ALGORITHM FOR LANG'S THEOREM

ARJEH M. COHEN AND SCOTT H. MURRAY

Abstract. We give an efficient 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.

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, ie, it is Las Vegas in the sense of [Bab97]. 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 $\bar{k}$. The affine space of dimension N can be identified with $\bar{k}^N$. An *affine variety* X is a subset of $\bar{k}^N$ 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 $F : \bar{k}^N \to \bar{k}^N$ that takes the qth 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^r. A *nonstandard Frobenius endomorphism* is a morphism $F' : X \to X$ such that $(F')^s = F^s$ for some positive integer s. The elements of X fixed by F' 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°, the component of the identity. This subgroup is normal and G/G° is finite, so for many purposes it suffices to study connected groups. An important result on linear algebraic groups over finite fields is:

Date: October 27, 2006.

The authors would like to thank Sergei Haller, Anthony Henderson, William M. Kantor, Gus Lehrer, T. A. Springer, and D. E. Taylor for useful discussions on this topic. The authors also thank the Magma project at the University of Sydney, where some of the work was carried out.

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 in k-split connected reductive groups described by the Steinberg presentation as in [CMT04]. In particular, the root datum, and hence the Cartan type, of G is known. Reductive groups are likely to be the critical case, since the problem for an arbitrary connected linear algebraic group could be solved by working down a composition series (see Section 3) and all simple connected groups are reductive. Our main result is:

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. Let c be in $G(k_r)$, and suppose we are given s, the order of $c^{F^{r-1}} \cdots c^F c$. Then we can find $a \in G(k_{rs})$ such that $c = a^{-F}a$ in Las Vegas time $O(n^9 r^2 s^2 \log^2(n) \log^2(q))$ where n is the reductive rank of G.*

We can improve significantly on this result for the classical groups:

Theorem 1.3. *Let G be a k-split simple connected classical group defined over the field k of size q. Let c be in $G(k_r)$ and suppose we are given s, the order of $c^{F^{r-1}} \cdots c^F c$. Then we can find $a \in G(k_{rs})$ such that $c = a^{-F}a$ in Las Vegas time $O(n^5 r^2 s^2 \log^2(q))$ where n is the reductive rank of G.*

The parameter s measures the size of the field extension required, as explained in Section 2. The input element c has size $O(n^2 r \log(q))$ and the output element a has size $O(n^2 rs \log(q))$. 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. 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 this basis may of interest in its own right and so we state it here.

Theorem 1.4. *Suppose that k is 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 $O(n^9 \log^2(n) \log^2(q))$.*

We note that this is similar to a result by Ryba [Ryb99].

The running times of the algorithms are analysed in Section 6, leading to proofs of Theorems 1.2 and 1.4.

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 $G(k_r)$.

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 $c^{F^{r-1}} \cdots c^F c$. 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

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

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

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 we consider s, the order of $c^{F^{r-1}} \cdots c^F c$, to be an input of our algorithm. While it is 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 algorithm of [CLG97]. If the representation has degree d, this takes Las Vegas time $O(d^3 \log(q) \log\log(q^d))$ plus the time required to factor a collection of integers of the form $q^{d_i} - 1$ with $\sum_i d_i \le d$.

Suppose now that G is a k-split reductive group with reductive rank n and semisimple rank ℓ. The element c, which is the input to our algorithm, has size $O((n + \ell^2) r \log(q))$; while the element a, which is the output, has size $O((n + \ell^2) rs \log(q))$. Since s need not be bounded by a polynomial in n, ℓ, 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 $\dot{w}$ is the Steinberg presentation). These elements have $r = 1$ and s at most $O(\ell^2)$.

3. Twisted eigenvectors

We can now give an outline of our main algorithm. Let $G = G(\bar{k})$ be a connected linear algebraic group defined over k. Suppose that V is a G-module of dimension d defined over k, so that F acts on $V = \bar{k}^d$ by taking the qth power of each component. We say that $v \in V$ is an *F-eigenvector* of c 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. By Lang's theorem, the k_{rs}-span of $E(k)$ must be equal to $V(k_{rs})$. There is a variety E defined over k such that $E(k_t)$ is the k_t-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 $K \le G$. 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 $a^{-F} z a = c$ for $z \in K$, then, for all $v \in V(k)$, $va = vza = va^F c = (va)^F c$ and so $va \in E(k)$. Conversely, if $V(k)a = E(k)$, then, for all $v \in V(k)$, $va = (va)^F c = va^F c$ and so $a^F c a^{-1} \in K$. □

LANG := **function**(G, c, s) [$c \in G(k_r)$, s a multiple of the order of $c^{F^{r-1}} \cdots c^F c$]
construct a module V for G
let $E(k) = F$-EIGENSPACE(c, V, s)
find a transformer $a \in G(k_{rs})$ for E
if V is faithful **then**
return a
else
construct a proper connected subgroup H of G containing the kernel of V
let $b =$ LANG$(H, a^F ca^{-1}, s)$
return ba
end if
end function

ALGORITHM 1. Algorithm outline for Lang's Theorem

F-EIGENSPACE := **function**(c, V, s) [$c \in G(k_r)$, s the order of $c^{F^{r-1}} \cdots c^F c$]
let S be the k-matrix of F acting of k_{rs}
let C be the k-matrix of c acting on $V(k_{rs}) = k_{rs}^d$
return the fixed point space of $S^{\oplus d}C$
end function

ALGORITHM 2. Deterministic method for computing F-eigenvalues

We call an element $a \in G(k_{rs})$ such that $V(k)a = E(k)$ a *transformer* in G for the k-form E. Our approach to solving Lang's Theorem is outlined in Algorithm 1. Note that s is taken to be the order of $c^{F^{r-1}} \cdots c^F c$ 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 that G is split reductive and let T_0 be a 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 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 simple 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 drs. The solution is then found by linear algebra over k. Computing S takes time $O(r^2s^2\log^2(q))$, where the second factor of $\log(q)$ is for computing qth powers. Finding C and the fixed space takes time $O(d^3r^3s^3\log(q))$. So the overall time is $O(d^3r^3s^3\log^2(q))$.

