An algorithm for Lang's Theorem

Arjeh M. Cohen\textsuperscript{a,}\textsuperscript{*}, Scott H. Murray\textsuperscript{b}

\textsuperscript{a} Eindhoven University of Technology, Department of Mathematics and Computer Science, PO Box 513, Eindhoven, Netherlands
\textsuperscript{b} Department of Mathematics and Statistics F07, University of Sydney, NSW 2006, Australia

ARTICLE INFO

Article history:
Received 6 June 2005
Available online 25 April 2009
Communicated by William M. Kantor

To John Cannon and Derek Holt on the occasions of their significant birthdays, in recognition of distinguished contributions to mathematics

Keywords:
Lie algebra
Linear algebraic group
Chevalley basis
Weyl group
Derangements
Las Vegas type algorithm
Maximal toral subalgebra

ABSTRACT

We give an efficient Las Vegas type algorithm for Lang's Theorem in split connected reductive groups defined over finite fields of characteristic greater than 3. This algorithm can be used to construct many important structures in finite groups of Lie type. We use an algorithm for computing a Chevalley basis for a split reductive Lie algebra, which is of independent interest. For our time analysis we derive that the proportion of reflection derangements in a Weyl group is less than $2/3$.

© 2009 Elsevier Inc. All rights reserved.

1. Introduction

A finite group of Lie type can be described as the rational points of a connected reductive algebraic group over a finite field. Given a structure in the algebraic group, such as a conjugacy class or a maximal torus, we want to find the corresponding structures in the finite group of Lie type. This can often be achieved with Lang’s Theorem. We provide a computationally efficient algorithm for Lang’s Theorem in split connected reductive groups. Our algorithm is randomised but guaranteed to return...
a correct answer, i.e., it is Las Vegas in the sense of [Bab97]. We have implemented this algorithms in the Magma computer algebra system [BC97]. Glasby and Howlett [GH97] have already solved this problem in a special case; our algorithm is inspired by their work and the proof of Lang’s Theorem given in [Mül03].

Throughout this paper, k is a finite field of size q and characteristic p, and k_r is the unique degree r extension of k in the algebraic closure \( \overline{k} \). The affine space of dimension N can be identified with \( \overline{k}^N \).

An affine variety \( X \) is a subset of \( \overline{k}^N \) that consists of the zeroes of a collection of polynomials. The variety is defined over k if it is closed under the action of the map \( F : \overline{k}^N \to \overline{k}^N \) that takes the \( q^t \) power of each component. The restriction of \( F \) to \( X \) is called the (standard) Frobenius endomorphism of \( X \). The set of rational points of \( X \) over \( k_r \), denoted by \( X(k_r) \), consists of those elements of \( X \) fixed by \( F^t \). A nonstandard Frobenius endomorphism is a morphism \( F^t : X \to X \) such that \((F^t)^s = F^s\) for some positive integer s. The elements of \( X \) fixed by \( F^t \) are the rational points of a k-form of \( X \). In this paper, Frobenius endomorphisms are standard unless otherwise stated.

A linear algebraic group is an affine variety with group multiplication and inversion given by rational functions. See, for example, [Spr98] for more details including the definitions of reductive and connected groups. Every linear algebraic group contains a maximal connected subgroup \( G^0 \), the component of the identity. This subgroup is normal and \( G/G^0 \) is finite, so for many purposes it suffices to study connected groups. An important result on linear algebraic groups over finite fields is:

**Theorem 1.1** (Lang’s Theorem). If \( G \) is a connected linear algebraic group defined over the finite field \( k \) with Frobenius map \( F \), then the map

\[
G \to G, \quad a \mapsto a^{-F} a
\]

is onto.

This is equivalent to the statement that the first Galois cohomology of \( G \) is trivial.

In this paper, we give an algorithm for Lang’s Theorem for \( G \) a k-split connected reductive group. This is likely to be the critical case for an algorithm for arbitrary connected algebraic groups (see Section 3). The group \( G \) is determined by the base field \( k \) and a root datum \((X, \Phi, Y, \Phi^\star)\) [Dem65]. We describe \( G \) by the Steinberg presentation with generators \( x_\alpha(a) \), for \( \alpha \in \Phi \) a root and \( a \in k \), and \( y \otimes t \), for \( y \in Y \) and \( t \in k^\times \). The relations are given in [CMT04, Section 4.1]. The action of the standard Frobenius map is given by \( x_\alpha(a)^F = x_\alpha(a^q) \) and \((y \otimes t)^F = y \otimes t^q \).

Recall that the (reductive) rank \( n \) of \( G \) is the rank of \( X \) and the semisimple rank \( \ell \) of \( G \) is the rank of the root system \( \Phi \). The fundamental group of \( G \) is the quotient of the full integer lattice \( \mathbb{Z}^\ell \) by the sublattice generated by the rows of the Cartan matrix. This group is finite and depends only on the Cartan type of \( G \). If \( G \) is simple of Cartan type \( A_\ell \), then the fundamental group is cyclic of order \( \ell + 1 \); for all other simple groups, the fundamental group has order at most 4.

We use soft-O notation to simplify our timings: recall that \( O^\sim(N) \) means \( O(N(\log(N))^c) \) for some constant \( c \). Addition, subtraction, multiplication, division, and equality testing in the field of size \( q \) all take time \( O^\sim(\log(q)) \) by [Shp99, Introduction]. In [CHM08], we showed that elements of \( G \) can be stored as canonical words of length \( O(n + \ell^2) \); and multiplication and inversion of elements in \( G(k) \) takes time \( O^\sim(n^3 \log(q)) \).

We can now state our main result:

**Theorem 1.2.** Let \( k \) be a finite field of size \( q \) and of characteristic greater than 3. Let \( G \) be a k-split connected reductive linear algebraic group of rank \( n \). Let \( m \) be the exponent of the fundamental group of \( G \). Let \( c \) be in \( G(k_r) \), and suppose we are given \( s \), the order of \( c^{F-1} \cdots c^{F \ell} \). Then we can find \( a \in G(k_{rs}) \) such that \( c = a^{-F} a \) in Las Vegas time \( O^\sim(n^3 m^2 r^2 s^2 \log(q)^2) \).

We can improve significantly on this result for simple classical groups:
Theorem 1.3. Let $G$ be a $k$-split simple classical group of rank $n$, defined over the field $k$ of size $q$. Let $m$ be the exponent of the fundamental group of $G$. Let $c$ be in $G(k_r)$ and suppose we are given $s$, the order of $c^{F_{r-1}} \cdots c^F$. Then we can find $a \in G(k_r)$ such that $c = a^{-F} a$ in Las Vegas time $O^\sim(n^3 m^2 r^2 s^2 \log(q))^2)$.

Note that a similar timing also applies to simple exceptional groups when $q$ has characteristic greater than 3, since the rank is bounded.

The parameter $s$ measures the size of the field extension required, as explained in Section 2. The input element $c$ has size $O^\sim(n^3 r \log(q))$ and the output element $a$ has size $O^\sim(n^2 rs \log(q))$. So our running time is polynomial in the size of the output rather than the input. In Section 3, we use the concept of $F$-eigenvectors to reduce to a problem involving forms of $G$-modules. A solution to this problem and a proof of Theorem 1.3 is given in Section 4.2. This solution uses the algorithm for computing a standard Chevalley basis in the Lie algebra of $G$ described in Section 5.

The key result in obtaining the Chevalley basis may be of interest in its own right and so we state it here.

Theorem 1.4. Suppose that $k$ is a finite field of size $q$ and characteristic greater than 3. Let $G$ be a $k$-split connected reductive group and let $L$ be the Lie algebra of $G$. We can find a split maximal toral subalgebra of $L$ in Las Vegas time $O^\sim(n^3 \log(q))^2)$.

Note that this is equivalent to time $O^\sim(d^{4.5} \log(q))^2)$, where $d$ is the dimension of $L$. This is similar to a result by Ryba [Ryb07].

The running times of the algorithms are analysed in Section 6, leading to proofs of Theorems 1.2 and 1.4. This uses an interesting extension of a standard result from combinatorics. Recall that a permutation is called a derangement if it has no fixed points. The proportion of derangements in the symmetric group $\text{Sym}_t$ acting on $t$ letters is known to approach $1/e$ as $t \to \infty$. We give a similar result for Weyl groups acting by conjugacy on reflections:

Theorem 1.5. The proportion of derangements in a Weyl group acting on reflections is less than $2/3$.

2. Minimum field degree

Computation in large finite fields is a challenging problem (see, for example, [LN97]). So we start with an easy result giving the size of the field extension needed for Lang’s Theorem. We define the minimum field degree of $g \in G$ as the smallest $r$ such that $g^{F_r} = g$. Note that $g$ has minimum field degree $r$ if, and only if, $k_r$ is the smallest extension of $k$ such that $g$ is in $G(k_r)$. The minimal field degree of $g$ can be computed by finding the smallest field $k_r$ containing all the field elements occurring in the canonical word for $g$.

We can now determine the minimal field degree of the output of our algorithm:

Proposition 2.1. Let $G$ be a connected linear algebraic group defined over $k$. Let $c$ be an element of $G$ with minimum field degree $r$ and let $s$ be the order of $c^{F_{r-1}} \cdots c^F$. If $c = a^{-F} a$ for some $a$ in $G$, then the minimum field degree of $a$ is $rs$.

Proof. Let $m$ be the minimum field degree of $a$. Clearly $k_r$ is a subfield of $k_m$, so $r$ is a divisor of $m$, say $ru = m$. Since $c^{F_r} = c$, we have

$$
(c^{F_{r-1}} \cdots c^F)^u = c^{F_{m-1}} \cdots c^F = a^{-F} a^{F_{m-1}} \cdots a^{-F^2} a^F a^{-F} a = a^{-F^m} a.
$$

Hence $a^{F^m} = a$ if, and only if, $u$ is a multiple of $s$. \qed

The most important consequence of this proposition is that the minimum field degree is independent of the particular choice of $a$ and can be computed beforehand. In all our timings of algorithms with input $c$, we consider $s$, the order of $c^{F_{r-1}} \cdots c^F$, to be an input of our algorithm. While it is
Let recompute $s$ eigenvalue" is always one). The set computing elements have straightforward to compute $s$, no polynomial time algorithm is known. The best known method for computing $s$ is to convert from the Steinberg presentation of $G$ to a faithful representation [CMT04] and then compute the order of the corresponding matrix using the Las Vegas algorithm of [CLG97].

Suppose now that $G$ is a $k$-split reductive group with reductive rank $n$ and semisimple rank $\ell$. The element $c$, which is the input to our algorithm, has size $O^\sim((n+\ell^2)r \log(q))$; while the element $a$, which is the output, has size $O^\sim((n+\ell^2)\ell r s \log(q))$. Since $s$ need not be bounded by a polynomial in $n$, $\ell$, $r$, and $\log(q)$, there is no algorithm for Lang's Theorem that is polynomial in the size of the input. The best we can hope for is an algorithm which is polynomial in the size of the output. We note that $s$ can be quite small in practice. For example, to construct twisted tori we need to apply Lang's Theorem to Weyl group representatives (the elements denoted $\hat{w}$ in the Steinberg presentation). These elements have $r = 1$ and $s$ at most $O(\ell^2)$.

3. Twisted eigenvectors

Let $V = \overline{k}^d$ be a split vector space defined over $k$, so that $F$ acts on $V = \overline{k}^d$ by taking the $q$th power of each coefficient. We say that $v \in V$ is an $F$-eigenvector of $c \in \text{GL}_d(k)$ if $v^F c = v$ (note that the "$F$-eigenvalue" is always one). The set $E(k)$ of all $F$-eigenvectors in $V$ is a $k$-space of dimension $d$. Once again take $r$ to be the minimum field degree of $c$, and $s$ to be the order of $cF^{r-1} \cdots c$. By Lang's Theorem, the $kF$-span of $E(k)$ must be equal to $V(k_{d})$. There is a variety $E$ defined over $k$ such that $E(k_{d})$ is the $k_{d}$-span of $E(k)$ for every positive integer $t$. Such a variety is called a $k$-form of $V$ [Spr98, Section 11.1].

The following easy lemma is the key to our recursive approach.

Lemma 3.1. Let $G$ be a connected linear algebraic group defined over $k$ and let $V$ be a $G$-module defined over $k$ with kernel $K \leq G$. Let $c$ be an element of $G$. Suppose that $E(k)$ is the set of $F$-eigenvectors of $c$ in $V$. Then $a \in G$ satisfies $c \in a^{-F} K a$ if, and only if, $V(k)a = E(k)$.

Proof. If $a^{-F}za = c$ for $z \in K$, then, for all $v \in V(k)$, $va = vza = vaF c = (va)^F c$ and so $va \in E(k)$. Conversely, if $V(k)a = E(k)$, then, for all $v \in V(k)$, $va = (va)^F c = vaF c$ and so $aF^{-1}ca^{-1} \in K$. □

Our approach to solving Lang's Theorem is outlined in Algorithm 1. We call an element $a \in G(k_{d})$ such that $V(k)a = E(k)$ a transformer in $G$ for the $k$-form $E$. If $V$ is faithful, then the previous lemma ensures that $a^{-F}a = c$. Otherwise we recurse to a connected subgroup containing the kernel $K$. Note that $s$ is taken to be the order of $cF^{r-1} \cdots c$ in the top-level function call. It is not necessary to recompute $s$ for the recursive calls since a multiple of the element order works just as well.

