \( i \) (in the case of skew-symmetric each \( R_{m} \) is of the form \( t(e_{i,j} - e_{j,i}) \) for some \( i < j \)).

Proof. Since \( XY \) is symmetric, the matrix \( X \) is of the form \( \begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix} \) where \( X_{11} \) is symmetric and \( X_{21} \) is a row of size \( l \) and \( X_{12} = \lambda X_{21} \). Clearly any such matrix is sum of the matrices of the form \( R_{m}Y \). A similar calculation proves the result for the skew-symmetric case.

We need certain Weyl group elements which can be used for interchanging rows. We use a formula \( w_{r} = x_{r}(1)x_{r}(-1)x_{r}(1) \) from the theory of Chevalley groups [2, Lemma 6.4.4] and construct elements \( w_{i,j} \) and \( w_{i,-j} \). In our algorithm, we need elements which interchanges \( i \)th row with \(-j\)th row for any \( i \). The element \( w_{i, -i} \) that we create when multiplied to a matrix \( g \) interchanges its rows while simultaneously multiplying some rows by \(-1\). However that does no harm to our algorithm.

Lemma 4.6. For \( 1 \leq i \leq l \),

1. the element \( w_{i,-i} = I + e_{i,-i} - e_{i,i} - e_{-i,i} - e_{-i,-i} \in \text{Sp}(2l, k) \) is a product of elementary matrices.
2. The element \( w_{i,-i} = I - e_{i,-i} - e_{i,i} - e_{-i,i} - e_{-i,-i} \in \text{O}(d, k) \) is a product of elementary matrices.

Proof. For the symplectic group \( \text{Sp}(2l, k) \) we have \( w_{i,-i} = x_{i,-i}(1)x_{i,-i}(1) \).

For the orthogonal group \( \text{O}(2l, k) \) we inductively produce these elements. First we get \( w_{i,j} = (I + e_{i,-j} - e_{j,i})/(I + e_{i,j} - e_{j,i}) = I - e_{i,j} - e_{j,i} - e_{i,-j} - e_{-i,j} + e_{i,-j} - e_j,-i + e_{j,i} - e_{-i,j} \) and \( w_{i,j} = I - e_{i,j} - e_{j,i} + e_{i,j} + e_{j,i} - e_{i,-j} - e_{-i,j} + e_{i,-j} - e_{-i,j} \). Now we set \( w_{i,-i} = w_{i} \). Then compute \( w_{l, (-1)} = w_{l,(-1)}w_{l,(-1)} = I - e_{l,(-1)} = -e_{(-1, l)} \).

Lemma 4.7. (1) In the case of \( \text{Sp}(2l, k) \), the element \( \text{diag}(1, \ldots, 1, 1, \ldots, 1, \lambda^{-1}) \) is a product of elementary matrices.
(2) In the case of $O(2l+1,k)$ the diagonal element $\text{diag}(-1,1,\ldots,1)$ is a product of elementary matrices.

\textbf{Proof.} In the case of $\text{Sp}(2l,k)$, we compute $w_{l,-l}(t) = (I + t\epsilon_{l,-l})(I - t^{-1}\epsilon_{l,l})(I + t\epsilon_{l,-l}) = I - \epsilon_{l,l} - \epsilon_{-l,-l} + t\epsilon_{l,-l} - t^{-1}\epsilon_{l,l}$ and then compute $h_l(\lambda) = w_{l,-l}(\lambda)w_{l,-l}(-1)$ which is the required element.

In the case of $O(2l+1,k)$ we compute $w_{l,0} = x_{l,0}(1)x_{0,l}(-1)x_{l,0}(1) = I - \epsilon_{l,-l} - \epsilon_{-l,l} - \epsilon_{l,l} - 2\epsilon_{0,0} - \epsilon_{l,-l}$ and multiply it with $w_l$ to get the required form.

\textbf{Remark :} In the case of $O(2l,k)$, the element $\text{diag}(1,\ldots,1\lambda^2,1,\ldots,1,\lambda^{-2})$ and in the case of $O(2l+1,k)$ the element $\text{diag}(1,\ldots,1\lambda^2,1,\ldots,1,\lambda^{-2})$ is a product of elementary matrices.

\textbf{Lemma 4.8.} Let $g = \begin{pmatrix} \alpha & X & * \\ * & A & * \\ * & C & * \end{pmatrix}$ be in $O(2l+1,k)$.

1. If $C = \text{diag}(1,\ldots,1,\lambda)$ and $X = 0$ then $A$ is of the form $\begin{pmatrix} A_{11} & -\lambda^T A_{21} \\ A_{21} & 0 \end{pmatrix}$ with $A_{11}$ skew-symmetric.
2. If $C = \text{diag}(1,\ldots,1,0,\ldots,0)$ with number of 1s equal $m < l$ and $X$ has first $m$ entries 0 then $A$ is of the form $\begin{pmatrix} A_{11} & 0 \\ * & * \end{pmatrix}$ with $A_{11}$ skew-symmetric.