F-EIGENSPACE := **function**(c, V, s) $\quad$ $[c \in G(k_r),\ s$ the order of $c^{F^{r-1}} \cdots c^F c]$
  repeat
    let x be a random $d \times d$ matrix over k_{rs}
    let $a = x + x^F c + x^{F^2} c^F c + \cdots + x^{F^{rs-1}} c^{F^{rs-2}} \cdots c^F c$
  until a is invertible
  return $V(k)a^{-1}$
end function

ALGORITHM 3. Las Vegas method for computing F-eigenvalues

An alternative method, due to Glasby and Howlett [GH97], is given in Algorithm 3. It takes time $O(d^2 r^2 s^2 \log^2(q))$ to apply F to a $d \times d$ matrix over k_{rs}, so computing a takes time $O(d^3 r^2 s^2 \log^2(q))$. 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 in $\mathrm{GL}(V)$ if the function returns a instead of $V(k)a^{-1}$.

We now have:

Theorem 3.2. *Let G be a connected linear algebraic group defined over k and let V be a G-module defined over k with dimension d. Let c be an element of G with minimum field degree r and let s be the order of $c^{F^{r-1}} \cdots c^F c$. Then we can compute a basis for the k-space $E(k)$ of F-eigenvectors of c in deterministic time $O(d^3 r^3 s^3 \log^2(q))$ or Las Vegas time $O(d^3 r^2 s^2 \log^2(q))$.*

4. Finding transformers

Let G be a k-split connected reductive linear algebraic group defined over k, let c be in $G(k_r)$, and let s be the order of $c^{F^{r-1}} \cdots c^F c$. Let T_0 be the standard k-split maximal torus of G determined by the Steinberg presentation. 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: split tori and classical groups. Then we give an algorithm for an arbitrary k-split connected reductive group. The key is to consider k-bases with some additional structure that ensures that G is transitive on all such bases (or G_{ad} is transitive in Subsection 4.3).

4.1. **Split tori and isogeny.** A *k-split torus T* of dimension n is just the direct product of n copies of $\bar{k}^\times$ with the Frobenius endomorphism taking the qth power of each component. The standard module V is just $\bar{k}^n$ with the componentwise action. Suppose $c = (c_1, \dots, c_n) \in T(k_r)$ and E is the variety of F-eigenvectors of c in V. Splitting T into n copies of $\bar{k}^\times$ and using Theorem 3.2, we can compute E in Las Vegas time $O(nr^2 s^2 \log^2(q))$. Now E has a basis of the form $a_1 e_1, \dots, a_n e_n$ where each $a_i \in k_{rs}^\times$ and e_i is the ith standard basis vector in V. Now $(a_1, \dots, a_n) \in T(k_{rs})$ 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 $c^{F^{r-1}} \cdots c^F c$. Then we can find an element a in $T(k_{rs})$ such that $c = a^{-F} a$ in Las Vegas time $O(nr^2 s^2 \log^2(q))$.*

Consider two connected linear algebraic groups G and H defined over k. Let ι be a homomorphism $G \to H$ defined over k which is onto with finite kernel K. Such a map is called an *isogeny*. Now suppose G and H are reductive and described by a Steinberg presentation with unipotent, Weyl, and toral generators as in [CMT04]. If there is an isogeny $\iota : G \to H$, then both groups have the same Cartan type. Furthermore, we can assume (after composing with an automorphism) that ι leaves unipotent and Weyl generators unchanged, and acts by a change of basis on the toral generators. We denote the standard tori generated by the toral generators of G (resp. H) by T_0 (resp. U_0). Note that $K \le Z(G) \le T_0$. An important invariant of ι is the exponent of the finite group K, which we denote by m.

For $g \in T_0(k_r)$, we have $\iota(g)^{F^r} = \iota(g^{F^r}) = \iota(g)$, so $\iota(g) \in U_0(k_r)$. This image can be computed in time $O(n^3 r \log(q))$ by linear algebra in $T_0(k_r)$.

For $h \in U_0(k_r)$, we can find $g \in T_0$ such that $\iota(g) = h$. Then $\iota(g^{-F^r} g) = h^{-F^r} h = 1$, ie, $g^{-F^r} g \in K$. Hence $(g^{-F^r} g)^m = 1$ and so $g^m \in T_0(k_r)$. 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 $O(n^3 rm \log(q))$ by linear algebra in $T_0(k_{rm})$.

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

(1) Lang's theorem can be solved for $c \in G(k_r)$ in time $O(n^3 r^2 s(c)^2 m^2 \log^2(q))$ plus the time needed to solve it for some $c' \in H(k_r)$ with $s(c') \le s(c)$.
(2) Lang's theorem can be solved for $c \in H(k_r)$ in time $O(n^3 rs(c) m^2 \log(q))$ plus the time needed to solve it for some $c' \in G(k_{rm})$ with $s(c') \le ms(c)$.

Proof. If $c \in G(k_r)$, then $c' = \iota(c)$ can be found in time $O(n^3 r \log(q))$. Clearly $s(c') \le s(c)$. Now we can find $a' \in H_{rs(c)}$ such that $a'^{-F} a' = c'$. Let $a \in G_{rsm}$ be a preimage of a' computed in time $O(n^3 rm \log(q))$. Consider $a^F ca^{-1} \in K(k_{rs(c)m}) \le T_0(k_{rs(c)m})$. Now

$$(a^F ca^{-1})^{F^{rs(c)m-1}} \cdots (a^F ca^{-1})^F (a^F ca^{-1}) = a^{F^{rs(c)m}} (c^{F^{rs(c)m-1}} \cdots c^F c) a^{-1} = 1,$$

So by Proposition 4.1, we can find $b \in T_0(k_{rs(c)m})$ such that $a^F ca^{-1} = b^{-F} b$ in Las Vegas time $O(nr^2 s(c)^2 m^2 \log^2(q))$. Now $(ab)^{-F} ab = c$ and Part (1) follows.