Suppose now that $G$ is a split connected reductive group described by a Steinberg presentation. Let $T_0$ be the subgroup generated by the elements $y \otimes t$, for $y \in Y$ and $t \in \mathbb{F}^\times$. Then $T_0$ is the standard $k$-split maximal torus of $G$. Using the methods of [CMT04], we can construct a module $V$ which is projectively faithful, that is, the kernel $K$ is contained in the centre $Z(G)$ of $G$. We can now
take $H = T_0$ in Algorithm 1, since $Z(G)$ is contained in every maximal torus of $G$. Since a split torus has an easily constructed faithful module, there is at most one recursive call for reductive groups. The same algorithm could, in principle, be used for a nonreductive connected group $G$: construct a reductive quotient $G/N$, take $V$ to be the $G$-module induced by a projectively faithful module for $G/N$, and take $H$ to be the preimage in $G$ of the maximal torus in $G/N$. However, finding the normal subgroup $N$ and constructing the quotient $G/N$ are nontrivial problems which lie beyond the scope of this paper.

Algorithms for finding transformers are discussed in the next section. We now give two algorithms for computing the $F$-eigenspace. The most straightforward method is given in Algorithm 2. The key is to consider $k_{rs}$ as a $k$-space of dimension $rs$ and to consider $V(k_{rs}) = k_{rs}^d$ as a $k$-space of dimension $d_{rs}$. The solution is then found by linear algebra over $k$. We compute $S$ in time $O^\sim((r^2s^2\log(q)^2))$ by taking $q$th powers of the elements in a $k$-basis of $k_{rs}$. Finding $C$ takes time $O^\sim(r^2s^2\log(q))$. The fixed space computation takes time $O^\sim(d^2r^2s^2\log(q))$. So the overall algorithm requires time $O^\sim(d^2r^2s^2\log(q)^2)$.

An alternative method, due to Glasby and Howlett [GH97], is given in Algorithm 3. It takes time $O^\sim(d^2rs\log(q)^2)$ to apply $F$ to a $d \times d$ matrix, so computing $a$ takes time $O^\sim(d^2r^2s^2\log(q)^2)$. Each randomly chosen $x$ has a probability of at least $1/4$ of yielding an invertible element $a$. Since this probability is bounded away from zero as $q$, $r$, $s$, and $d$ become large, the algorithm is Las Vegas. Note that we have an algorithm for Lang’s Theorem for the case $G = \text{GL}(V)$ if the function returns $a$ instead of $V(k)a^{-1}$.

We now have

**Theorem 3.2.** Let $V$ be a split vector space over $k$ with dimension $d$. Let $c$ be an element of $\text{GL}(V)$ with minimum field degree $r$ and let $s$ be the order of $c^{F-1} \cdots c^F$. We can compute a basis for the $k$-space $E(k)$ of $F$-eigenvectors of $c$ in deterministic time $O^\sim(d^2r^2s^2\log(q)^2)$ or Las Vegas time $O^\sim(d^2r^2s^2\log(q)^2)$.

### 4. Finding transformers

Let $G$ be a $k$-split connected reductive linear algebraic group defined over $k$. Suppose that $G$ is described by the Steinberg presentation with root datum $(X, \Phi, Y, \Phi^*)$. Let $c$ be in $G(k_F)$, and let $s$ be the order of $c^{F-1} \cdots c^F$. Let $V$ be a projectively faithful $G$-module and compute $E$, the $k$-form of $F$-eigenvectors of $c$. In this section, we show how to find a transformer $a \in G(k_{rs})$ such that $E(k)a = V(k)$. First we consider two special cases: $k$-split tori and classical groups. Then we give an algorithm for an arbitrary $k$-split connected reductive group. The key is to consider bases of $V(k)$ with some additional structure that ensures that $G$ is transitive on all such bases (or $G_{\text{ad}}$ is transitive in Section 4.3).
4.1. Split tori and isogeny

A $k$-split torus $T$ of dimension $n$ is the split connected reductive group with root datum $(\mathbb{Z}^n, \emptyset, \emptyset)$. So $T$ is just $\mathbb{Z}^n \otimes \bar{k}^\times = (\bar{k}^\times)^n$ with the Frobenius endomorphism taking the $q$th power of each component. The standard module $V$ is just $k^n$ with the componentwise action. Suppose $c = (c_1, \ldots, c_n) \in T(k_r)$ and $E$ is the variety of $F$-eigenvectors of $c$ in $V$. Applying Theorem 3.2 to each component separately, we can compute $E$ in Las Vegas time $O^\ast(nr^2s^2 \log(q)^2)$. This gives a basis of $E$ of the form $a_1e_1, \ldots, a_re_r$ where each $a_i \in k_r^\times$ and $e_i$ is the $i$th standard basis vector in $V$. Now $(a_1, \ldots, a_r) \in T(k_{rs})$ is a transformer for $E$. Hence we have proved

**Proposition 4.1.** Let $T$ be a $k$-split torus of dimension $n$. Let $c$ be in $T(k_r)$, and suppose we are given $s$, the order of $c^{F^{-1}} \cdots c^F$. Then we can find an element $a$ in $T(k_{rs})$ such that $c = a^{-F}a$ in Las Vegas time $O^\ast(nr^2s^2 \log(q)^2)$.

We now give an application of this proposition to isogenous groups. Consider two split connected reductive groups $G_1$ and $G_2$ defined over $k$. Let $(X_i, \Phi_i, Y_i, \Phi_i^\ast)$ be the root datum of $G_i$ for $i = 1, 2$. Suppose that there is an isomorphism $\phi : Y_1 \otimes \bar{k}^\times \to Y_2 \otimes \bar{k}^\times$ such that $\phi(Y_1) \subseteq Y_2$ and $\phi(\Phi_i^\ast) = \Phi_2^\ast$. For $\alpha \in \Phi_1$, define $\vec{\alpha} \in \Phi_2$ by $\phi(\alpha^\ast) = \vec{\alpha}^\ast$.

We can easily modify the presentation of $G_2$ so that the signs defined in [CMT04, Section 2] agree (i.e., $\epsilon_{\alpha, \beta} = \epsilon_{\vec{\alpha}, \vec{\beta}}$ for all $\alpha, \beta \in \Phi_1$). Then $\iota : G_1 \to G_2$ defined by

$$\iota(x_a(a)) = x_{\vec{a}}(a) \quad \text{and} \quad \iota(y \otimes t) = \phi(y) \otimes t$$

is an isogeny, i.e., an epimorphism with finite kernel. Every isogeny from a split connected reductive group $G_1$, with kernel contained in the centre of $G_1$, can be put in this form by precomposing with an automorphism of $G_1$ [Car93]. Denote by $T_1$ the standard torus $Y_1 \otimes \bar{k}^\times$. Note that the kernel $K$ of $\iota$ is a finite subgroup of $Z(G_1) \subseteq T_1$. An important invariant of $\iota$ is the exponent of $K$, which we denote by $m$. Note that $m$ is bounded by the exponent of the fundamental group of $G_1$ (or $G_2$, since the groups have the same Cartan matrix).

For $g \in T_1(k_r)$, we have $\iota(g)^F = \iota(g^F) = \iota(g)$, so $\iota(g) \in T_2(k_r)$. This image can be computed in time $O^\ast(n^2r \log(q))$ by linear algebra over $k_r$.

For $h \in T_2(k_r)$, we can find $g \in T_1$ such that $\iota(g) = h$. Then $\iota(g^{-F}g) = h^{-F}h = 1$, i.e., $g^{-F}g \in K$. Hence $(g^{-F}g)^m = 1$ and so $g^m \in T_1(k_r)$. Using the fact that $T_0$ is a direct sum of copies of $\bar{k}^\times$, such a $g$ must be in $T_0(k_{rm})$. This preimage can be computed in time $O^\ast(n^2rm \log(q))$.

**Proposition 4.2.** Let $G_1$ and $G_2$ be $k$-split connected reductive linear algebraic groups defined over $k$ with reductive rank $n$. Suppose we have an isogeny $\iota : G_1 \to G_2$, defined as above, whose kernel has exponent $m$. For $c$ in $G_1$, let $s(c)$ denote the order of $c^{F^{-1}} \cdots c^F$, where $r$ is the minimum field degree of $c$.

1. Lang's Theorem can be solved for $c \in G_1(k_r)$ in time $O^\ast(n^3r^2s(c)^2m^2 \log(q)^2)$, plus the time needed to solve it for some $c \in G_2(k_r)$ with $s(c) \leq s(c)$.

2. Lang's Theorem can be solved for $c \in G_2(k_r)$ in time $O^\ast(n^3rs(c)m^2 \log(q)^2)$, plus the time needed to solve it for some $c \in G_1(k_{r_m})$ with $s(c) \leq ms(c)$.

**Proof.** If $c \in G_1(k_r)$, then $c' = \iota(c)$ can be found in time $O^\ast(n^3r \log(q))$. Clearly $s(c') \leq s(c)$. Now we can find $a' \in G_2(k_{r_m})$ such that $a'^{-F}a' = c'$. Let $a \in G_1(k_{r_m})$ be a preimage of $a'$ computed in time $O^\ast(n^3rm \log(q)^2)$. Consider $a^{F^{-1}}c^{-1} \in K(k_{r_m}) \subseteq T_1(k_{r_m})$. Now

$$(a^{F^{-1}}c^{-1})^{F^{-1}c^{-1}} \cdots (a^{F^{-1}}c^{-1})^F (a^{F^{-1}}c^{-1}) = a^{F^{-1}c^{-1}}(c^{F^{-1}c^{-1}} \cdots c^F)c^{-1} = 1.$$

So by Proposition 4.1, we can find $b \in T_1(k_{r_m})$ such that $a^{F^{-1}}c^{-1} = b^{-F}b$ in Las Vegas time $O^\ast(nr^2s(c)^2m^2 \log(q)^2)$. Now $(ba)^{-F}ba = c$ and Part (1) follows.
If \( c \in G_2(k_\ell) \), we can find an element \( c' \in G_1(k_m) \) such that \( \iota(c') = c \) in time \( O^*(n^3 m \log(q)) \). Since \((c' F^{F^{-1}} \cdots c' F^c c') = c \in k_m, \) we get \( s(c') \mid ms(c) \). We can now find \( a' \in G_2(k_{rs(c)m^2}) \) such that \( c' = a'^{-F} a \). Then \( a = \iota(a') \) can be computed in time \( O^*(n^3 rs(c)m^2 \log(q)) \) and \( a^{-F} a = c \). \( \square \)

Let \( G \) be a split connected reductive group with root datum \((X, \Phi, Y, \Phi^*)\). Define \( Y_{sc} = \mathbb{Z}\Phi^* \) and let \( X_{sc} \) be its dual lattice in \( X \otimes \mathbb{Q} \). Then \((X_{sc}, \Phi, Y_{sc}, \Phi^*)\) is also a root datum, with corresponding group denoted \( G_{sc} \). There is an isogeny map \( G_{sc} \to G \) induced by the embedding \( Y_{sc} \to Y \). Note that \( G_{sc} \) is simply connected if \( G \) is semisimple. A dual construction gives us a group \( G_{ad} \), which is adjoint when \( G \) is semisimple, and an isogeny \( G \to G_{ad} \). It is well known that the action of \( G_{ad} \) on the corresponding Lie algebra is faithful. In light of the above proposition, an effective algorithm for Lang’s Theorem need only find a transformers for adjoint groups.

4.2. Classical groups

We now show how to find transformers for the classical groups, using the standard representations. See [CHM08] for the relationship between these representations and the Steinberg presentations. Throughout this section we take \( V = k^d \) and \( B_0 \) to be the standard basis \( e_1, \ldots, e_d \) of \( V(k) \).

The easiest case is \( G = \text{GL}_d(k) \): Let \( B \) be a \( k \)-basis of \( E(k) \). Let \( a \) be the matrix whose rows are the elements of \( B \). Then \( B_{0d} = B \), and so \( a \) is a transformer for \( E \).

Now suppose \( G = \text{SL}_d(k) \). Given a basis \( B \) of \( V \), define its \textit{volume}, denoted \( \text{vol}(B) \), to be the determinant of the matrix whose rows are the elements of \( B \). Then \( B_0 \) has volume one and \( G \) is transitive on all bases of volume one. Now suppose \( B \) is a basis of \( E(k) \), the set of \( F \)-eigenvectors of \( c \in G \). Then \( B^F c = B \), so

\[
\text{vol}(B)^F = \text{vol}(B^F) = \text{vol}(Bc^{-1}) = \text{vol}(B) \det(c)^{-1} = \text{vol}(B),
\]

and so \( \text{vol}(B) \in k \). We can now construct a basis \( B' \) of \( E(k) \) with volume one by dividing the first element of \( B \) by the scalar \( \text{vol}(B) \). So the matrix that takes \( B_0 \) to \( B' \) is a transformer in \( G \).

Now suppose that \( q \) is odd. Let \( M \) be an orthogonal or symplectic form on \( V \) whose value is written \( (u, v) \) for \( u, v \in V \). Further suppose that \( M \) is defined over \( k \). Then the invariant group

\[
G = \{ x \in \text{GL}_d (\bar{k}) \mid (ux, vx) = (u, v) \}
\]

is a reductive linear algebraic group defined over \( k \). Note that \( G \) is not necessarily split or connected however. Let \( \delta \) be a fixed nonsquare in \( k \). Define the \( m \times m \) matrix

\[
A_m = \begin{pmatrix}
0 & & \\
& 1 & \\
& & \ddots \\
& & & 1
\end{pmatrix}.
\]

Then the form \( M \) has precisely one of the following Gram matrices \( M_B \) with respect to some basis \( B \):

- If \( M \) is orthogonal and \( d = 2\ell + 1 \), then

\[
M_B = A_d \quad \text{or} \quad \begin{pmatrix}
A_{\ell} \\
& \delta \\
& & A_{\ell}
\end{pmatrix}.
\]
NORMALBasis := function(U)
    let u be a nonzero element of U
    if dim(U) = 1 then
        find a ∈ k such that a² = (u, u) or a²δ = (u, u)
        return u/a
    end if
    let v be a nonzero element of u⁻¹ \ ku
    if dim(U) = 2 then
        if (u, u) ∈ −δ(v, v)k² then [U anisotropic]
            find a, b ∈ k such that (u, u)a² + (v, v)b² = 1
            find c ∈ k such that ((u, u)a² − (v, v)b²)c² = −δ
            return au + bv, c(au − bv)
        else [U isotropic]
            find a, b ∈ k such that (u, u)a² + (v, v)b² = 0
            let w be a nonzero element of (au + bv)⁻¹
            return au + bv, w
        end if
    end if
    let w be a nonzero vector in (ku + kv)⁻¹ \ (ku + kv)
    find a, b, c ∈ k such that (u, u)a² + (v, v)b² + (w, w)c² = 0
    let x be a nonzero element of (au + bv + cw)⁻¹
    return au + bv + cw, NORMALBasis((u, v)⁻¹), x
end function

Algorithm 4. Finding a normal basis for a space with a bilinear form.