\textbf{Proof.} We use the equation $T g \beta g = \beta$ and get $2TXX = -(CA + TAC)$. In the first case $X = 0$, so use \ref{4.2} to get the required form for $A$. In the second case, we note that $TXX$ has top-left block 0 and get the required form.

\textbf{Lemma 4.9.} Let $g = \begin{pmatrix} \alpha & X & Y \\ * & A & * \\ * & 0 & D \end{pmatrix}$ be in $O(2l+1,k)$ then $X = 0$ and $D = TA^{-1}$.

\textbf{Proof.} We compute $T g \beta g = \beta$ and get $2TXX = 0$ and $2TXY + TAD = I$. This gives the required result.

\textbf{Lemma 4.10.} Let $g = \begin{pmatrix} \alpha & 0 & Y \\ 0 & A & B \\ F & 0 & D \end{pmatrix}$, with $A$ an invertible diagonal matrix. Then, $g \in O(2l+1,k)$ if and only if $\alpha^2 = 1, F = 0 = Y, D = A^{-1}$ and $TDB + TBD = 0$.

\textbf{Proof.}

\begin{equation*}
T g \beta g = \begin{pmatrix}
\alpha & 0 & T_F \\
0 & T_A & 0 \\
T_Y & T_B & T_D
\end{pmatrix}
\begin{pmatrix}
2 & 0 & 0 \\
0 & 0 & I \\
0 & I & 0
\end{pmatrix}
\begin{pmatrix}
\alpha & 0 & Y \\
0 & A & B \\
F & 0 & D
\end{pmatrix}
\end{equation*}

Equating this with $\beta$ gives us the required result.
5. Computing Spinor Norm for Orthogonal Groups

In this section, we show how we can use Gaussian elimination to compute spinor norm for orthogonal groups. The classical way to define spinor norm is via Clifford algebras [8, Chapters 8 & 9]. Spinor norm is a group homomorphism \( \Theta : O(d, k) \to k^\times / k^{\times 2} \), restriction of which to \( SO(d, k) \) gives \( \Omega(d, k) \) as kernel. However, in practice, it is difficult to use that definition to compute the spinor norm. Wall [17], Zassenhaus [18] and Hahn [9] developed a theory to compute the spinor norm. For our exposition, we follow [16, Chapter 11].

Let \( g \) be an element of the orthogonal group. Consider \( g = I - g \) and \( V_g = \tilde{g}(V) \) and \( V^g = ker(\tilde{g}) \). Using \( \beta \) we define Wall’s bilinear form \([ \ , \ ]_g\) on \( V_g \) as follows:
\[
[u, v]_g = \beta(u, y), \text{ where, } v = \tilde{g}(y).
\]
This bilinear form satisfies following properties:

1. \( [u, v]_g + [v, u]_g = \beta(u, v) \) and \( [u, u]_g = Q(u) \) for all \( u, v \in V_g \).
2. \( g \) is an isometry on \( V_g \) with respect to \([ \ , \ ]_g\).
3. \( [v, u]_g = -[u, gv] \) for all \( u, v \in V_g \).
4. \([ \ , \ ]_g\) is non-degenerate.

Then the spinor norm is
\[
\Theta(g) = \text{disc}(V_g, [ \ , \ ]_g) \text{ if } g \neq I
\]
extended to \( I \) by defining \( \Theta(I) = \overline{T} \). An element \( g \) is called regular if \( V_g \) is non-degenerate subspace of \( V \) with respect to the form \( \beta \). Hahn [9] Proposition 2.1] proved that for a regular element \( g \) the spinor norm is \( \Theta(g) = \det(\tilde{g} |_{V_g}) \text{disc}(V_g) \). This gives

**Proposition 5.1.**

1. For a reflection \( \rho_v \), \( \Theta(\rho_v) = \overline{Q(v)} \).
2. \( \Theta(-1) = \text{disc}(V, \beta) \).
3. For a unipotent element \( g \) the spinor norm is trivial, i.e., \( \Theta(g) = \overline{T} \).

Murray and Roney-Dougal [13] used the formula of Hahn to compute spinor norm. However, we show (Corollary B) that the Gaussian elimination developed in Section [4] outputs the spinor norm quickly. First we observe the following:

**Lemma 5.2.** For the group \( O(d, k) \), \( d \geq 4 \),

1. \( \Theta(x_{i,j}(t)) = \Theta(x_{i,-j}(t)) = \Theta(x_{0,j}(t)) = \overline{T} = \Theta(x_{0,0}(t)) \).
2. \( \Theta(w_l) = \overline{T} \).
3. \( \Theta(\text{diag}(1, \ldots, 1, \lambda, 1, \ldots, 1, \lambda^{-1})) = \overline{\lambda} \).