If $c \in H(k_r)$, we can find an element $c' \in G(k_{rm})$ such that $\iota(c') = c$ in time $O(n^3 rm \log(q))$. Since $(c'^{F^{r-1}} \cdots c'^F c')^{s(c)} \in K$, we get $s(c') \le ms(c)$. We can now find $a' \in H(k_{rs(c)m^2})$ 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 $a^{-F} a = c$ and Part (2) is proved. □

4.2. **Classical groups.** We now show how to find transformers for the classical groups, using the standard representations. Throughout this subsection we take $V = \bar{k}^d$ and B_0 to be the standard basis $e_1, \ldots, e_d$ of $V(k)$.

The simplest case is $G = \mathrm{GL}_d(\bar{k})$. Let B be a k-basis of $E(k)$. Let a be the matrix whose rows are the elements of B. Then $B_0 a = B$, and so a is a transformer for E.

Now suppose $G = \mathrm{SL}_d(\bar{k})$. Given a basis B of V, define its *volume*, denoted $\mathrm{vol}(B)$, 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 $B^F c = B$, and so

$$\mathrm{vol}(B)^F = \mathrm{vol}(B^F) = \mathrm{vol}(Bc^{-1}) = \mathrm{vol}(B)\det(c)^{-1} = \mathrm{vol}(B),$$

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

Now suppose that q is odd and M is a nondegenerate orthogonal or symplectic form on V written (u, v) for $u, v \in V$. Further suppose that M is defined over k. Then the invariant group

$$G = \{x \in \mathrm{GL}_d(\bar{k}) \mid (ux, vx) = (u, v)\}$$

is a reductive linear algebraic group defined over k. Note that G is not necessarily split or connected however. Define the $m \times m$ matrix

$$A_m = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix}$$

and let δ be a fixed nonsquare in k. 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
$$M_B = A_d \quad \text{or} \quad \begin{pmatrix} & & A_\ell \\ & \delta & \\ A_\ell & & \end{pmatrix}.$$
- If M is orthogonal and $d = 2\ell$, then
$$M_B = A_d \quad \text{or} \quad \begin{pmatrix} & & & A_{\ell-1} \\ & 1 & & \\ & & -\delta & \\ A_{\ell-1} & & & \end{pmatrix}.$$
- If M is symplectic, then $d = 2\ell$ and
$$M_B = \begin{pmatrix} & A_\ell \\ -A_\ell & \end{pmatrix}.$$

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

Given a nondegenerate 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 by standard techniques in time $\log^2(q)$. Note that this construction is rational (that is, it does not use extensions of k) and takes time $O(d^3 \log(q) + d \log^2(q))$.

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 $G = \mathrm{SO}(V, M)$, then this problem can be avoided. Without loss of generality, the standard basis B_0

NormalBasis := **function**(U)
  let u be a nonzero element of U
  if $\dim(U) = 1$ **then**
    find $a \in k$ such that $a^2 = (u,u)$ or $a^2\delta = (u,u)$
    return u/a
  end if
  let v be a nonzero element of $u^\perp \setminus ku$
  if $\dim(U) = 2$ **then**
    if $(u,u) \in -\delta(v,v)k^{\times 2}$ **then** [U anisotropic]
      find $a, b \in k$ such that $(u,u)a^2 + (v,v)b^2 = 1$
      find $c \in k$ such that $((u,u)a^2 - (v,v)b^2)c^2 = -\delta$
      return $au + bv, c(au - bv)$
    else [U isotropic]
      find $a, b \in k$ such that $(u,u)a^2 + (v,v)b^2 = 0$
      let w be a nonzero element of $(au + bv)^\perp$
      return $au + bv$, w
    end if
  end if
  let w be a nonzero vector in $(ku + kv)^\perp \setminus (ku + kv)$
  find $a, b, c \in k$ such that $(u,u)a^2 + (v,v)b^2 + (w,w)c^2 = 0$
  let x be a nonzero element of $(au + bv + cw)^\perp$
  return $au + bv + cw$, NormalBasis($\{u,v\}^\perp$), x
end function

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

is normal. Suppose that B is a normal basis of $E(k)$. As with the special linear group, $\mathrm{vol}(B)$ is in k. Also

$$\det(M_B) = \det(BM_{B_0}B^T) = \mathrm{vol}(B)^2 \det(M_{B_0}).$$

But the two choices given above for the Gram matrix have determinants in different cosets of $k^{\times 2}$, hence $M_{B_0} = M_B$. It now remains to ensure that $\mathrm{vol}(B)$ is one. Now $\mathrm{vol}(B)^2 = \det(M_{B_0})/\det(M_B) = 1$, so suppose $\mathrm{vol}(B) = -1$. 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.

Now suppose we have 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 $\iota : \mathrm{SL}_n(\bar{k}) \to G$ with $m \le n+1$. By Proposition 4.2(2), we can solve Lang's Theorem in G in Las Vegas time $O(n^5 r^2 s^2 \log^2(q))$.

If G is not of type A_ℓ, then there is a series of at most 2 isogeny maps connecting G with one of the groups considered above. For each of these maps, m is at most 4. By Proposition 4.2, we can solve Lang's Theorem in Las Vegas time $O(n^3 r^2 s^2 \log^2(q))$.

We have now proved Theorem 1.3. For groups of Cartan type G_2 and F_4, a similar result can probably be obtained by exploiting the structure of composition and Jordan algebras, respectively [SV00].

4.3. **Adjoint representation.** Now consider an arbitrary k-split connected reductive linear algebraic group G, with reductive rank n and semisimple rank ℓ. Then G has a root datum $(X, \Phi, Y, \Phi^\star)$ with respect to a k-split maximal torus T_0. Here X and Y are free $\mathbb{Z}$-modules of dimension n with a bilinear pairing $\langle \circ, \circ \rangle : X \times Y \to \mathbb{Z}$ putting them in duality. We fix dual bases $e_1, \ldots, e_n$ for X and $f_1, \ldots, f_n$ for Y. The roots Φ are a finite subset of X and the coroots $\Phi^\star$ are a finite subset of Y. There is a one-to-one correspondence $\star : \Phi \to \Phi^\star$ such that $\langle \alpha, \alpha^\star \rangle = 2$ for every $\alpha \in \Phi$. For more details see [CMT04].