• If M is orthogonal and d = 2ℓ, then

\[
M_B = A_d \quad \text{or} \quad \begin{pmatrix}
1 & A_{\ell-1} \\
A_{\ell-1} & -\delta
\end{pmatrix}.
\]

• If M is symplectic, then d = 2ℓ and

\[
M_B = \begin{pmatrix}
-A_\ell & A_\ell \\
A_\ell & -A_\ell
\end{pmatrix}.
\]

A normal basis for M is a basis of V such that M_B is one of these matrices.

Given a symplectic or orthogonal form M on the k-space U, Algorithm 4 constructs a normal basis for U. The quadratic equations involved always have solutions by the standard classification theory of bilinear forms over finite fields (see [Gro02] for more details). Each of these equations can be solved in Las Vegas time \( O^{-}(\log(q)^{2}) \) by [vzGS92]. Note that this construction is rational (that is, it does not use extensions of k) and takes time \( O^{-}(d^{3}\log(q) + d\log(q)^{2}) \).

If the form M is symplectic, we are done: our transformer is simply the matrix taking a normal basis of V(k) to a normal basis of E(k).

If M is orthogonal, the two normal bases may have different Gram matrices, in which case the equation in Lang’s Theorem has no solution. This is to be expected, since G is not connected in this case. If we take \( G = \text{SO}_d(M) \), then this problem can be avoided. Without loss of generality, the standard basis \( B_0 \) is normal. Suppose that B is a normal basis of E(k). As with the special linear group, vol(B) is in k. Also

\[
\det(M_B) = \det(BM_B B^T) = \text{vol}(B)^2 \det(M_{B_0}).
\]

But the two choices given above for the Gram matrix have determinants in different cosets of \( k^{2} \), hence \( M_{B_0} = M_B \). It now remains to ensure that vol(B) is one. Now vol(B)^2 = det(M_{B_0})/det(M_B) = 1,
so suppose $\operatorname{vol}(B) = -1$. If $M_B = A_d$, then exchanging the first and last vectors in $B$ results in a new normal basis with volume one. Otherwise, negating the $(\ell + 1)$st vector in $B$ has the same effect.

Similar methods work for quadratic forms in characteristic two. Using the Las Vegas algorithm of Theorem 3.2 to find a basis for $E(k)$, we now have

**Proposition 4.3.** Let $G$ be $\operatorname{GL}_d(k)$, $\operatorname{SL}_d(k)$, $\operatorname{Sp}_d(M)$ for some symplectic form $M$, or $\operatorname{SO}_d(M)$ for some orthogonal or quadratic form $M$. Let $c$ be an element of $G$ with minimum field degree $r$ and let $s$ be the order of $c^{d-1} \cdots c^2 c$. Then we can find $a \in G(k_{rs})$ such that $c = a^{-f} a$ in Las Vegas time $O^\sim (d^3 r^2 s^2 \log(q)^2)$.

Note that this result applies to nonsplit special orthogonal groups, and could easily be extended to the unitary groups as well.

We can now prove Theorem 1.3: Let $G$ be a split simple classical group $G$ of (reductive and semisimple) rank $n$. Then $G$ is isogenous to one of the groups considered above, with $d = O(n)$.

If $G$ has type $A_n$, then there is an isogeny map $\operatorname{SL}_{n+1}(k) \to G$ with $m \leq n + 1$. We can easily ensure that this map is defined with respect to the Steinberg presentation as in the previous section. By Proposition 4.2(2), we can solve Lang’s Theorem in $G$ in Las Vegas time $O^\sim (n^4 m^2 r^2 s^2 \log(q)^2)$.

If $G$ is of type $B_n$, $C_n$, or $D_n$, then let $G_{sc}$ be the simply connected group with the same Cartan type as $G$. We can find isogenies $G_{sc} \to G$ and $G_{sc} \to H$ as in the previous section, where $H$ is either $\operatorname{SO}_{2n+1}(M)$, $\operatorname{Sp}_{2n}(M)$, or $\operatorname{SO}_{2n}(M)$ for the appropriate form $M$. For each of these isogenies, $m$ is at most 4. So, by Proposition 4.2, we can solve Lang’s Theorem in Las Vegas time $O^\sim (n^4 r^2 s^2 \log(q)^2)$.

The exceptional groups can also be described as invariant groups of multilinear structures. We could find transformers for these group by normalising the corresponding structures. Examples include composition algebras for groups of type $G_2$ and Jordan algebras for groups of type $F_4$ [SV00].

### 4.3. Adjoint representation

Now consider an arbitrary $k$-split connected reductive linear algebraic group $G$, with reductive rank $n$ and semisimple rank $\ell$. Then $G$ is given by the Steinberg presentation with root datum $(X, \Phi, Y, \Phi^*)$ and standard $k$-split maximal torus $T_0 = Y \otimes \bar{k}$. Fix dual bases $e_1, \ldots, e_n$ for $X$ and $f_1, \ldots, f_n$ for $Y$. The Lie algebra $L = L(G)$ is a $G$-module defined over $k$. This is called the **adjoint representation** of $G$ and it is projectively faithful. Now $L(k)$ has basis elements $e_\alpha$ for $\alpha \in \Phi$ and $h_i \in L(T_0)$ for $i = 1, \ldots, n$ with structure constants:

\[
[h_i, h_j] = 0, \quad (1)
\]

\[
[e_\alpha, h_i] = (\alpha, f_i)e_\alpha, \quad (2)
\]

\[
[e_{-\alpha}, e_\alpha] = \sum_{i=1}^n (e_i, \alpha^*) h_i, \quad (3)
\]

\[
[e_\alpha, e_\beta] = \begin{cases} N_{\alpha\beta} e_{\alpha+\beta} & \text{for } \alpha + \beta \in \Phi, \\ 0 & \text{for } \alpha + \beta \notin \Phi, \beta \neq -\alpha, \end{cases} \quad (4)
\]

where the integral constants $N_{\alpha\beta}$ are defined in [Car72]. Such a basis is called a **Chevalley basis**. Computing the structure constants as in [CMT04,CHM08], we can construct $L(G)$ from the root datum in time $O^\sim ((n + \ell)^3 \log(q))$. The action of $G$ on $L$ is given by

\[
h_i(y \otimes t) = h_i, \quad h_i x_\alpha(a) = h_i + (\alpha, f_i) a e_\alpha,
\]

\[
e_\beta(y \otimes t) = t(\beta, y) e_\beta, \quad e_\beta x_\alpha(a) = \sum_{i=1}^{q_{a\beta}} M_{\alpha\beta}^i a^{i e_{\alpha+\beta}},
\]

with $q_{a\beta}$ and $M_{a\beta}^i$ as defined in [CMT04].
Choose simple roots \(\alpha_1, \ldots, \alpha_\ell\), and fix a linear ordering \(\prec\) on \(\Phi^+\) which is compatible with height, i.e., \(h(\alpha) < h(\beta)\) implies that \(\alpha < \beta\). Given a nonsimple positive root \(\xi\), take the positive roots \(\alpha, \beta\) such that \(\xi = \alpha + \beta\) and \(\alpha\) is as small as possible with respect to the ordering on \(\Phi^+\). We call \((\alpha, \beta)\) the extraspecial pair of \(\xi\). We can choose a Chevalley basis of \(L\) so that the integers \(N_{\alpha\beta}\) are positive on extraspecial pairs by [Car72]. We call such a basis a standard Chevalley basis. Note that, as with the normal bases in Section 4.2, the problem of finding a standard Chevalley basis is rational over \(k\).

The linear map \(a\) taking the standard Chevalley basis of \(L(k)\) to a standard Chevalley basis of \(E(k)\) must be an automorphism of \(L(k)\). We now need to find a transformer in \(G\). Define \(G_{\text{ad}}\) as in Section 4.1 and let \(\Gamma\) be the automorphism group of the Dynkin diagram of \(G\). For each element of \(\Gamma\), fix a graph automorphism normalising both \(T_0\) and the Borel subgroup determined by \(\Phi^+\), as in [Car72]. If the characteristic of \(k\) is greater than 3, then it follows from [Hog82] that

\[
\text{Aut}(L(k_{ts})) \cong C(\Gamma \ltimes G_{\text{ad}}(k_{ts})),
\]

where \(C\) is the pointwise stabiliser of \((Z(L) \cap [L, L])(k_{ts})\) inside \(\text{GL}(Z(L)(k_{ts}))\). We can compute a decomposition \(a = zy b\) with \(z \in C\), \(y\) a graph automorphism, and \(b \in G_{\text{ad}}(k_{ts})\) in \(O(d^2)\) operations over \(k_{ts}\) using a slight modification of Algorithm 6 of [CMT04]. Since \(L(k)zy = L(k)\), the element \(b\) is a transformer in \(G_{\text{ad}}\). The dimension of \(L\) is \(O(n + \ell^2)\). Hence Lang’s Theorem can be solved for \(c \in G_{\text{ad}}(k_{ts})\) in time \(O^-(s^2\log(q)^3)\), once we have a standard Chevalley basis for \(E(k)\).

Using the isogeny map \(G \to G_{\text{ad}}\), we can apply Proposition 4.2(2) to obtain 

**Proposition 4.4.** Suppose that \(k\) has characteristic greater than 3. Let \(G\) be a \(k\)-split connected reductive group and let \(L\) be the Lie algebra of \(G\). Let \(m\) be the exponent of the fundamental group of \(G\). Let \(c\) be an element of \(G(k)\) and suppose we are given \(s\), the order of \(e^c = 1\).\(e^c\)\(c\) in \(L\). We can find \(a \in G(k_{ts})\) such that \(c = a^{-1}e^c a\) in Las Vegas time \(O^-(n^3m^2s^2\log(q)^3)\), plus the time needed to find a standard Chevalley basis of \(E(k)\).

We give an algorithm for finding a standard Chevalley basis in the next section. The timing of this algorithm is analysed in Section 6, leading to a proof of Theorem 1.2.

5. Computing a standard Chevalley basis

We now give an algorithm for constructing a Chevalley basis of the Lie algebra \(L\) of a \(k\)-split connected reductive group \(G\). Recall that \(L\) is a \(p\)-Lie algebra [Jac62, Section V.7]. The first and hardest step is finding a \(k\)-split maximal toral \(p\)-subalgebra. This is similar to the algorithm of [dGIR96] for finding a Cartan subalgebra, but ensuring that the subalgebra is \(k\)-split makes things considerably more complex.

Our algorithm only works for fields of characteristic \(p > 3\). Whenever possible we state results for characteristics 2 and 3, in the hope that the gaps in our argument for small \(p\) can be filled later.

We assume that \(L\) is given as a structure constant algebra, but we frequently compute in the adjoint representation. Throughout this section \(n\) denotes the reductive rank of \(G\), \(\ell\) denotes the semisimple rank of \(G\), and \(d\) denotes the dimension of the Lie algebra \(L\). Recall that our Steinberg presentation of \(G\) determines a \(k\)-split maximal torus \(T_0\).

5.1. Toral subalgebras

A Lie algebra \(L\) over a field of characteristic \(p\) is called a \(p\)-Lie algebra if it is equipped with a map \(p : L \to L\), written \(x \mapsto x^p\), satisfying the axioms

\[
(x + y)^p = x^p + y^p + \sum_{i=1}^{p-1} s_i(x, y),
\]

where \(s_i\) are structure constants.
so a maximal toral subalgebra is automatically a k-split subalgebra of the p-Lie algebra of an ak-split connected reductive group G.

Part (1) is proved.

Part (4) is proved.

Part (3) is given in [Hum78, Lemma 8.1] for characteristic zero, but the same proof works for positive characteristic. Part (2) is Corollary 13.5 of [Hum67].

Let \( L \) be the p-Lie algebra of an ak-split connected reductive group G.

\begin{align*}
(ax)^p &= a^p x^p, \\
[x, y^p] &= x(ady)^p,
\end{align*}

where \( x, y \in L, a \in \mathbb{k}, s_i \) is defined in [Jac62, Section V.7], and \( a^p \) and \((ady)^p\) are the usual \( p \)th powers in \( \mathbb{k} \) and the ring of linear maps on \( L \), respectively.

Given values of the p-map on a basis of \( L \), we can compute the values on an arbitrary element using Eqs. (5) and (6). But \( s_p-1 \) involves Lie products of length \( p \), so the time taken for this computation is not polynomial in \( \log(p) \). For our purposes, it suffices to know the value of \( x^p \) up to the centre \( Z(L) \). Given \( x \in L \), we can use (7) to compute the coset \( x^p + Z(L) \) in time \( O^\sim(\ell^6 \log(p) \log(q)) \), since \( \dim(L/Z(L)) = O(\ell^2) \). We also define the q-map by applying the p-map \( e \) times, where \( q = p^e \); values of this map modulo \( Z(L) \) can be computed in time \( O^\sim(\ell^6 \log(q)^2) \).