**Proof.** We use Proposition 5.1. The first one follows as all elementary matrices are unipotent. The element \( w_l = \rho_{(e_l + e_{-l})} \) is a reflection thus \( \Theta(w_l) = \overline{Q(e_l + e_{-l})} = \overline{T} \).

For the third part we note that \( \text{diag}(1, \ldots, 1, \lambda, 1, \ldots, 1, \lambda^{-1}) = \rho_{(e_l + e_{-l})} \rho_{(e_\lambda + \lambda e_{-l})} \) and hence the spinor norm \( \Theta(\text{diag}(1, \ldots, 1, \lambda, 1, \ldots, 1, \lambda^{-1})) = \Theta(\rho_{(e_\lambda + \lambda e_{-l})}) = \overline{Q(e_\lambda + \lambda e_{-l})} = \overline{\lambda} \).

**Proof of Corollary B.** Let \( g \in O(d, k) \). From Theorem A, we write \( g \) as a product of elementary matrices and a diagonal matrix \( \text{diag}(1, \ldots, 1, \lambda, 1, \ldots, 1, \lambda^{-1}) \). Furthermore, the spinor norm of an elementary matrix is \( \overline{T} \). Thus \( \Theta(g) = \Theta(\text{diag}(1, \ldots, 1, \lambda, 1, \ldots, 1, \lambda^{-1})) = \overline{\lambda} \).

6. Double Coset Decomposition for Siegel Maximal Parabolic

In this section, we compute the double coset decomposition with respect to Siegel maximal parabolic subgroup using our algorithm. Let \( P \) be the Siegel maximal parabolic of \( G \) where \( G \) is either \( O(d, k) \) or \( Sp(2l, k) \). In Lie theory, a parabolic is obtained by fixing a subset of
simple roots\textsuperscript{[2]} Section 8.3]. Siegel maximal parabolic corresponds to the subset consisting of all but the last simple root. Geometrically, a parabolic subgroup is obtained as fixed subgroup of a totally isotropic flag\textsuperscript{[12]} Proposition 12.13. The Siegel maximal parabolic is the fixed subgroup of following isotropic flag (with the basis in Section\textsuperscript{2}): \[\{0\} \subset \{e_1, \ldots, e_l\} \subset V.\]

Thus $P$ is of the form \[
\begin{pmatrix}
\alpha & 0 & Y \\
E & A & B \\
F & 0 & D
\end{pmatrix}
\] in $O(2l+1, k)$ and \[
\begin{pmatrix}
A & B \\
0 & D
\end{pmatrix}
\] in $Sp(2l, k)$ and $O(2l, k)$.

The problem is to get the double coset decomposition $P \setminus G / P$. That is, we want to write \[G = \bigsqcup_{\omega \in \hat{W}} P \omega P \] as disjoint union where $\hat{W}$ is a finite subset of $G$. Equivalently, given $g \in G$ we need an algorithm to determine the unique $\omega \in \hat{W}$ such that $g \in P \omega P$. If $G$ is connected with Weyl group $W$ and suppose $W_p$ is the Weyl group corresponding to $P$ then\textsuperscript{[3]} Proposition 2.8.1

\[P \setminus G / P \longleftrightarrow W_p \setminus W / W_p.\]

We need a slight variation of this as the orthogonal group is not connected.

In the case of $Sp(2l, k)$, the Weyl group $W = N(T) / T$ where $T$ is a diagonal maximal torus and \[T = \{\text{diag}(\lambda_1, \ldots, \lambda_l, \lambda_1^{-1}, \ldots, \lambda_l^{-1}) \mid \lambda_i \in k^\times\}.\] The group $W$ is isomorphic to a subgroup of $S_{2l}$, the symmetric group on $2l$ symbols $\{1, \ldots, l, -1, \ldots, -l\}$ and is generated by elements $w_{i, i+1}$ and $w_{i, -i}$ which map to permutations $(i, i+1)(-i, -(i+1))$ and $(i, -i)$ respectively. Thus $W$ is isomorphic to $S_l \times (\mathbb{Z}/2\mathbb{Z})^l$ and the subgroup $W_p$ is generated by $w_{i, i+1}$ which proves that the subgroup \[{(i, i+1)(-i, -(i+1)) \mid 1 \leq i \leq l}\] is isomorphic to $S_l$.

For $Sp(2l, k)$, we set $\hat{W} = \{\omega_0 = I, \omega_1 = w_{1, -1} \cdots w_{i, -i} \mid 1 \leq i \leq l\}$ and note that $W = \bigsqcup_{i=0}^{l} W_p \omega_i W_p$.