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_α for $\alpha \in \Phi$ and $h_i \in L(T_0)$ for $i = 1, \ldots, n$ with structure constants:

$$[h_i, h_j] = 0, \tag{1}$$

$$[e_\alpha, h_i] = \langle \alpha, f_i \rangle \, e_\alpha, \tag{2}$$

$$[e_{-\alpha}, e_\alpha] = \sum_{i=1}^{n} \langle e_i, \alpha^\star \rangle h_i, \tag{3}$$

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

where the integral constants $N_{\alpha\beta}$ are defined in [Car72]. Such a basis is called a *Chevalley basis.*

Choose simple roots $\alpha_1, \ldots, \alpha_\ell$, and fix a linear ordering $<$ on Φ^+ which is compatible with height, ie, $\mathrm{ht}(\alpha) < \mathrm{ht}(\beta)$ implies that $\alpha < \beta$. Given a nonsimple positive root ξ, take the positive roots α, β such that $\xi = \alpha + \beta$ and α is as small as possible with respect to the ordering on Φ^+. We call (α, β) the *extraspecial pair* of ξ. 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 Subsection 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 $L(k_{rs})$. We now need to find a transformer in G. Let G_{ad} be the adjoint group with the same Cartan type as G and let Γ be the automorphism group of the Dynkin diagram of G. For each element of Γ, fix a graph automorphism normalising T_0 and the Borel subgroup determined by Φ^+, as in [Car72]. Take Z to be a complement to $Z(L) \cap [L, L]$ in $Z(L)$; by construction, our graph automorphisms fix Z pointwise. If the characteristic of k is greater than 3, then it follows from [Hog82] that

$$\mathrm{Aut}(L) = \mathrm{Aut}(Z) \times (\Gamma \ltimes G_{\mathrm{ad}}).$$

We can compute a decomposition $a = z\gamma b$ with $z \in \mathrm{Aut}(Z)$, γ a graph automorphism, and $b \in G_{\mathrm{ad}}(k_{rs})$ in time $O(d^3 rs \log(q))$ using a slight modification of Algorithm 6 of [CMT04]. Since $L(k)z\gamma = L(k)$, the element b is a transformer in G_{ad}. It is easily checked on a case-by-case basis that the number of roots of G is $O(\ell^2)$ and so the dimension of L is $O(n+\ell^2)$. Hence Lang's Theorem can be solved for $c \in G_{\mathrm{ad}}(k_r)$ in time $O((n+\ell^2)^3 r^2 s^2 \log^2(q))$, once we have a standard Chevalley basis for $E(k)$.

Suppose now that G is simple, so that $\ell = n$. Then there is an isogeny map $G \to G_{\mathrm{ad}}$ with m at most $n+1$. We can now apply Proposition 4.2(2) and obtain:

Proposition 4.3. *Suppose that k has characteristic greater than 3. Let G be a k-split connected simple linear algebraic group and let L be the Lie algebra of G. Let c be an element of $G(k_r)$ and suppose we are given s, the order of $c^{F^{r-1}} \cdots c^F c$. Let E be the variety of F-eigenvectors of c in L. We can find $a \in G(k_{rs})$ in Las Vegas time $O(n^8 r^2 s^2 \log^2(q))$ 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. Once we have a split maximal toral p-subalgebra, a Chevalley basis can be constructed using [Car72, Section 4.2].

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, ℓ 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 $p : L \to L$ satisfying the axioms

$$(x+y)^p = x^p + y^p + \sum_{i=1}^{p-1} s_i(x,y), \tag{5}$$

$$(ax)^p = a^p x^p, \tag{6}$$

$$[xy^p] = x(\operatorname{ad} y)^p \tag{7}$$

where $x, y \in L$, $a \in \bar{k}$, s_i is defined in [Jac62, Section V.7], and a^p and $(\operatorname{ad} y)^p$ are the usual pth powers.

Given values of the p-map on a basis of L, we can compute the values on an arbitrary element using Equations (5) and (6). But s_{p-1} involves Lie products of length p, so the time taken for this computation is not polynomial in $\log(p)$. Given $x \in L$, we can use (7) to compute the coset $x^p + Z(L)$ in time $O(\ell^6 \log(q) \log(p))$, since $\dim(L/Z(L))$ is $O(\ell^2)$. 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 $O(\ell^6 \log^2(q))$.

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 $H_0 := L(T_0) = \langle h_1, \dots, h_n \rangle$ 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 $h_\alpha = \sum_{i=1}^{n} \langle e_i, \alpha^\star \rangle h_i$, then the coefficient of e_α in $[z, h_\alpha]$ is $2a_\alpha$. Since $[z, h_\alpha] = 0$ and $p > 2$, we get $a_\alpha = 0$. Hence z is in $H_0 = \langle h_1, \dots, h_n \rangle$. 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 $O(\ell^7 \log^2(q))$.*

```
MaximalToralSubalgebra := function(L)
  repeat take x random in L until x is semisimple
  let M = C_L(x)
  if M is abelian then
    return M
  else
    return MaximalToralSubalgebra(M)
  end if
end function
```

ALGORITHM 5. Finding a maximal toral subalgebra in L

Proof. First check that H is abelian of dimension n, and compute H/Z. Note that H/Z has dimension at most ℓ. By Theorem 5.1(2), it suffices to determine if $H/Z(L)$ is a split toral algebra. This is done by testing whether $b^q + Z(L) = b + Z(L)$ where $b + Z(L)$ runs over a basis of $L/Z(L)$. As we argued at the beginning of this section, this takes time $O(\ell^6 \log^2(q))$ for each basis element. □

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 algorithm is to randomly select a series of increasingly split maximal toral subalgebras. We now assign a conjugacy class of W to every maximal toral subalgebra H, which measures how split H is. See [Leh92] for a more detailed version of this construction. There exists $g \in G(\bar{k})$ such that $H = {H_0}^g$, by Theorem 5.1(5). Note that ${H_0}^F = H_0$ and $H^F = H$, since both are defined over k. Now

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

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

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

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 $\alpha \in \Phi$ is a linear functional $H_0 \to \bar{k}$ defined over k. This decomposition is defined over k by [Sel67, Theorem 6]. If the characteristic of k is greater than 3, every root space has dimension one.