We say that \( x \in L \) is semisimple if it is contained in the p-subalgebra generated by \( x^p \). A toral subalgebra of \( L \) is a subalgebra defined over \( k \) consisting entirely of semisimple elements. Note that a toral subalgebra need not be a p-subalgebra. However every subalgebra \( H \) of \( L \) is contained in a minimal p-subalgebra called the p-closure of \( H \) in \( L \). The p-closure of a toral subalgebra is toral, and so a maximal toral subalgebra is automatically a p-subalgebra. An \( n \)-dimensional toral p-subalgebra \( H \) is k-split if \( H(k) \) is isomorphic, as a p-Lie algebra, to the vector space \( k^n \) with trivial Lie product and the p-map acting componentwise.

If \( L \) is the Lie algebra of a k-split connected reductive group G, then the values of the p-map on a Chevalley basis are

\[ h_i^p = h_i \quad \text{and} \quad e_\alpha^p = 0, \]

provided that \( p > 3 \). Clearly \( H_0 := L(T_0) = \langle h_1, \ldots, h_n \rangle \) is a k-split toral subalgebra.

We say that the Lie algebra \( L \) is k-split if it contains a maximal toral subalgebra which is k-split. The following theorem collects together the properties of toral subalgebras which we need.

**Theorem 5.1.** Let \( L \) be the p-Lie algebra of a k-split connected reductive group G.

1. \( L \) is k-split with split maximal toral subalgebra \( H_0 \).
2. The centre of \( L \) is a k-split toral subalgebra when \( p > 2 \).
3. Every toral subalgebra of \( L \) is abelian.
4. Every (k-split) maximal toral subalgebra of \( L \) is the Lie algebra of a (k-split) maximal torus of \( G \) (when \( p > 2 \)).
5. The maximal toral subalgebras of \( L \) are G-conjugate.
6. The k-split maximal toral subalgebras of \( L \) are G(k)-conjugate when \( p > 2 \).

**Proof.** In Part (1) it only remains to prove maximality, which follows from [Hum67, Proposition 13.2]. Part (3) is given in [Hum78, Lemma 8.1] for characteristic zero, but the same proof works for positive characteristic. Part (5) is Corollary 13.5 of [Hum67].

We now prove Part (2). Let \( \{e_\alpha, h_i\} \) be a Chevalley basis with respect to \( H_0 \). Suppose that \( z \in Z(L) \) and write

\[ z = \sum_{i=1}^{n} t_i h_i + \sum_{\alpha \in \Phi} a_\alpha e_\alpha. \]

Let \( h_\alpha = \sum_{i=1}^{n} (\alpha, e_i^*) h_i \); then the coefficient of \( e_\alpha \) in \( [z, h_\alpha] \) is \( 2a_\alpha \). Since \( [z, h_\alpha] = 0 \) and \( p > 2 \), we get \( a_\alpha = 0 \). Hence \( z \) is in \( H_0 = \langle h_1, \ldots, h_n \rangle \). Since \( H_0 \) is a split toral subalgebra, \( Z(L) \) is also (The idea for this proof is from [Hog82, Lemma 6.10]).

Every maximal toral subalgebra of \( L \) is the Lie algebra of a maximal torus of \( G \) by [Hum67, Proposition 13.2]. For \( p > 2 \), split tori correspond to split toral subalgebras by [Sel67, Theorem 9]. Hence Part (4) is proved.
From now on we assume $p > 2$. By [Hum67, Proposition 13.6], $T \mapsto L(T)$ gives a one-to-one correspondence between maximal tori of $G$ and maximal toral subalgebras of $L$. Once again, split tori correspond to split toral $p$-algebras. Part (6) now follows from the corresponding result for tori.

**Corollary 5.2.** Given a subalgebra $H$ of $L$ defined over $k$, we can determine if $H$ is $k$-split maximal toral in time $O^-(n^3\ell^4 \log(q)^2)$.

**Proof.** First check that $H$ is abelian of dimension $n$. If so, then compute $Z(L)$ in time $O^-(n + \ell^2)^3 \log(q))$. Note that $H/Z(L)$ has dimension at most $\ell$. By Theorem 5.1(2), it suffices to determine if $H/Z(L)$ is a split toral algebra. This is done by testing whether $b^n + Z(L) = b + Z(L)$ where $b + Z(L)$ runs over a basis of $L/Z(L)$. As we argued at the beginning of this section, this takes time $O^-(\ell^9 \log(q)\ell^2)$ for each basis element. Using the fact that $\ell \leq n$, we get the result. \(\square\)

Since semisimple elements are common in $L(k)$ (see Section 6) and the centraliser of such an element is reductive of rank $n$, we can find a maximal toral subalgebra by Algorithm 5.

The basic idea of our method is to randomly select a series of increasingly split maximal toral subalgebras. We now assign a conjugacy class of $W$ measures how split $G$ the adjoint action of $G$ on $L$ is. See [Leh92] for a more detailed version of this construction. We will denote the adjoint action of $G$ on $L$ by exponentiation. By Theorem 5.1(5) there exists $g \in G(k)$ such that $H = H_0^g$. Note that $H_0^F = H_0$ and $H^F = H$, since both are defined over $k$. Now

$$H_0^F g^{-1} = \left( (H_0^g)^F \right)^{g^{-1}} = (H^F)^{g^{-1}} = H_0^{g^{-1}} = H_0,$$

so $g^F g^{-1}$ is in $N_G(H_0) = N_G(T_0)$. Let $w$ be the image of $g^F g^{-1}$ under projection onto the Weyl group $W = N_G(T_0)/T_0$. The element $w$ is uniquely determined by $H$ up to conjugacy in $W$.

### 5.2. Root decompositions of $L$

The root decomposition of $L$ with respect to $H_0$ is

$$L = H_0 \oplus \bigoplus_{\alpha \in \Phi_k} L_\alpha,$$

where the root space $L_\alpha = \{ b \in L \mid [b, h] = \alpha(h)b \text{ for all } h \in H_0 \}$ and each root $\alpha \in \Phi_k = \Phi(L, H_0)$ is a linear functional $H_0 \rightarrow k$. This decomposition is defined over $k$ by [Sel67, Theorem 6]. When the characteristic $p$ of $k$ is greater than 3 or $p = 3$ and $G$ has no components of type $G_2$ and $A_2$, [Hog82] ensures that each space $L_\alpha$ has dimension one. In this case there is a bijective correspondence between $\Phi_k$ and $\Phi$, the root system contained in $R$.

Let $H$ be a maximal toral subalgebra of $L$, fix $g \in G(k)$ such that $H = H_0^g$ and let $w$ be the image of $g^F g^{-1}$ in $W$. For $\alpha \in \Phi_k$, define $\alpha^g : H \rightarrow k$ by $\alpha^g(h) = \alpha(h^{g^{-1}})$. As $p > 2$, each $\alpha \in \Phi_k$ induces a nonzero map $\alpha^g$ and so the root space decomposition with respect to $H$ is a direct sum.
\textbf{GeneralisedRoots} := \textbf{function}(L, H) \\
let \text{basis} = \{h_1, \ldots, h_n\} be a basis of H \\
let \mathcal{F} = \{\}\ and \define \text{L}(0) = L \\
for i = 1, \ldots, n \ do \\
let \mathcal{F}' = \emptyset \\
for f \in \mathcal{F} \ do \\
compute g, \text{ the characteristic polynomial of } h_i \text{ on } L_f \\
for f_i \text{ an irreducible factor of } g \ do \\
add (f_1, \ldots, f_{i-1}, f_i) \text{ to } \mathcal{F}' \text{ where } f = (f_1, \ldots, f_{i-1}) \\
define L_{(f_1, \ldots, f_i)} = \{x \in L_f | x f_i(\text{ad}(h_i)) = 0\} \\
end for \\
end for \\
let \mathcal{F} = \mathcal{F}' \\
end for \\
remove \{X, \ldots, X\} \text{ from } \mathcal{F} \quad \text{[since } L_{(X, \ldots, X)} = H\} \\
return \mathcal{F} \\
end function


\[ L = H \oplus \bigoplus_{\alpha \in \Phi_k} L_{\alpha^g}, \]

where \( L_{\alpha^g} = \{b \in L | [b, h] = \alpha^g(h)b \text{ for all } h \in H\} = L_{\alpha^g}. \) This decomposition is not defined over \( k \) in general, but certainly over \( k. \) It has \(|\Phi_k|\) components distinct from \( H. \)

Fix a basis \( h_1, \ldots, h_n \) of \( H \) and let \( f = (f_1, \ldots, f_n) \) be a sequence of irreducible polynomials in \( k[X] \) with \( f_i(X) \neq X \) for at least one \( i. \) Define

\[ L_f = \{y \in L | y f_i(\text{ad}(h_i)) = 0 \text{ for } i = 1, \ldots, \ell\}. \] (8)

If \( L_f \neq 0, \) we call \( f \) a \textit{generalised root} and \( L_f \) a \textit{generalised root space}. The \textit{generalised root decomposition} of \( L \) with respect to \( H \) is

\[ L = H \oplus \bigoplus_{f \in \mathcal{F}} L_f, \] (9)

where \( \mathcal{F} = \mathcal{F}(L, H) \) is the set of generalised roots of \( L \) with respect to \( H. \) This decomposition is defined over \( k. \) The generalised roots are computed by Algorithm 6. Complete factorisation of a polynomial of degree \( d \) over \( k \) takes Las Vegas time \( O^\sim(d^2 \log(q)^2) \) by [vzGS92]. Computing the nullspaces \( L_{(f_1, \ldots, f_i)} \) is the dominant contribution to the running time of this algorithm. Since the sum of the degrees of all the \( f_i \) is at most \( nd, \) the algorithm takes time \( O^\sim(nd^3 \log(q)^2). \)

In fact, we do not study this algorithm directly to \( L \), since we want our time to depend on \( \ell \) but not on \( n. \) Rather, we apply it to the quotient of \( L \) by a Lie algebra of its centre. This is necessary for analysing the recursion in Algorithm 8.

Given a generalised root \( f \in \mathcal{F}(L, H), \) the subspace \( L_f \) is a direct sum of components \( L_{\alpha^g} \) of the root decomposition with respect to \( H. \) So we can partition \( \Phi \) into subsets \( \Phi_f \) such that \( L_f = \bigoplus_{\alpha \in \Phi_f} L_{\alpha^g}. \) Define the \textit{degree of } \( f \) to be the lowest common multiple of the degrees of the \( f_i. \)

Given a generalised root \( f, \) we define

\[ f_- = ((-1)^{\text{deg}(f_1)} f_1(-X), \ldots, (-1)^{\text{deg}(f_n)} f_n(-X)). \]

Clearly \( \Phi_{f_-} = -\Phi_f. \) Note that we can have \( f = f_- \) when the degree of \( f \) is greater than one.

We now prove some properties of the sets \( \Phi_f. \)

\textbf{Lemma 5.3.} Suppose \(|\Phi| = |\Phi_k| \) (so \( p > 3 \) or \( p = 3 \) and the type of \( G \) is distinct from \( G_2 \) and \( A_2). \) Let \( f \) be a generalised root of \( L = L(G) \) with respect to \( H. \)
(1) The action of $F$ on $\{L_\alpha^g : \alpha \in \Phi_f\}$ is equivalent to the action of $w$ on $\Phi_f$.

(2) $\Phi_f$ is a union of orbits of $w$ on $\Phi$.

(3) If $\text{deg}(f) = 1$, then $w$ acts trivially on $\Phi_f$. If in addition $q > 3$, then $\Phi_f$ contains a single root.

(4) Suppose $p > 2$. If $\text{deg}(f) = 2$ and $f = f_-$, then $w$ acts on $\Phi_f$ by negation.

**Proof.** Write $g^F g^{-1} = t_w$ for some $t \in T_0$. Now

$$L_\alpha^g F = L_\alpha^g F = L_\alpha^F g F = L_\alpha^g = L_\alpha^t w g = L_\alpha w^g = L_{\alpha w}^g,$$

and so Part (1) is proved. Part (2) follows since $L_f^F = L_f$.

Part (3) holds because $L_f$ is a root space when $\text{deg}(f) = 1$.

Suppose $\text{deg}(f) = 2$ and $f = f_-$. Let $\alpha \in \Phi_f$. Then $L_{\alpha F}^F = L_{(\alpha w)^g}$ and so $(\alpha w)^g(h_i)$ and $\alpha^g(h_i)$ are conjugate roots of $f_i$. But if $\text{deg}(f_i) = 2$, then $f = f_-$ implies that the conjugate roots are negatives of each other. And if $\text{deg}(f_i) = 1$, then $f = f_-$ implies that the only root of $f_i$ is zero. In either case $(\alpha w)^g(h_i) = -\alpha^g(h_i)$ and so $w$ acts on $\Phi_f$ by negation. □

5.3. Fundamental subalgebras

Now that we have the generalised root decomposition of $L$ with respect to $H$, we consider the subalgebra generated by a generalised root space $L_f$. Such subalgebras often turn out to be fundamental in the following sense.

We define a (split) fundamental subgroup of $G$ as a connected reductive subgroup normalised by a (split) maximal torus. A subalgebra $M$ of $L$ is (split) fundamental if it is normalised by a (split) maximal toral subalgebra of $L$.

**Lemma 5.4.** Let $\Psi$ be a closed subsystem of $\Phi$ and $H$ a maximal toral subalgebra of $L$. Then there is a fundamental Lie subalgebra of $L$ with root system $\Psi$ normalised by $H$.