In the case of $O(d, k)$, we set $\hat{W} = \{\omega_0 = I, \omega_1 = w_{1, -1} \cdots w_{i, -i} \mid 1 \leq i \leq l\}$ where $w_{i, -i}$ is inductively produced (see Lemma\textsuperscript{4.6}).

**Theorem 6.1.** Let $P$ be the Siegel maximal parabolic subgroup in $G$, where $G$ is either $O(d, k)$ or $Sp(d, k)$. Let $g \in G$. Then there is an efficient algorithm to determine $\omega$ such that $g \in P \omega P$. Furthermore, $\hat{W}$ the set of all $\omega$s is a finite set of $l+1$ elements where $d = 2l$ or $2l+1$.

**Proof.** Let $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in O(2l, k)$ or $Sp(2l, k)$. We note that elementary matrices $E_1$ and $E_2$ are in $P$. The proof is just keeping track of elements of $P$ in our Gaussian elimination algorithm. The step 1 in our algorithm in Section 4 says that there are elements $p_1, p_2 \in P$ such that $p_1gp_2 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ where $C_1$ is a diagonal matrix with $m$ non-zero entries. Clearly $m = 0$ if and only if $g \in P$. In that case $g$ is in the double coset $P \omega_0 P = P$. Now suppose $m \geq 1$. Then in Step 2 we multiply by $E_2$ to make the first $m$ rows of $A_1$ zero, i.e., there is a $p_3 \in P$ such that $p_3p_1gp_2 = \begin{pmatrix} \tilde{A}_1 & \tilde{B}_1 \\ C_1 & D_1 \end{pmatrix}$ where first $m$ rows of $\tilde{A}_1$ are zero. After this we interchange rows $i$ with $-i$ for $1 \leq i \leq m$ which makes $C_1$ zero, i.e., multiplying by $\omega_m$ we get $\omega_m p_3p_1gp_2 = \begin{pmatrix} A_2 & B_2 \\ 0 & D_2 \end{pmatrix} \in P$. Thus $g \in P \omega_m P$.

For $O(2l+1, k)$ we note that the elementary matrices $E_1, E_2$ and $E_4a$ are in $P$. Rest of the proof is similar to the earlier case and follows by carefully keeping track of elementary matrices used in our algorithm in Section\textsuperscript{4.2}.
ACKNOWLEDGEMENT

Authors thank Dipendra Prasad and K. N. Raghavan for friendly and useful discussions.

REFERENCES

1. Peter Brooksbank, Constructive recognition of classical groups in their natural representation, Journal of Symbolic Computation 35 (2003), 195–239.
2. Roger Carter, Simple groups of Lie type, Pure and Applied Mathematics, vol. 28, John Wiley & Sons, 1972.
3. ______, Finite groups of Lie type, John Wiley & Sons, 1993.
4. C. Chevalley, Sur certains groupes simples, Tohoku Math. J. 7 (1955), no. 2, 14–66.
5. Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor, Computing in groups of Lie type, Mathematics of computation 73 (2003), no. 247, 1477–1498.
6. Elliot Costi, Constructive membership testing in classical groups, Ph.D. thesis, Queen mary, Univ. of London, 2009.
7. Joseph F. Grcar, Mathematicians of Gaussian elimination, Notices of the AMS 58 (2011), no. 6, 782–792.
8. Larry C. Grove, Classical groups and geometric algebra, vol. 39, American Mathematical Society, Graduate Studies in Mathematics, 2002.
9. Alexander J. Hahn, Unipotent elements and the spinor norms of Wall and Zassenhaus, Arch. Math. (Basel) 32 (1979), no. 2, 114–122.
10. William Kantor and Ákos Seress, Black box classical groups, vol. 149, Memoirs of the American Mathematical Society, 2001.
11. C. R. Leedham-Green and E. A. O’Brien, Constructive recognition of classical groups in odd characteristic, J. Algebra 322 (2009), no. 3, 833–881.
12. Gunter Malle and Donna Testerman, Linear algebraic groups and finite groups of lie type, Cambridge University Press, 2011.
13. Scott H. Murray and Colva M. Roney-Dougal, Constructive homomorphisms for classical groups, Journal of Symbolic Computation 46 (2011), 371–384.
14. Ákos Seress, An introduction to computational group theory, Notices of the AMS 44 (1997), no. 6, 671–679.
15. Robert Steinberg, Lectures on Chevalley groups. notes prepared by John Faulkner and Robert Wilson, Yale University, 1968.
16. Donald E. Taylor, The geometry of the classical groups, Heldermann Verlag, 1992.
17. G. E. Wall, The structure of a unitary factor group, Inst. Hautes Études Sci. Publ. Math (1959), no. 1, 23 pp.
18. Hans Zassenhaus, On the spinor norm, Arch. Math. (1962), no. 13, 434–451.