Let H be a maximal toral subalgebra of L, fix $g \in G(\bar{k})$ such that $H = {H_0}^g$ and let w be the image of $g^F g^{-1}$ in W. For $\alpha \in \Phi$, define $\alpha^g : H \to \bar{k}$ by $\alpha^g(h) = \alpha(h^{g^{-1}})$. Then the root decomposition with respect to H is

$$ L = H \oplus \bigoplus_{\alpha \in \Phi} L_{\alpha^g}, $$

where $L_{\alpha^g} = \{b \in L \mid [b,h] = \alpha^g(h)b \text{ for all } h \in H\} = {L_\alpha}^g$. This decomposition is not defined over k in general.

```
GeneralisedRoots := function(L, H)
  let h_1, ..., h_n be a basis of H
  let 𝓕 = {()} and define L_() = L
  for i = 1, ..., n do
    let 𝓕' = ∅
    for f ∈ 𝓕 do
      compute g, the characteristic polynomial of h_i on L_f
      for f_i an irreducible factor of g do
        add (f_1, ..., f_{i-1}, f_i) to 𝓕' where f = (f_1, ..., f_{i-1})
        define L_(f_1,...,f_i) = {x ∈ L_f | x f_i(ad(h_i)) = 0}
      end for
    end for
    let 𝓕 = 𝓕'
  end for
  remove (X, ..., X) from 𝓕        [since L_(X,...,X) = H]
  return 𝓕
end function
```

ALGORITHM 6. Generalised roots

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

$$L_f = \{y \in L \mid y f_i(\mathrm{ad}(h_i)) = 0 \text{ for } i = 1, \ldots, \ell\}.$$

If $L_f \neq 0$, we call f a *generalised root* and L_f a *generalised root space*. The *generalised root decomposition* of L with respect to H is

$$L = H \oplus \bigoplus_{f \in \mathcal{F}} L_f,$$

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 time at most $O(d^3(\log(d) + \log(q))\log(q))$, as shown in [vzGG03]. Factoring the characteristic polynomials g is the dominant contribution to the running time of this algorithm. Since each g has degree at most d, and the sum of the degrees of all the gs is at most nd, the algorithm takes time $O(nd^3(\log(d) + \log(q))\log(q))$.

In fact, we do not apply this algorithm directly to L, since we want our time to depend on ℓ but not on n (this is necessary for analysing the recursion in Algorithm 8). By Theorem 5.1(2), the centre $Z(L)$ is contained in H. So we can construct a basis $h_1, \ldots, h_n$ for $H(k)$ with $\langle h_1, \ldots, h_m \rangle = Z(L)$ central for some $m \leq n$. Extend this to a basis B of $L(k)$. Let ϕ be the pullback map $L/Z(L) \to L$ which takes $b + Z$ to b for all $b \in B$. Note that ϕ is a linear map, but need not be a Lie algebra map. We compute in $L/Z(L)$, since it has dimension $O(\ell^2)$ independent of n, and the results are then transfered into L via ϕ. However, $L/Z(L)$ need not be the Lie algebra of a group of Lie type, so most of our theoretical results do not apply to this quotient.

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 $f' = (f_1, \ldots, f_m, X, \ldots, X)$ of length n. It is now easy to see that $\phi((L/Z(L))_f) = L_{f'}$. Hence the generalised root decomposition of L with respect to H follows immediately once we have the decomposition of $L/Z(L)$ with respect to H/Z. Since the dimension of $L/Z(L)$ is $O(\ell^2)$, the decomposition of $L/Z(L)$ can be computed in time $O(\ell^7(\log(\ell) + \log(q))\log(q))$.

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

$$f_- = ((-1)^{\deg(f_1)} f(-X), \ldots, (-1)^{\deg(f_n)} f(-X)).$$

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 Φ_f.

Lemma 5.3. *Let f be a generalised root of $L = L(G)$ with respect to H.*

(1) The action of F on $\{L_{\alpha^g} \mid \alpha \in \Phi_f\}$ is equivalent to the action of w on Φ_f.
(2) Φ_f is a union of orbits of w on Φ.
(3) If $\deg(f) = 1$, then w acts trivially of Φ_f. If in addition $q > 3$, then Φ_f contains a single root.
(4) If $\deg(f) = 2$ and $f = f_-$, then w acts on Φ_f by negation.

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

$${L_{\alpha^g}}^F = {L_\alpha}^{gF} = {L_\alpha}^{F^{-1}gF} = {L_\alpha}^{g^F} = {L_\alpha}^{t\dot{w}g} = {L_{\alpha w}}^g = L_{(\alpha w)^g},$$

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 $\deg(f) = 1$.

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

5.3. **Fundamental subalgebras.** Now that we have the generalised root decomposition of L with respect to H, we consider the subalgebra M_f generated by a generalised root space L_f. Such subalgebras often turn out to be fundamental: 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 the Lie algebra of a (split) fundamental group. This subgroup is denoted G_M. Fundamental subalgebras clearly normalise a maximal toral subalgebra.

The most important properties of such algebras for our purposes are:

Theorem 5.4. *Suppose that k has characteristic greater than 3. Let M be a fundamental subalgebra of L normalised by the maximal toral subalgebra H.*

(1) $M \cap H$ is a maximal toral subalgebra of M.
(2) If H is a split maximal toral subalgebra, then M is split fundamental.

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

$$M + H = H \oplus \bigoplus_\beta M_\beta, \tag{8}$$

where β 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 $M_\beta \leq M$. Since $p > 3$, every M_β has dimension one. So, by intersecting (8) 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.

Finally if M normalises H and H is split, then, by Theorem 5.1(4), $H = L(T)$ for some split maximal torus T of G. Then G_M normalises T and Part (2) is proved. □

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 Ψ. 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 5.5. *Suppose that k has odd characteristic. Let M be the subalgebra generated by $\sum_{\alpha\in\Psi} L_{\alpha^g}$, where Ψ is an orbit in Φ under the action of $w \in W$.*

(1) M is fundamental or soluble.
(2) If M is fundamental, then G_M is semisimple.
(3) M is fundamental if, and only if, $\overline{\Psi}$ is a subsystem.
(4) If $\overline{\Psi}$ is a subsystem and w is inner on $\overline{\Psi}$, then M is split fundamental.