**Proof.** There exists $g \in L$ such that $H = H_0 g$. Put $M = H + \sum_{\alpha \in \Psi} L_\alpha^g$. Then $M$ is a subalgebra of $L$ normalised by $H$. □

The most important properties of such algebras for our purposes are

**Theorem 5.5.** Suppose $p > 2$. Let $M$ be a subalgebra of $L$ normalised by the maximal toral subalgebra $H$.

(1) $M \cap H$ is a maximal toral subalgebra of $M$.

(2) The subspace $H + M$ of $L$ is the Lie algebra of a closed connected algebraic subgroup $G_M$ of $G$.

**Proof.** We have $H \leq C_{M+H}(H) \leq C_L(H) = H$, so $M + H$ has root decomposition

$$M + H = H \oplus \bigoplus_\beta M_\beta,$$

where $\beta$ runs over $\Phi(M + H, H)$, the set of roots of $M + H$ with respect to $H$. Suppose $m + h \in M_\beta$ where $m \in M$ and $h \in H$. Then, for all $h' \in H$, $[m, h'] = [m + h, h'] = \alpha(h')(m + h)$. But $[m, h'] \in M$, and so $h \in M$ and $M_\beta \leq M$. So, by intersecting (10) with $M$, we obtain the root decomposition

$$M = (H \cap M) \oplus \bigoplus_\beta M_\beta,$$

and so $H \cap M$ is a maximal toral subalgebra of $M$ and (1) is proved.
As for (2), \( H \) normalises \( M \), so the subspace \( H + M \) is a Lie subalgebra of \( L \). By Theorem 5.1(4), there is maximal torus \( T \) of \( G \) whose Lie algebra coincides with \( H \). For each \( \beta \in \Phi(M + H, H) \) as above, there is a root group \( T_\beta \) in \( G \) with respect to \( T \) whose Lie algebra is \( M_\beta \). The product of all \( T_\beta \) for \( \beta \in \Phi(M + H, H) \) and \( T \) is a closed connected algebraic subgroup of \( G \) with Lie algebra \( M + H \). This settles the theorem. \( \square \)

Recall that the closure \( \overline{\Psi} \) of \( \Psi \subseteq \Phi \) is just the set of all roots that can be written as a sum of elements of \( \Psi \). Note that if \( \overline{\Psi} \) is also closed under negation, it is a subsystem. If \( \overline{\Psi} \) is a subsystem, we say \( w \in W \) is inner on \( \overline{\Psi} \) if the action of \( w \) on \( \overline{\Psi} \) is induced by an element of \( W(\overline{\Psi}) \).

**Lemma 5.6.** Suppose \(|\Phi| = |\Phi_k|\). Let \( M \) be the subalgebra generated by \( \sum_{\alpha \in \Psi} L_\alpha s \), where \( \Psi \) is a \( w \)-invariant subset of \( \Phi \).

1. If \( \Psi \) is a single \( w \)-orbit, then either \( \overline{\Psi} \) is a subsystem of \( \Phi \) or \( M \) is soluble.
2. If \( \overline{\Psi} \) is a subsystem and \( w \) is inner on \( \overline{\Psi} \), then \( M \) is split fundamental.

**Proof.** Since \( [\sum_{\alpha \in \Psi} L_\alpha s, H] \leq \sum_{\alpha \in \Psi} L_\alpha s \), we have \([M, H] \leq M\) and so \( M \) is normalised by \( H \). Since \([L_\alpha, L_\beta] \leq L_{\alpha + \beta}\) (recalling that \( L_0 = H \)), we have

\[
M = (H \cap M) \oplus \bigoplus_{\alpha \in \overline{\Psi}} L_\alpha s.
\]

Let \( \Psi = \Psi_1 \cup \ldots \cup \Psi_m \) be the finest decomposition of \( \Psi \) into pairwise orthogonal subsets. Then \( \overline{\Psi} = \overline{\Psi}_1 \cup \ldots \cup \overline{\Psi}_m \) is also an orthogonal decomposition. Clearly \( w \) permutes the sets \( \Psi_i \) and, since \( w \) is transitive on \( \Psi_i \), it must be transitive on \( \overline{\Psi}_i \). Since \( -\overline{\Psi}_1 \) is never orthogonal to \( \overline{\Psi}_1 \), either we have \(-\overline{\Psi}_1 = \overline{\Psi}_1\) or \(-\overline{\Psi}_1\) is disjoint from \( \overline{\Psi}_1 \). By the transitivity of \( w \), whichever of these cases holds for \(-\overline{\Psi}_1\), also holds for all \(-\overline{\Psi}_i\). In particular, \( \overline{\Psi} \) is closed under negation iff \( \overline{\Psi}_1 \) is. Let \( \psi \) be the sum of all the elements of \( \overline{\Psi}_1 \). Now \( \overline{\Psi}_1 \) is closed under negation iff \( \psi = 0 \) (since \( \psi = 0 \) implies \(-\alpha = \sum_{\beta \in \overline{\Psi}_1, \beta \neq \alpha} \beta \in \overline{\Psi}_1 \) for all \( \alpha \in \overline{\Psi}_1 \), and the converse is trivial). We define \( M_i = H_i \oplus \bigoplus_{\alpha \in \overline{\Psi}_i} L_\alpha s \), where \( H_i \) is the subalgebra of \( H \) generated by \([L_\alpha s, L_{-\alpha} s]\) for all \( \alpha \in \overline{\Psi}_i \). Note that \( M = \bigoplus_i M_i \).

Suppose first that \( \psi \neq 0 \). Then the root subsystem generated by \( \Psi_1 \) is just \( \overline{\Psi}_1 \cup -\overline{\Psi}_1 \). Since this root subsystem is irreducible, \( \psi \) induces an ordering on it which makes \( \overline{\Psi}_1 \) the set of positive roots. Hence \( M_1 \) is contained in the Borel subalgebra of the Lie algebra of a simple group, and so must be soluble. The transitivity of \( w \) on the sets \( \overline{\Psi}_i \) implies that \( M_i \) is soluble for every \( i \), and so \( M = \bigoplus_i M_i \) is soluble. If \( \psi = 0 \), then \( \overline{\Psi}_1 \) is an irreducible root subsystem and so \( \Psi \) is a root subsystem of \( \Phi \). Part (1) is now proved.

Now suppose that \( \overline{\Psi} \) is closed under negation and \( w \) is inner on \( \overline{\Psi} \). By Lang's Theorem applied to \( M + H \), cf. Theorem 5.5(2), we can find \( h \in G_M \) such that \( h^F h^{-1} = \hat{w} \). On the other hand, \( g \) satisfies \( g^F g^{-1} = t \hat{w} \) for some \( t \in T_0 \). Now the map \( \hat{w} F \) is a nonstandard Frobenius endomorphism since \( \hat{w} F = \hat{w} \) and so \((\hat{w} F)^m = F^m \), where \( m \) is the order of \( \hat{w} \). Furthermore \( T_0 \hat{w} F = T_0 \). So, by Lang's Theorem in \( T_0 \), there is a \( u \in T_0 \) such that \( t = u^{\hat{w} F} u^{-1} \). Set \( \hat{g} = u^{-\hat{w} F} g \), so that

\[
\hat{g}^F \hat{g}^{-1} = u^{-\hat{w} F} g^F g^{-1} u^{\hat{w} F} t u \hat{w} = \hat{w}
\]

and \( H_0^\hat{g} = H_0^{\hat{w}^{-1} u^{-1} \hat{w}} g = H_0^g = H \). Hence \( h^F h^{-1} = \hat{g}^F \hat{g}^{-1} \), that is \( \hat{g} h^{-1} \) is defined over \( k \) and so \( H^{h^{-1}} = H_0^h h^{-1} \) is split. So

\[
[M, H^{h^{-1}}] = [M^h, H]^{h^{-1}} = [M, H]^{h^{-1}} \leq M^{h^{-1}} = M,
\]

which shows that \( M \) is split fundamental. \( \square \)
We will apply the lemma to the Lie subalgebra of $L$ generated by $L_f$; here $\Psi = \Phi_f$ as defined in (8). It is $w$-invariant according to Lemma 5.3(2).

5.4. Finding a split maximal toral subalgebra

We begin with the smallest simple Lie algebras known: those of type $A_1$, that is, isogenous to $\mathfrak{sl}_2$. As $p$ is odd, there is in fact only one isomorphism class of such Lie algebras for each $k$. An advantage of this type is that each involution induced on a subroot system of this type is inner, so Lemma 5.6(2) applies. We indicate how to find a split maximal toral subalgebra in such an algebra and provide a timing analysis. The timings for the general case will be dealt with in Section 6.4.

Lemma 5.7. Let $M$ be a Lie algebra of type $A_1$ and reductive rank 1 over $k$, with $q = |k|$ odd, $q \geq 5$. Then there are $q^3 - q^2$ nonzero semisimple elements in $M$. Of these, exactly $\frac{1}{2}(q^3 - q)$ have a characteristic polynomial that factorises completely into linear terms. In particular, we can find a split maximal toral subalgebra of $M$ in Las Vegas time $O^\sim(\log(q)^2)$.

Proof. As the characteristic of $k$ is distinct from 2, each Lie algebra of type $A_1$ and reductive rank 1 over $k$ is isomorphic to the standard Lie algebra of $A_1$ over $k$. Therefore, without loss of generality, we may assume that $M$ is the Lie algebra of $2 \times 2$ matrices over $k$ having trace 0. In this model the counts for semisimple elements are easily verified.

Algorithm 7 gives an explicit description of a Las Vegas algorithm for finding a split maximal toral subalgebra of $M$. It uses the characterisation of semisimple elements as those whose minimal polynomial is squarefree. As the minimal polynomial of $\text{ad}(x)$ for $x \in M$ has degree at most 3 with one factor equal to $X$, the hardest part of the factorisation can be reduced to finding the square root of an element in $k$. Hence, computations can be carried out in time $O^\sim(\log(q)^2)$.

According to the count of split semisimple elements above, by a single choice of $x \in M$ in Algorithm 7 we obtain a split maximal toral subalgebra of $M$ with probability at least

$$\frac{q^3 - q}{2q^3} = \frac{1}{2} \left(1 - \frac{1}{q^2}\right) \geq \frac{12}{25}.$$ 

This shows that the Las Vegas time is also $O^\sim(\log(q)^2)$. \[]

The probability estimate in the above proof is a special case of the lower bound in Proposition 6.1 below.

Suppose now that we have found a nontrivial split fundamental subalgebra $M$ of type $A_1$. The following proposition shows that we can use recursion to find a split maximal toral subalgebra of $L$.

Proposition 5.8. Suppose $p > 2$. Let $M$ be a split fundamental subalgebra of $L$ of type $A_1$. Let $K$ be a split maximal toral subalgebra of $M$. Then $C_L(K)$ is a split fundamental subalgebra of $L$. Moreover, it is the Lie algebra of the $k$-split closed reductive subgroup $C_G(K)$ of $G$ of reductive rank $n$.

Proof. Let $H$ be a split maximal toral subalgebra of $L$ that normalises $M$. Let $G_M$ be the split fundamental subgroup of $G$ defined in Theorem 5.5(2). By construction, the maximal torus $T$ corresponding to $H$ (cf. Theorem 5.1(4)) normalises $G_M$ and so $H$ normalises $M$. Moreover, by Theorem 5.5(1), $H \cap M$ is a split maximal toral subalgebra of $M$. By Theorem 5.1(6), there is a conjugator $g'$ in $G_M(K)$ so that
\textbf{SplitMaximalToralSubalgebra} := \textbf{function} (L, Z) \\
\textbf{end function}

\begin{algorithm}
\textbf{repeat}
\textbf{end if}
\textbf{end function}
\end{algorithm}

We now have a method for finding split maximal toral subalgebras of $L$, as documented in Algorithm 8. Let $p > 3$.

For the sake of efficiency, we take $Z = Z(L)$ initially (the algorithm can also be invoked with $Z = \{0\}$). Let us argue why. By Theorem 5.1(2), the centre $Z(L)$ of $L$ is contained in $H$. Moreover, by (9), there is a basis $h_1, \ldots, h_r$ for $H(k)$ such that, for some $r \leq n$, $Z = \langle h_1, \ldots, h_r \rangle$ is central. Extend this to a basis of $L(k)$. Let $\phi$ be the pullback map $L/Z \rightarrow L$ via this basis. We compute in $L/Z$, since it has dimension $O(\ell^2)$ independent of $n$, and the results are then transferred into $L$ via $\phi$. Let $\mathcal{F}$ be the set of generalised roots of $L/Z(L)$ with respect to $H/Z(L)$. Given $f = (f_1, \ldots, f_m) \in \mathcal{F}$ define the sequence $f' = (X, \ldots, X, f_1, \ldots, f_m)$ of length $n$. It is now easy to see that $\phi((L/Z)f) = Lf'$. Hence the generalised root space decomposition of $L/Z$ with respect to $H$ follows immediately once we have the decomposition of $L/Z$ with respect to $H/Z$. Since the dimension of $L/Z$ is $O(\ell^2)$, the generalised root space decomposition of $L/Z$ can be computed in time $O^\ast(\ell^7 \log(q)^2)$.

Working modulo $Z$, Algorithm 8 finds a maximal toral subalgebra $H$ of $L$ by use of Algorithm 5. If it is split, we are done. Otherwise, we continue by computing its generalised roots $\mathcal{F}$.