Proof. Since $[\sum_{\alpha\in\Psi} L_{\alpha^g}, H] \leq \sum_{\alpha\in\Psi} L_{\alpha^g}$, we have $[M,H] \leq M$ and so M normalises H. Since $[L_\alpha, L_\beta] \leq L_{\alpha+\beta}$ (recalling that $L_0 = H$), we have

$$M = (H \cap M) \oplus \bigoplus_{\alpha\in\overline{\Psi}} L_{\alpha^g}.$$

Let $\Psi = \Psi_1 \cup \cdots \cup \Psi_m$ be the finest decomposition of Ψ into pairwise orthogonal subsets. Then $\overline{\Psi} = \overline{\Psi}_1 \cup \cdots \cup \overline{\Psi}_m$ is also an orthogonal decomposition. Clearly w permutes the sets Ψ_i and, since w is transitive on Ψ, it must be transitive on them. Since $-\overline{\Psi}_1$ is never orthogonal to $\overline{\Psi}_1$, we either 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 ψ 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 $M_i = H_i \oplus \bigoplus_{\alpha\in\overline{\Psi}_i} L_{\alpha^g}$, where H_i is the subalgebra of H generated by $[L_{\alpha^g}, L_{-\alpha^g}]$ 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 Ψ_1 is just $\overline{\Psi}_1 \cup -\overline{\Psi}_1$. Since this root subsystem is irreducible, ψ induces an ordering on it which makes $\overline{\Psi_1}$ the set of positive roots. Hence M_1 is just 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 M_1 is fundamental with G_{M_1} a simple group. Hence $M = \bigoplus_i M_i$ is fundamental with G_M a semisimple group. Parts (1), (2) and (3) are now proved.

Now suppose that $\overline{\Psi}$ is closed under negation and w is inner on $\overline{\Psi}$. By Lang's theorem in G_M, we can find $h \in G_M$ such that $h^F h^{-1} = \dot{w}$. On the other hand, g

Components := **function**(L)
  let H := MaximalToralSubalgebra(L)
  let $\mathcal{F}$ = GeneralisedRoots(L, H)
  for each $f \in \mathcal{F}$ **let** M_f be the subalgebra generated by L_f
  construct the graph with vertices $\mathcal{F}$
    and an edge (f, g) whenever $M_f \cap M_g$ is not contained in H
  let $C = \emptyset$
  for each graph component c **do**
    add the subalgebra $\langle M_f \mid f \in c \rangle$ to C
  end for
  return C
end function

Algorithm 7. Direct sum components

satisfies $g^F g^{-1} = t\dot{w}$ for some $t \in T_0$. Now the map $\dot{w}F$ is a nonstandard Frobenius endomorphism since $\dot{w}^F = \dot{w}$ and so $(\dot{w}F)^m = F^m$, where m is the order of $\dot{w}$. Furthermore ${T_0}^{\dot{w}F} = T_0$. So, by Lang's theorem in T_0, there is a $u \in T_0$ such that $t = u^{\dot{w}F} u^{-1}$. Set $\tilde{g} = u^{-\dot{w}} g$, so that

$$\tilde{g}^F \tilde{g}^{-1} = u^{-\dot{w}F} g^F g^{-1} u^{\dot{w}} = u^{-\dot{w}F} t u \dot{w} = \dot{w}$$

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

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

and M is split fundamental by Theorem 5.4(2). □

An immediate application is Algorithm 7 for computing the direct sum decomposition of a Lie algebra L. Although more than one w-orbit of Φ can have the same generalised root, this clearly is not possible for orbits in different components of Φ. The components returned are fundamental subalgebras.

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

Proposition 5.6. *Suppose that the characteristic of k is greater than 3. Let M be a split fundamental subalgebra of L. Let K be a split maximal toral subalgebra of M. Then $C_L(K)$ is a split fundamental subalgebra of L with full rank n. Hence a split maximal toral subalgebra of $C_L(K)$ is also a split maximal toral subalgebra of L.*

Proof. Let G_M be the split fundamental subgroup of G such that $L(G_M) = M$. Let T be a split maximal torus of G which normalises G_M and let $H = L(T)$. Then $U = G_M \cap T$ is a split maximal torus of G_M. By Theorem 5.1(6), we can assume without loss of generality that $K = L(U)$.

Let $C = C_G(U)$. Clearly C is normalised by T and it is reductive by [Hum75, Corollary 26.2A], hence it is split fundamental.

Let Ψ be the subset of $\Phi = \Phi(G, T)$ consisting of roots of G_M, or equivalently of M. Let Ψ' be the elements of Φ which are orthogonal to all elements of Ψ. Then

SplitMaximalToralSubalgebra := **function**(L, Z) $\qquad [Z \leq Z(L)]$
  repeat
    let $H/Z =$ MaximalToralSubalgebra(L/Z)
    if H is split **then return** H
    let $\mathcal{F} =$ GeneralisedRoots$(L/Z, H/Z)$
    for each $f \in \mathcal{F}$ **compute** $M_f = \phi(\langle (L/Z)_f \rangle)$
  until we find $A \subseteq \mathcal{F}$ such that $M_A = \langle \sum_{f \in A} M_f \rangle < L$ is split fundamental
  let $H_A =$ SplitMaximalToralSubalgebra$(M_A, \phi(Z(M_A/Z)))$
  let $C_A = \phi(C_{L/Z}(H_A))$ and $Z = \phi(Z(C_A/Z))$
  let $K = Z$
  for M in Components(C_A, Z) **do**
    let $K = K +$ SplitMaximalToralSubalgebra(M, Z)
  end for
  return K
end function

ALGORITHM 8. Finding a split maximal toral subalgebra

Ψ' is the root system of C and

$$L(C) = H \oplus \bigoplus_{\alpha \in \Psi'} L_\alpha.$$

Clearly $L(C) \leq C_L(K)$.

Conversely, suppose $x \in C_L(K)$. Let $\{e_\alpha, h_i\}$ be a Chevalley basis of L with respect to H and write

$$x = \sum_{i=1}^{n} t_i h_i + \sum_{\alpha \in \Phi} a_\alpha e_\alpha.$$

If $\alpha \notin \Psi'$ then there exists $\beta \in \Psi$ such that $\langle \alpha, \beta^\star \rangle \neq 0$. By the basic properties of root data $|\langle \alpha, \beta^\star \rangle| \leq 3$, so $\langle \alpha, \beta^\star \rangle$ is still nonzero considered as an element of k. Now $h_\beta = [e_{-\beta}, e_\beta]$ is in K, and so $[x, h_\beta] = 0$. But the coefficient of e_α in $[x, h_\beta]$ is $a_\alpha \langle \alpha, \beta^\star \rangle$ by (2). Hence $a_\alpha = 0$ for all $\alpha \notin \Psi'$ and so $x \in L(C)$.

The second conclusion is an immediate consequence of the first. □

We now have a method for finding split maximal toral subalgebras of L: Find a maximal toral subalgebra H, and compute its generalised roots. For each generalised root f, construct the subalgebra M_f generated by L_f. Now, assuming that we can find $A \subseteq \mathcal{F}$ for which $M_A = \langle \sum_{f \in A} M_f \rangle$ is known to be split fundamental and strictly contained in L, find a split maximal toral subalgebra H_A of M_A. By Proposition 5.6, a split maximal toral subalgebra of $C_L(H_A)$ is a split maximal toral subalgebra of L. Since M_A and $C_L(H_A)$ are split fundamental subalgebras of L, Theorem 5.4(2) ensures that they are also the Lie algebras of k-split connected reductive algebraic groups and so this recursion is valid. Algorithm 8 gives the precise method we use. Note that the second argument Z passed to this function is intended to indicate that we have a basis of $L(k)$ extending a basis of $Z(k)$, and the pullback map $\phi : L/Z \to L$. We take $Z = Z(L)$ initially. In Section 6, we give a method for ensuring that M_A is known to be split fundamental.

5.5. **Finding a Chevalley basis.** We start by giving a recognition theorem for a standard Chevalley basis.

Theorem 5.7. *Suppose the finite field k has characteristicgreater than 3. Let G be a k-split connected reductive linear algebraic group defined over k and let L be the Lie algebra of G. Let H be a k-split maximal toral subalgebra of L and let $L = H \bigoplus_\alpha L_\alpha$ be the root decomposition of L. Suppose we have a basis of L consisting of $h_i \in H$ for $i = 1, \ldots, n$ and $e_\alpha \in L_\alpha$ for $\alpha \in \Phi$. Further suppose this basis satisfies the equation*

$$[e_{-\alpha}, e_\alpha] = \sum_{i=1}^{n} \langle e_i, \alpha^\star \rangle h_i$$

for every simple root α and the equations

$$[e_\alpha, e_\beta] = N_{\alpha\beta} e_{\alpha+\beta} \quad \text{and} \quad [e_{-\alpha}, e_{-\beta}] = N_{-\alpha,-\beta} e_{-\alpha-\beta}$$

for every extraspecial pair (α, β). Then this is a standard Chevalley basis.

Proof. We need to prove that this basis satisfies the defining equations given in Subsection 4.3. Equation (1) follow from the fact that a toral subalgebra is abelian, Equation (1) is given, and the Equation (4) follows from [Car72, Theorem 4.2.1]. It remains to prove Equation (2).

For $y \in Y$, define $h_y = \sum_{i=1}^n \langle e_i, y \rangle h_i \in H(k)$. It suffices to prove that

$$[e_\alpha, h_y] = \langle \alpha, y \rangle \, e_\alpha, \tag{9}$$

for some collection of elements y generating Y.

Now (9) is true for all $y \in \Phi^\star$ by [Car72, Theorem 4.2.1]. If $\langle \alpha, y \rangle = 0$ for all $\alpha \in \Phi$, then h_y is central and so (9) is trivially true. Together, these two kinds of element generate Y and so we are done. □

A consequence of this theorem is Algorithm 9 for finding a Chevalley basis of L. Note that for an extraspecial pair (α, β), we have $0 < N_{\alpha\beta} \leq 3$, so division by $N_{\alpha\beta}$ is not a problem. The basis $\{h_i\}$ can be computed by elementary linear algebra. Note that in the second for-loop, the roots are taken in the linear order $<$ of Subsection 4.3, thus ensuring that e_α and e_β are already known when we compute e_γ.

6. 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. Subsection 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 6.3.

Throughout this section, n is the reductive rank of G, ℓ 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].

StandardChevalleyBasis := **function**(L)
  let H = SplitMaximalToralSubalgebra(L)
  compute the root system Φ and root spaces L_α for $\alpha \in \Phi$
  find simple roots $\alpha_1, \dots, \alpha_\ell$ for Φ
  for $i = 1, \dots, \ell$ **do**
    let $\alpha = \alpha_i$
    choose nonzero $e_\alpha \in L_\alpha$ and $f_\alpha \in L_{-\alpha}$
    find $a \in k$ such that $[e_\alpha, [f_\alpha, e_\alpha]] = 2ae_\alpha$
    let $e_{-\alpha} = f_\alpha / a$, $h_\alpha = [e_{-\alpha}, e_\alpha]$
  end for
  compute a basis $\{h_i\}$ for $H(k)$ with $h_\alpha = \sum_i \langle e_i, \alpha^\star \rangle h_i$ for simple roots α
  for γ a nonsimple root **do**
    let (α, β) be the extraspecial pair of γ
    let $e_\gamma = [e_\alpha, e_\beta]/N_{\alpha\beta}$, $e_{-\beta} = [e_{-\alpha}, e_{-\beta}]/N_{-\alpha,-\beta}$
  end for
  return $\{e_\alpha, h_i\}$
end function