Assume $\deg(f) \leq 1$ or $\deg(f) = 2$ and $f = f_\cdot$ for some $f \in \mathcal{F}$. Then $M_f(k) = (L_f(k) + L_{f_\cdot}(k))$ is a subalgebra of type $A_1$ normalised by $H$. For $\deg(f) = 1$, this is immediate from Lemma 5.3(3), so, in order to see this, assume $\deg(f) = 2$ and $f = f_\cdot$. If $i$ is such that $\deg(f_i) = 2$, then $f_i = X^2 - a_i$ for some $a_i \in k$, and so $f_i$ factors into linear terms over $k_2$, whereas $f_i = X$ if $\deg(f_i) = 1$; therefore, $M_f(k_2)$ is generated by $L_f(k_2) = L_X(k_2) + L_{-X}(k_2)$ for some linear form $X$ on $H(k_2)$ (with both $L_X$ and $L_{-X}$ of dimension 1 as $p > 3$); as $w$ interchanges $L_X$ and $L_{-X}$, it is inner on $\{X, -X\}$ and so Lemma 5.6(2) shows that the Lie algebra $M_f(k_2)$ is of type $A_1$.

We continue with $f \in \mathcal{F}$ as above. A pair of linearly independent nilpotent elements in $M_f$ can be transformed, by an element of $G(k)$, to a pair of elements $e_\alpha, e_{-\alpha}$ of the standard Chevalley basis for some $\alpha \in \Phi$. Hence, there is an element $g' \in G(k)$ so that $M_f = (e_\alpha, e_{-\alpha})g'$. Now $M_f$ is normalised by the split maximal toral subalgebra $H^{g'}$ of $L$, so it is a split fundamental subalgebra of $L$. If $\deg(f) = 1$, then $K = H \cap M$ is a split maximal toral subalgebra of $M$; if $\deg(f) = 2$ and $f = f_\cdot$, a split maximal toral subalgebra $K$ of $M$ is found by Algorithm 7.

By Proposition 5.8, a split maximal toral subalgebra of the Lie algebra $C_L(K)$ of the reductive group $C_G(K)$ has rank $n$ and so is also a split maximal toral subalgebra of $L$. Since $K$ is contained in the centre of $C_L(K)$, the recursion with $(C_L(K), K)$ instead of $(L, Z)$ is valid. At each recursive call, the rank of $Z$ has increased, so the total number is at most $\ell$ if we start with $Z = Z(L)$ and $n$ if we start with $Z = \{0\}$. 

$K = (H \cap M)^{g'} = H^{g'} \cap M$. But then $H^{g'}$ is a split maximal toral subalgebra of $L$ containing $K$. As $H^{g'}$ is abelian, it follows that $H^{g'}$ is a split maximal toral subalgebra of $L$ contained in $C_L(K)$.

By [Hum75, Corollary 26.2A], $C_L(K)$ is a reductive group. It is normalised by $T^{g'}$ and so it is $k$-split fundamental. Also, $L(C_G(K)) = C_L(K)$ by [Spr98, Theorem 4.4.4].
Finding a standard Chevalley basis

We now show how to find a standard Chevalley basis for \( L(k) \), as defined in Section 4.3. We assume that we have been given a root datum \((X, \Phi, Y, \Phi^\ast)\) for the split connected reductive group \( G \) with Lie algebra \( L \). Our computations use the root datum, but not the group.

Let \( H \) be a \( k \)-split maximal toral subalgebra of \( L \) computed as in Section 5.4. The root decomposition

\[
L = H \oplus \bigoplus_{\alpha \in \Phi_k} L_\alpha
\]

can be computed by linear algebra over \( k \). The identification of \( \Phi_k \) with \( \Phi \) can be found by computing simple roots for each system and reordering the roots so that the Cartan matrices are identical. The details are given in [dG00, Chapter 5] for characteristic zero, but the method is identical in our case.

Fix dual bases \( e_1, \ldots, e_n \) for \( X \) and \( f_1, \ldots, f_n \) for \( Y \). Let \( \alpha_1, \ldots, \alpha_\ell \) be simple roots of \( \Phi \). Then Algorithm 9 can be used to find elements \( e_\alpha \) in each \( L_\alpha \) satisfying (4) of Section 4.3. We take the \( N_{\alpha\beta} \) as in a standard Chevalley basis (Section 4.3). So, for each extraspecial pair \((\alpha, \beta)\), we have \( 0 < N_{\alpha\beta} \leq 3 \) and hence division by \( N_{\alpha\beta} \) is not a problem.

Finding a basis \( h_1, \ldots, h_n \) of \( H(k) \) satisfying Eqs. (2) and (3) is just a matter of solving linear equations in \( n^2 \) variables. We conclude

**Lemma 5.9.** Algorithm 9 finds a standard Chevalley basis in time \( O(n^6 \log(q)^2) \) plus the time to compute the split maximal toral subalgebra \( H \).

6. Reflection derangements and time analysis

Let \( L \) be the Lie algebra of the \( k \)-split connected reductive linear algebraic group \( G \). We now find bounds on the probability of finding a maximal toral subalgebra \( H \leq L \) and a set \( A \) of generalised roots such that \( M_A \) is known to be split fundamental. To simplify our analysis, we just bound the probability that Algorithm 5 finds a maximal toral subalgebra in a single step, or equivalently that the random element chosen is regular semisimple. Section 6.1 gives bounds on the frequencies of regular semisimple elements corresponding to Weyl group elements. In Section 6.2, we bound the proportion of suitable Weyl group elements. We give the proof of Theorem 1.2 in Section 6.4.

Throughout this section, \( n \) is the reductive rank of \( G \), \( \ell \) is the semisimple rank of \( G \), \( d \) is the dimension of \( L \), and \( d_1, \ldots, d_\ell \) are the invariant degrees of \( G \) as defined in [Car72, Section 9.3].
6.1. Regular semisimple elements

An element of $L$ is regular semisimple if its centraliser is a maximal toral subalgebra. For any subvariety $S$ of $L$, let $S_{rss}$ be the variety of regular semisimple elements in $S$. Recall from Section 5.1 that the maximal toral subalgebras of $L$ are classified up to $G(k)$-conjugacy by the conjugacy classes of $W$. Fix $w$ in $W$ and let $L_{rss,w}$ be the set of elements $x \in L$ which are regular semisimple and such that there exists $g \in G$ with $C_L(x) = H_0^g$ and $g^T_0 g^{-1} \in T_0 w$. Although we give direct proofs, many results in this section also follow from Gus Lehrer’s analysis of hyperplane complements [Leh92, Leh98].

The following result bounds our chances of finding a regular semisimple element in $L(k)$ whose centraliser corresponds to the $W$-class of a given $w$.

**Proposition 6.1.** Let $L$ be the Lie algebra of a $k$-split connected reductive group $G$ with root datum $(X, \Phi, Y, \Phi^*)$. Let $w$ be an element of the Weyl group $W$. Define

$$Q_w(x) = \prod_{i=1}^\ell (1 - x^{c_i}) \in \mathbb{Q}(x).$$

Then

$$\left(1 - \sum_{i=1}^\ell \frac{c_i}{q^i}\right) Q_w(1/q) \frac{|W^w|}{|W|} \leq \frac{|L_{rss,w}(k)|}{|L(k)|} \leq Q_w(1/q) \frac{|W^w|}{|W|},$$

where $c_i = c_i(w)$ is the number of $w$-orbits in $\Phi$ consisting of roots $\alpha$ with the property that $i$ is the largest integer for which $\alpha, \alpha w, \ldots, \alpha w^{i-1}$ are $k$-linearly independent.

**Proof.** Fix some $g \in G$ such that $g^T_0 g^{-1} = \hat{w}$ and define $H_w = H_0^g$. Let $T_w = T_0^g$ so that $L(T_w) = H_w$. Then

$$L_{rss,w}(k) = \{x \in L_{rss}(k) \mid x \in H_w(k)^h \text{ for some } h \in G(k)\},$$

which is in one-to-one correspondence with

$$\{ (x, H) \in L_{rss}(k) \times H_w(k)^{G(k)} \mid x \in H \}.$$

Since $N_{G(k)}(H_w(k))/T_w(k) \cong C_W(w)$, we have $|H_w(k)^{G(k)}| = |G(k)|/|T_w(k)| |C_W(w)|$. Hence

$$\frac{|L_{rss,w}(k)|}{|L(k)|} = \left| (H_w)_{rss}(k) \right| \frac{|G(k)|}{|L(k)||T_w(k)|} \frac{|W^w|}{|W|}.$$

Given a root $\alpha \in \Phi$, define

$$H_\alpha = \{ h \in H_w \mid \alpha^g(h) = 0 \}.$$

Then $H_\alpha$ is a hyperplane in $H_w$ and $(H_w)_{rss} = H_w - \bigcup_{\alpha \in \Phi} H_\alpha$. Now $H_\alpha^\perp = H_{\alpha^\perp}$, so $H_\alpha(k) = (\bigcap_{\alpha \in \Phi^w} H_\alpha)(k)$. This space has codimension $i$, the largest integer such that $\alpha, \alpha w, \ldots, \alpha w^{i-1}$ are linearly independent. So, for each $i = 1, \ldots, \ell$, we are removing $c_i$ subspaces of codimension $i$ from a $k$-space of dimension $n$. Hence

$$q^n \left(1 - \sum_{i=1}^\ell \frac{c_i}{q^i}\right) \leq \left| (H_w)_{rss}(k) \right| \leq q^n.$$
Using Theorem 9.4.10 of [Car72] and the fact that our group is untwisted, we get

\[ |G(k)| = q^d \prod_{i=1}^{\ell} \left( 1 - \frac{1}{q^{d_i}} \right). \]

Using Proposition 3.3.5 of [Car93] and the fact that \( F \) is the standard Frobenius, we find that \( T_w(k) \) has order \( \det_Y(qI - w) \). Hence

\[ |G(k)| \mid L(k) \mid T_w(k) \mid = \frac{q^d \prod_{i=1}^{\ell} (1 - 1/q^{d_i})}{q^d \det_Y(qI - w)} = \frac{Q_w(1/q)}{q^n}. \]

6.2. Reflection derangements

Recall from Section 5.2 that there is a relationship between the generalised roots \( f \) with respect to a maximal toral subalgebra and the orbits of the corresponding Weyl group element \( w \) on \( \Phi \). This relationship need not be a one-to-one correspondence. As we saw in Lemma 5.3(3) and (4), this relationship is almost a one-to-one correspondence when the degree of \( f \) is one, or the degree is two and \( f = f_- \). This happens when there is a root \( \alpha \) such that \( \alpha w = \pm \alpha \). In other words, when a reflection \( s_\alpha \) is fixed under conjugation by \( w \).

In this section, we count the number of Weyl group elements of this kind. Given a permutation representation of a group, an element of the group is called a derangement with respect to the representation if it fixes no points at all. The proportion of derangements of the symmetric group \( \text{Sym}_t \) acting on \( t \) letters is known to approach \( 1/e \) as \( t \to \infty \). We give similar results for a Weyl group acting on its reflections by conjugation. We refer to these elements as reflection derangements. We are grateful to Anthony Henderson for helping us with the proof of this proposition.

**Proposition 6.2.** If \( W \) is an irreducible Coxeter group of classical type \( A_\ell, B_\ell/C_\ell \), or \( D_\ell \), then the proportion of its reflection derangements approaches \( 2e^{-3/2}, e^{-5/4} \), or \( 2e^{-5/4} + (4e)^{-1} \), respectively, as \( \ell \to \infty \). For exceptional types, the proportions are as listed below:

<table>
<thead>
<tr>
<th></th>
<th>( G_2 )</th>
<th>( F_4 )</th>
<th>( E_6 )</th>
<th>( E_7 )</th>
<th>( E_8 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( G_2 )</td>
<td>1/3</td>
<td>1/4</td>
<td>1409/2592</td>
<td>1646/2835</td>
<td>3385549/6220800</td>
</tr>
</tbody>
</table>

**Proof.** Denote by \( f \) the number of reflection derangements of \( W \). We wish to determine \( f / |W| \).

**Type \( A_\ell \):** The Weyl group \( W(A_\ell) \) can be identified with the symmetric group \( \text{Sym}_{\ell+1} \) on \( \ell + 1 \) letters. Write \( m = \ell + 1 \) and write \( d_m \) for the proportion of permutations in \( \text{Sym}_m \) without fixed points in \( \{1, \ldots, m\} \). Denote by \( R_m \) the set of all permutations in \( \text{Sym}_m \) with at most one fixed point in \( \{1, \ldots, m\} \).

An element of \( \text{Sym}_m \) does not fix a reflection if, and only if, it belongs to \( R_m \) and does not contain a transposition \( (i, j) \) in its cycle decomposition. So

\[ f = \left| R_m - \bigcup_{1 \leq i < j \leq m} R_m^{i,j} \right|. \]

where

\[ R_m^{i,j} = \{ w \in R_m \mid w \text{ contains } (i, j) \}. \]
We compute $f$ by inclusion/exclusion. As $R_{ij}^m$ and $R_{ij}^{m'}$ intersect trivially for $j \neq j'$ we can find $f$ as an alternating sum over $h$-tuples of commuting transpositions:

$$\sum_{h=0}^{\lfloor m/2 \rfloor} (-1)^h \binom{m}{2h} \frac{(2h)!}{2^h h!} |R_{m-2h}|.$$ 

Since, clearly, $|R_m| = d_m + md_{m-1}/m$,

$$f = m! \sum_{h=0}^{\lfloor m/2 \rfloor} \left(-\frac{1}{2}\right)^h \frac{1}{h!} (d_{m-2h} + d_{m-2h-1}).$$

As $\lim_{m \to \infty} d_m = 1/e$, the required proportion tends to

$$\lim_{m \to \infty} \frac{f}{m!} = \sum_{h=0}^{\infty} \left(-\frac{1}{2}\right)^h \frac{1}{h!} \frac{2}{e} = e^{-\frac{1}{2}} \frac{2}{e} = 2e^{-\frac{3}{2}}.$$

**Types $B_\ell$ and $C_\ell$:** The Weyl group $W = W(B_\ell) = W(C_\ell)$ can be identified with the group of all permutations $w$ of $\{\pm 1, \ldots, \pm \ell\}$ such that $(-i)w = -(iw)$. Define the homomorphism $\phi : W \to \text{Sym}_\ell$ by $iw^\phi = |iw|$. Then $w \in W$ fixes no reflections if, and only if, $w^\phi$ is a derangement of $\text{Sym}_\ell$ and, for every transposition $(i, j)$ contained in the cycle decomposition of $w^\phi$, either $(i, j, -i, -j)$ or $(j, i, -j, -i)$ is contained in the cycle decomposition of $w$.

Writing $S_\ell$ for elements of $W$ such that $w^\phi$ is a derangement and $S_{ij}^\ell = \{w \in S_\ell \mid w \text{ contains } (i, j)(-i, -j) \text{ or } (i, j)(-i, j)\}$, we find that

$$f = \left| S_\ell - \bigcup_{1 \leq i < j \leq \ell} S_{ij}^\ell \right|.$$ 

Again, we can count $f$ by taking alternating sums over $h$-tuples of commuting transpositions in $W^\phi$. As each transposition in the decomposition of an element of $w^\phi$ corresponds to two 4-cycles as indicated above, we find an extra factor $2^h$ compared to the $A_\ell$ case:

$$\sum_{h \geq 0, 2h \leq \ell} (-1)^h \binom{\ell}{2h} \frac{(2h)!}{2^h h!} 2^h |S_{\ell-2h}|.$$ 

As $|S_\ell| = 2^\ell \ell!d_\ell$,

$$f = \sum_{h \geq 0, 2h \leq \ell} (-1)^h \frac{\ell!}{h!} 2^{\ell-2h} d_{\ell-2h}.$$ 

As $\lim_{m \to \infty} d_m = 1/e$ and $|W(B_\ell)| = 2^\ell \ell!$, the required proportion tends to

$$\lim_{m \to \infty} \frac{f}{2^\ell \ell!} = \sum_{h=0}^{\infty} \left(-\frac{1}{4}\right)^h \frac{1}{h!} \frac{1}{e} = e^{-\frac{1}{4}} e^{-1} = e^{-\frac{3}{4}}.$$
Type $D_\ell$: The Weyl group $W(D_\ell)$ is the subgroup of $W(B_\ell)$ consisting of all elements $w$ such that $\prod_{i=1}^\ell i w$ is positive. In cycle notation, this means that $w$ has an even number of negative cycles (that is, cycles in which both positive and negative numbers occur).

Define $\phi : W \to \text{Sym}_\ell$ as the restriction of the map for type $B_\ell$. Then $w \in W$ does not commute with any reflection if, and only if,

(i) $w^\phi$ fixes at most one element of $\{1, \ldots, \ell\}$ and, for every transposition $(i, j)$ contained in the cycle decomposition of $\phi(w)$, the cycle occurring in $w$ is $(i, j, -i, -j)$ or $(j, i, -j, -i)$; or

(ii) $w^\phi$ has exactly two fixed points, say $i$ and $j$, and the cycle decomposition of $w$ contains $(i, -i)(j, -j)$ or $(i)(j, -j)$.

The number of elements of the type (ii) is clearly $\left(\frac{\ell}{2}\right) d_{\ell-2} 2^{\ell-2} (\ell - 2)!$, contributing

$$\lim_{\ell \to \infty} \frac{\left(\frac{\ell}{2}\right) 2^{\ell-2} d_{\ell-2} (\ell - 2)!}{|W(D_\ell)|} = \lim_{\ell \to \infty} 2^{-2} d_{\ell-2} = \frac{1}{4e}$$

to the required asymptotic proportion.

Writing $T_\ell$ for elements of $W$ such that $w^\phi$ fixes at most two elements and

$$T_{\ell}^{i,j} = \{ w \in T_\ell \mid w \text{ contains } (i, j)(-i, -j) \text{ or } (i, -j)(j, -i) \},$$

we find that the set of elements of type (i) is

$$T_\ell = \bigcup_{1 \leq i < j \leq \ell} T_\ell^{i,j}.$$

Again, we take alternating sums over $h$-tuples of commuting transpositions in $\phi(W)$. As each transposition in the decomposition of an element of $\phi(w)$ corresponds to two 4-cycles as indicated above, we find the same factor $2^h$ as for the $B_\ell$ case:

$$\sum_{h=0}^{[\ell/2]} (-1)^h \frac{\ell!}{(2h)!} 2^h h! 2^h |T_\ell-2h|.$$ 

As $|T_\ell| = 2^{\ell-1} \ell! (d_{\ell} + d_{\ell-1})$, the result is

$$\sum_{h=0}^{[\ell/2]} (-1)^h \frac{1}{4} (d_{\ell-2h} + d_{\ell-2h-1}),$$

which contributes

$$\lim_{m \to \infty} \frac{f}{2^m m!} = \sum_{h=0}^{\infty} (-1)^h \frac{1}{h!} \frac{1}{e} = 2e^{-1} e^{-1} = 2e^{-2}$$

to the required proportion. Hence, the asymptotic proportion is $(4e)^{-1} + 2e^{-5/4}$.

The exceptional types: These were computed by machine.
Corollary 6.3 (Theorem 1.5). The proportion of reflection derangements in a Weyl group is less than $\frac{2}{3}$.

Proof. Recall that if $a_n > 0$ converges monotonically to zero, then $\sum_{i=0}^{\infty} (-1)^i a_i$ is called an alternating series. The maximum value of the partial sums $s_n = \sum_{i=0}^{n} (-1)^i a_i$ of such a series is one of the first two partial sums. Since the series in the proof of the previous proposition are sums of alternating sequences, it is always possible to find a constant $M$ such that the maximum value of the partial sums is one of $s_1, \ldots, s_M$. It is now easy to show on a case-by-case basis that the proportion of reflection derangements in an irreducible Weyl group is at most $\frac{2}{3}$.

If $W$ is a direct product decomposition into $s$ irreducible Weyl groups, then an element of $W$ is a reflection derangement if and only if each component of $w$ is a reflection arrangement, and so their proportion is at most $\left(\frac{2}{3}\right)^s \leq \frac{2}{3}$.

Together with Proposition 6.1, this shows that the chance of finding a regular semisimple element of $L$ corresponding to a reflection nonderangement in the Weyl group is at least one third, provided $q$ is large enough. To complete the analysis, we need a more precise bound on the probability of finding such regular semisimple elements.

6.3. Bounds on the number of particular semisimple elements

The following useful lemma can be proved by elementary calculus.

Lemma 6.4. Let $a_1, \ldots, a_m$ be a sequence of nonnegative integers and suppose that no integer appears more than a times in this sequence. Then

$$\prod_i \left( 1 - \frac{1}{q^a} \right) \geq \left( 1 - \frac{1}{q} \right)^{2a}.$$  

We now start by looking at the Coxeter class in the Weyl group. The Coxeter element is actually a reflection derangement, but this proof is the model for our next result.

Proposition 6.5. Suppose that $W$ is an irreducible Weyl group. If $w_c$ is a Coxeter element of $W$, then

$$|L_{\text{rss}}, w_c(k)| \geq \left( 1 - \frac{\ell}{q^{\ell/2}} \right) \left( 1 - \frac{1}{q} \right)^{4} \frac{1}{h},$$

where $h$ is the order of $w_c$.

Proof. Suppose $\alpha$ is a root and $\alpha w_c^m$ is a linear combination of $\alpha, \alpha w_c, \ldots, \alpha w_c^{m-1}$. We prove that $m \geq \ell/2$ on a case-by-case basis:

Type $A_\ell$: Identify $W$ with $\text{Sym}_{\ell+1}$ and consider $\Phi$ to consist of roots $e_i - e_j$ with $i \neq j$. We can take $w_c = (1, 2, \ldots, \ell + 1)$ and $\alpha = e_i - e_j$. So $\alpha w_c^m = e_{i+m} - e_{j+m}$ with the subscripts taken modulo $\ell + 1$. Hence $\alpha w_c^m$ is a linear combination of $\alpha, \ldots, \alpha w_c^{m-1}$ iff $i + m$ and $j + m$ are both in $[i, i + m - 1] \cup [j, j + m - 1]$ modulo $\ell + 1$. By the pigeon hole principle, this can only happen if $m \geq (\ell + 1)/2$.

Type $C_\ell$: Identify $W$ with the set of permutations $w$ of $\{\pm 1, \ldots, \pm \ell\}$ such that $(-i)w = -(iw)$ for $i = 1, \ldots, \ell$. Consider $\Phi = \Phi(C_\ell)$ to consist of roots $\varepsilon e_i - \delta e_j$ with $\varepsilon, \delta \in \{\pm 1\}$, $i, j = 1, \ldots, \ell$ and $\varepsilon i \neq \delta j$. We can take

$$w_c = (1, 2, \ldots, \ell, -1, -2, \ldots, -\ell)$$

and $\alpha = \varepsilon e_i - \delta e_j$. The same argument used in type $A_\ell$ now shows that $m \geq \ell/2$. 

Type $B_c$: The permutation action of $W(B_c)$ on its roots is isomorphic to the action of $W(C_i)$ on its roots, so the same argument works.

Types $D_i$: Identify $W$ with the elements of $W(C_i)$ such that $\prod_{i=1}^{\ell}(i w) > 0$ and consider $\Phi$ to consist of the roots $\varepsilon \varepsilon_i - \delta \delta_j$ with $\varepsilon, \delta \in \{\pm 1\}$, $i, j = 1, \ldots, \ell$ and $i \neq j$. We can take $w_c = (1, 2, \ldots, \ell - 1, -1, -2, \ldots, -\ell + 1)(\ell, -\ell)$. Once again $m \geq \ell/2$ if $i, j \neq \ell$. If $i = \ell$, $j \neq \ell$, then $\alpha w_c^m = (-1)^m \varepsilon \varepsilon_i - \delta \delta_{j+m}$ with the second subscript taken modulo $\ell - 1$, and so $m \geq \ell - 1$.

Exceptional types: These are easily checked by computer.

It is well known that every orbit of $w_c$ on $\Phi$ has size $h$, so $\sum_i c_i(w_c) = 2N/h = \ell$. We have shown that $c_i(w_c) = 0$ for $i < \ell/2$, so

$$1 - \sum_{i=1}^{\ell} \frac{c_i(w_c)}{q^i} \geq 1 - \frac{\ell}{q^{\ell/2}}.$$  

The functions $Q_{w_c}(X)$ are straightforward to compute and are given in Table 1. The terms in which every coefficient is positive can be ignored, since they are bounded below by 1 when we set $X = 1/q$. Since no term $1 - X^0$ appears more than twice in these polynomials and $q \geq 3$, it follows by Lemma 6.4 that $Q_{w_c}(1/q) \geq (1 - 1/q)^6$.

The required inequality now follows from the first inequality of Proposition 6.1 and the fact that the centraliser of $w_c$ has order $h$. □

We now consider reflection nonderangements that are, in some sense, close to being Coxeter elements.

**Proposition 6.6.** Suppose that $W$ is an irreducible Weyl group. If $W$ is classical with rank at least 7 then there is a reflection nonderangement $w$ such that

$$\frac{|L_{\text{rss}, w}(k)|}{|L(k)|} \geq \left(1 - \frac{3}{q} - \frac{4}{q^2} - \frac{\ell + 5}{q^{(\ell-2)/2}}\right) \left(1 - \frac{1}{q}\right)^6 \frac{1}{4\ell}.$$

For other Cartan types there is a reflection nonderangement $w$ such that

$$\frac{|L_{\text{rss}, w}(k)|}{|L(k)|} \geq \left(1 - \sum_{i=1}^{\ell} \frac{c_i}{q^i}\right) \left(1 - \frac{1}{q}\right)^6 \frac{1}{c},$$

with the constants $c$ and $c_i$ listed in Table 2.
Table 2
The constants $c$ and $c_i$ for small rank and exceptionals.

<table>
<thead>
<tr>
<th>Type</th>
<th>$c_1$</th>
<th>$c_2$</th>
<th>$c_3$</th>
<th>$c_4$</th>
<th>$c_5$</th>
<th>$c_6$</th>
<th>$c_7$</th>
<th>$c_8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_1$</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_2$</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$B_2, C_2$</td>
<td>8</td>
<td>4</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$G_2$</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_3$</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$B_3, C_3$</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_4$</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$B_4, C_4$</td>
<td>12</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$D_4$</td>
<td>16</td>
<td>5</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$F_4$</td>
<td>36</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_5$</td>
<td>8</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$B_5, C_5$</td>
<td>16</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$D_5$</td>
<td>16</td>
<td>3</td>
<td>5</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_6$</td>
<td>10</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$B_6, C_6$</td>
<td>20</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>$D_6$</td>
<td>24</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>$E_6$</td>
<td>36</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>$E_7$</td>
<td>60</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$E_8$</td>
<td>108</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>9</td>
</tr>
</tbody>
</table>

Proof. Fix a root $\beta$. Assume $\beta$ is short (resp. long) for Cartan type $B_\ell$ (resp. $C_\ell$). Let $\Phi_\beta = \{ \gamma \in \Phi \mid \langle \gamma, \beta^\ast \rangle = 0 \}$. Then $\Phi_\beta$ is a subsystem of $W$ and, except in type $D_4$, it has at most two irreducible components. Let $\Phi_\beta'$ be the irreducible summand of $\Phi_\beta$ of maximal rank. Let $s_\beta$ be the reflection in $\beta$ and let $w_\beta$ be the Coxeter element of $W(\Phi_\beta')$. We take $w = s_\beta w_\beta$, except for type $A_1$ where we use $w = 1$, type $G_2$ where we use $w = s_\beta$, and type $D_4$ where we use $s_1 s_2 s_1 s_3 s_2 s_1 s_4 s_2 s_1 s_3 s_2$. (Here $s_i$ is the $i$th simple reflection, with the numbering given in [Bou75].) These elements are all reflection nonderangements.

First we prove that

$$\sum_{i=1}^\ell c_i \leq \frac{3}{q} + \frac{4}{q^2} + \frac{\ell + 5}{q^{(\ell-2)/2}}$$

for the classical types of rank at least 7.

Type $A_\ell$: Assume $\beta = e_1 - e_2$. Then $\Phi_\beta$ has type $A_{\ell-2}$, and so orbits within $\Phi_\beta$ contribute at most $\frac{\ell-2}{q^{(\ell-1)/2}}$ to the sum, as in the previous proof. If $\alpha \notin \Phi_\beta$, then $\alpha = \pm(e_i - e_j)$ where $i = 1$ or 2 and $j > 2$. These roots form one orbit of size 2 and either two orbits of size $\ell - 1$ or one orbit of size $2(\ell - 1)$. So these orbits contribute at most $1/q + 2/q^{\ell}$. Type $B_\ell$ with $\beta$ short: Assume $\beta = e_1 - e_2$. Then $\Phi_\beta$ has type $B_{\ell-1}$, and so the orbits within $\Phi_\beta$ contribute at most $\frac{\ell-1}{q^{(\ell-1)/2}}$. If $\alpha \notin \Phi_\beta$, then $\alpha = \pm(e_i - e_j)$ where $i = 1$ or 2 and $j > 2$. These roots form four orbits of size two with $m = 1$ and four orbits with $m = \ell - 2$.

Type $C_\ell$ with $\beta$ long: This is similar to type $B_\ell$, with the short roots and long roots exchanged.

Type $D_\ell$: Assume $\beta = e_1 - e_2$. Then $\Phi_\beta$ has type $D_{\ell-2}A_1$ and $\Phi_\beta'$ is the subsystem of type $D_{\ell-2}$. So the orbits within $\Phi_\beta'$ contribute at most $\frac{\ell-2}{q^{(\ell-1)/2}}$ to the sum. If $\alpha \notin \Phi_\beta'$, then $\alpha = \pm(e_i - e_j)$ where $i = 1$ or 2 and $j > 2$. These roots form at most four orbits with $m = \ell - 2$.

The values of the constants in Table 2 are easily computed in Magma [BC97]. The constant $c$ is just $|C_W(w)|$. The functions $Q_w(X)$ are given in Table 3. Applying Lemma 6.4, we get $Q_w(1/q) \geq (1 - 1/q)^6$. 


For groups not covered in Table 2, let $h_β$ be the Coxeter number of $Φ'_β$. Then the centraliser of $w_β$ in $W(Φ'_β)$ has order $h_β$, and the centraliser of $w$ in $W$ has order $2h_β \leq 4\ell$. The required result now follows from the first inequality of Proposition 6.1. □

6.4. Time analysis

Finally we are in a position to give an analysis of Algorithm 8, which searches for a split maximal toral subalgebra.

As discussed in Section 6.2, the probability of finding $f$ with $\text{deg}(f) = 1$, or with $\text{deg}(f) = 2$ and $f = f_-$, is bounded below by the chance of the corresponding Weyl group element being a reflection nonderangement.

The following result immediately implies Theorem 1.4.

**Theorem 6.7.** Suppose that the characteristic of $k$ is greater than 3. Let $G$ be a $k$-split connected reductive group and let $L$ be the Lie algebra of $G$. We can find a split maximal toral subalgebra of $L$ in Las Vegas time $O^-(n^3\ell^6 \log(q))^2$.

**Proof.** Before calling Algorithm 8, we compute the centre $Z(L)$ of $L$, which takes time $O^-(n + \ell^3 \log(q))$.

Algorithm 8 begins by calling Algorithm 5 which takes the time of computing the centraliser of an element $x$ and the computation of the minimal polynomial of $\text{ad}(x)$, all of which is bounded by $O^-(n^3 \log(q))^2$. Also, testing whether a maximal toral subalgebra $H/Z$ is split and finding the generalised roots of $L/Z$ with respect to $H/Z$ can be computed in $O^-(\ell^2 \log(q))^2$. In view of Lemma 5.7, the computation time for $M/Z$ and $K/Z$ in each of the cases is also bounded from above by this estimate. We conclude that the computations within the main loop take time $O^-(\ell^7 \log(q))^2$.

Therefore, the critical time estimate hinges on the probability of finding a suitable maximal toral subalgebra, that is, the centraliser of an element of $L_{rss}(k)$ for $w$ a reflection nonderangement. A lower bound on the ratio $|L_{rss}(k)/L(k)|$ can be obtained by consideration of a single component of $Φ$, so, for the remainder of the time analysis we can assume, without loss of generality, that $Φ$ is irreducible.

| $A_1$ | $1 - X$ |
| $A_2$ | $1 - X^3$ |
| $A_3$ | $(1 - X)(1 - X^3)(1 + X^2)$ |

$A_7$ (\(\ell > 3\))

$\prod_{i \in \{1, \ldots, \ell+1\}\setminus\{2, \ell-1\}}(1 - X^i)$

$B_2, C_2$

$(1 - X)^2(1 + X^3)$

$B_3, C_3$

$(1 - X)(1 - X^2)(1 - X^6)$

$B_4, C_4$

$(1 - X)(1 - X^3)(1 - X^4)(1 - X^8)$

$B_7, C_7$ (\(\ell > 4\))

$(1 - X)(1 - X^{\ell-2})(3 - (\ell)^{1/2})\prod_{i \in \{2, \ldots, \ell\}\setminus\{\ell-1\}}(1 - X^2i)$

$D_4$

$(1 - X)^2(1 + X^6)(1 + X^2)^2$

$D_6$

$(1 - X)^2(1 - X^3)(1 - X^6)(1 + X^2)(1 + X^4)$

$D_7$ (\(\ell > 6\))

$(1 - X)^2\prod_{i \in \{1 - \ell, \ell\}}(1 - X^i)\prod_{i \in \{4, \ldots, \ell-1\}\setminus\{\ell-3\}}(1 - X^{2i})(1 + X^2)(1 + X^2 + X^4)$

$G_2$

$1 - X^6$

$F_4$

$\prod_{i \in \{1, 3, 8, 12\}}(1 - X^i)$

$E_6$

$(1 - X)^2\prod_{i \in \{5, 8, 9, 12\}}(1 - X^i)$

$E_7$

$(1 - X)^2\prod_{i \in \{5, 6, 12, 14, 18\}}(1 - X^i)(1 + X^2)(1 + X^4)$

$E_8$

$(1 - X)^2\prod_{i \in \{6, 12, 14, 20, 24, 30\}}(1 - X^i)(1 + X^2)(1 + X^4)(1 + X^3 + X^6)$

<table>
<thead>
<tr>
<th>$Q_w(X)$</th>
<th>$A_1$</th>
<th>$A_2$</th>
<th>$A_3$</th>
<th>$A_7$</th>
<th>$B_2, C_2$</th>
<th>$B_3, C_3$</th>
<th>$B_4, C_4$</th>
<th>$B_7, C_7$</th>
<th>$D_4$</th>
<th>$D_6$</th>
<th>$D_7$</th>
<th>$G_2$</th>
<th>$F_4$</th>
<th>$E_6$</th>
<th>$E_7$</th>
<th>$E_8$</th>
<th>$Q_w(X)$</th>
</tr>
</thead>
</table>

**Table 3**

The functions $Q_w(X)$. 

<table>
<thead>
<tr>
<th>$A_1$</th>
<th>$A_2$</th>
<th>$A_3$</th>
<th>$A_7$</th>
<th>$B_2, C_2$</th>
<th>$B_3, C_3$</th>
<th>$B_4, C_4$</th>
<th>$B_7, C_7$</th>
<th>$D_4$</th>
<th>$D_6$</th>
<th>$D_7$</th>
<th>$G_2$</th>
<th>$F_4$</th>
<th>$E_6$</th>
<th>$E_7$</th>
<th>$E_8$</th>
<th>$Q_w(X)$</th>
</tr>
</thead>
</table>

For groups not covered in Table 2, let $h_β$ be the Coxeter number of $Φ'_β$. Then the centraliser of $w_β$ in $W(Φ'_β)$ has order $h_β$, and the centraliser of $w$ in $W$ has order $2h_β \leq 4\ell$. The required result now follows from the first inequality of Proposition 6.1. □

6.4. Time analysis

Finally we are in a position to give an analysis of Algorithm 8, which searches for a split maximal toral subalgebra.

As discussed in Section 6.2, the probability of finding $f$ with $\text{deg}(f) = 1$, or with $\text{deg}(f) = 2$ and $f = f_-$, is bounded below by the chance of the corresponding Weyl group element being a reflection nonderangement.

The following result immediately implies Theorem 1.4.

**Theorem 6.7.** Suppose that the characteristic of $k$ is greater than 3. Let $G$ be a $k$-split connected reductive group and let $L$ be the Lie algebra of $G$. We can find a split maximal toral subalgebra of $L$ in Las Vegas time $O^-(n^3\ell^6 \log(q))^2$.

**Proof.** Before calling Algorithm 8, we compute the centre $Z(L)$ of $L$, which takes time $O^-(n + \ell^3 \log(q))$.

Algorithm 8 begins by calling Algorithm 5 which takes the time of computing the centraliser of an element $x$ and the computation of the minimal polynomial of $\text{ad}(x)$, all of which is bounded by $O^-(n^3 \log(q))^2$. Also, testing whether a maximal toral subalgebra $H/Z$ is split and finding the generalised roots of $L/Z$ with respect to $H/Z$ can be computed in $O^-(\ell^2 \log(q))^2$. In view of Lemma 5.7, the computation time for $M/Z$ and $K/Z$ in each of the cases is also bounded from above by this estimate. We conclude that the computations within the main loop take time $O^-(\ell^7 \log(q))^2$.

Therefore, the critical time estimate hinges on the probability of finding a suitable maximal toral subalgebra, that is, the centraliser of an element of $L_{rss}(k)$ for $w$ a reflection nonderangement. A lower bound on the ratio $|L_{rss}(k)/L(k)|$ can be obtained by consideration of a single component of $Φ$, so, for the remainder of the time analysis we can assume, without loss of generality, that $Φ$ is irreducible.
By Proposition 6.6, if $G$ is classical with rank at least 7, we obtain a split toral subalgebra in $L/Z$ of rank at least 1 with probability at least

$$
\left( 1 - \frac{1}{q} \right)^6 \left( 1 - \frac{3}{q} - \frac{4}{q^2} - \frac{\ell + 5}{q^{(\ell-2)/2}} \right) \frac{1}{4\ell}.
$$

For $q \geq 5$ and $\ell \geq 7$, this is at least

$$
\left( \frac{4}{5} \right)^6 \left( 1 - \frac{3}{5} - \frac{4}{25} - \frac{12}{5^{5/2}} \right) \frac{1}{4\ell} > 0.
$$

Similarly for the Cartan types in Table 2, except for $D_4$,

$$
\left( 1 - \sum_{i=1}^{c_i} \frac{c_i}{q^i} \right) \left( 1 - \frac{1}{q} \right)^6 \frac{1}{c} \geq \left( 1 - \sum_{i=1}^{c_i} \frac{c_i}{5^i} \right) \left( 1 - \frac{1}{5} \right)^6 \frac{1}{c} > 0.
$$

For type $D_4$, the bound is negative for $q = 5$, but positive for $q \geq 7$. So it remains to consider the Lie algebra $D_4(5)$. But for any fixed Lie algebra, it is easily seen that there is a nonzero chance of the algorithm working, since there is a fixed positive lower bound on the probability that the toral subalgebra found by Algorithm 5 is already split. Therefore, we have shown that there is a constant $C > 0$ such that the probability of success after one iteration of the main loop is at least $C/\ell$.

Since

$$
\lim_{\ell \to \infty} \left( 1 - \frac{C}{\ell} \right)^{a\ell} = e^{-aC},
$$

we can choose $a$ such that

$$
\left( 1 - \frac{C}{\ell} \right)^{a\ell} \leq \frac{1}{e^A}
$$

for all $\ell$. Hence the probability of failure after $a\ell \log(\ell)$ repetitions of the loop is at most

$$
\left( 1 - \frac{C}{\ell} \right)^{a\ell \log(\ell)} \leq \left( \frac{1}{e^A} \right)^{\log(\ell)} = \frac{1}{e^A}.
$$

Clearly the depth of recursion is at most $\ell$, which contributes a further factor of $\ell$ to our timing, so the total number of recursive calls is at most $\ell^2 \log(\ell)$. Hence the overall probability of success is at least

$$
\left( 1 - \frac{1}{e^A} \right)^{\ell^2 \log(\ell)} \geq \frac{1}{2}.
$$

Hence Algorithm 8 takes Las Vegas time $O^\sim(\ell^9 \log(q)^2)$. Combining this with the preprocessing time of $O^\sim((n + \ell^2)^3 \log(q))$, and using the fact that $n \geq \ell$ we get the desired result. □

**Corollary 6.8.** Suppose that the characteristic of $k$ is greater than 3. Let $G$ be a $k$-split connected reductive group and let $L$ be the Lie algebra of $G$. We can find a Chevalley basis of $L$ in Las Vegas time $O^\sim(n^3 \ell^6 \log(q)^2)$. 
Proof. The time taken to find a split maximal toral subalgebra clearly dominates the time for Algorithm 9, which is dealt with in Theorem 6.7.

Hence, combining this corollary with Lemma 5.9 and Proposition 4.4, we see that the algorithm for Lang's Theorem takes time

\[
O^*(n^3 \epsilon^6 \log(q)^2 + n^6 m^2 r^2 s^2 \log(q)^2),
\]

which easily leads to the timing in Theorem 1.2.

References