ALGORITHM 9. Finding a standard Chevalley basis

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 Subsection 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 $L_{\text{rss},w}$ 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 $g^F g^{-1} \in T_0 \dot{w}$. 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 $(X, \Phi, Y, \Phi^\star)$. Let w be an element of the Weyl group W. Define*

$$Q_w(X) = \frac{\prod_{i=1}^{\ell}(1 - X^{d_i})}{\det_Y(1 - wX)}.$$

Then

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

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

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

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

which is in one-to-one correspondence with

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

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

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

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

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

Then H_α is a hyperplane in H_w and $(H_w)_{\mathrm{rss}} = H_w - \bigcup_{\alpha\in\Phi} H_\alpha$. Now ${H_\alpha}^F = H_{\alpha w}$, so $H_\alpha(k) = \left(\bigcap_j H_{\alpha w^j}\right)(k)$. 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

$$q^n \left(1 - \sum_{i=1}^{\ell} \frac{c_i}{q^i}\right) \leq |(H_w)_{\mathrm{rss}}(k)| \leq q^n.$$

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

$$\frac{|G(k)|}{|L(k)||T_w(k)|} = \frac{q^d \prod_i (1 - 1/q^{d_i})}{q^d \det_Y(qI - w)} = \frac{Q_w(1/q)}{q^n}.$$

□

The following useful lemma can be proved by elementary calculus.

Lemma 6.2. *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*

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

6.2. **Reflection derangements.** Recall from Subsection 5.2 that there is a relationship between between the generalised roots f with respect to a toral subalgebra and the orbits of the corresponding Weyl group element w on Φ. 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 α such that $\alpha w = \pm\alpha$. In other words, when a reflection s_α 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 Sym_m acting on m letters is known to approach $1/e$ as $m \to \infty$. 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 6.3. *If W is an irreducible Coxeter group of classical type* A_ℓ, $\mathrm{B}_\ell\,/\,\mathrm{C}_\ell$, *or* D_ℓ, *then the proportion of its reflection derangements approaches* $2e^{-3/2}$, $e^{-5/4}$, $2e^{-5/4}+(4e)^{-1}$, *respectively, as* $\ell \to \infty$. *For exceptional types, the proportions are as listed below:*

G_2	F_4	E_6	E_7	E_8
1/3	1/4	1409/2592	1646/2835	3385549/6220800

Proof. Denote by f the number of reflection derangements of W. We wish to determine $f/|W|$.

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

An element of 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

$$f = \left| R_m - \bigcup_{1\le i<j\le m} R_m^{i,j} \right|$$

where

$$R_m^{ij} = \{w \in R_m \mid w \text{ contains } (i,j)\}.$$

We compute f by inclusion/exclusion. As R_m^{ij} and $R_m^{ij'}$ 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, $|R_m| = d_m + m d_{m-1}/m$,

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

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

Writing S_ℓ for elements of W such that w^ϕ is a derangement and

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

we find that

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

Again, we can count f by taking alternating sums over h-tuples of commuting transpositions in W^ϕ. As each transposition in the decomposition of an element of w^ϕ corresponds to two 4-cycles as indicated above, we find an extra factor 2^h compared to the A_ℓ 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 $|W(\mathrm{B}_\ell)| = 2^\ell \ell!$, the required proportion tends to

$$\lim_{m\to\infty} \frac{f}{2^\ell \ell!} = \sum_{h=0}^{\infty} \left(-\frac{1}{4}\right)^h \frac{1}{h!}\frac{1}{e} = e^{-\frac{1}{4}} e^{-1} = e^{-\frac{5}{4}}.$$

Type D_ℓ: The Weyl group $W(\mathrm{D}_\ell)$ is the subgroup of $W(\mathrm{B}_\ell)$ consisting of all elements w such that $\prod_{i=1}^{\ell} iw$ 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 $\phi : W \to \mathrm{Sym}_\ell$ as the restriction of the map for type B_ℓ. Then $w \in W$ does not commute with any reflection if, and only if,

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

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

$$\lim_{\ell\to\infty} \frac{\binom{\ell}{2} 2^{\ell-2} d_{\ell-2} (\ell-2)!}{|W(\mathrm{D}_\ell)|} = \lim_{\ell\to\infty} 2^{-2} d_{\ell-2} = \frac{1}{4e}$$

to the required asymptotic proportion.

Writing T_ℓ for elements of W such that w^ϕ 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_ℓ case:

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

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

$$\sum_{h=0}^{\lfloor \ell/2 \rfloor} \left(-\frac{1}{4}\right)^h (d_{\ell-2h} + d_{\ell-2h-1})\,,$$

which contributes

$$\lim_{m\to\infty} \frac{f}{2^\ell \ell!} = \sum_{h=0}^{\infty} \left(-\frac{1}{4}\right)^h \frac{1}{h!}\frac{2}{e} = 2e^{-\frac{1}{4}}e^{-1} = 2e^{-\frac{5}{4}}$$

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

The exceptional types: These were computed by machine. □

Corollary 6.4. *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 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 $\left(\frac{2}{3}\right)^s \le \frac{2}{3}$. □

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 certain regular semisimple elements.

6.3. **Time analysis.** We 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*

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

where h *is the order of* w_c.

Proof. Suppose α 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 $m \ge \ell/2$ on a case-by-case basis:

Type A_ℓ**:** Identify W with $\mathrm{Sym}_{\ell+1}$ and consider Φ to consist of roots $e_i - e_j$ with $i \ne j$. 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 $\alpha, \ldots, \alpha {w_c}^m$ 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 $m \ge (\ell + 1)/2$.

A_ℓ	$\prod_{i=1}^{\ell}(1-X^i)$
$\mathrm{B}_\ell, \mathrm{C}_\ell$	$(1-X^\ell)\prod_{i=1}^{\ell-1}(1-X^{2i})$
D_ℓ	$\prod_{i\in\{1,\ell-1,\ell\}}(1-X^i)\prod_{i=2}^{\ell-2}(1-X^{2i})$
G_2	$(1-X^2)(1-X^3)(1+X)$
F_4	$(1-X^6)\prod_{i\in\{4,6,8\}}(1-X^i)$
E_6	$(1-X^6)\prod_{i\in\{1,4,5,6,8\}}(1-X^i)(1+X^3+X^6)$
E_7	$(1-X^6)\prod_{i\in\{1,6,8,10,12,14\}}(1-X^i)(1+X^3+X^6)$
E_8	$\prod_{i\in\{1,8,10,12,14,18,20,24\}}(1-X^i)(1+X^3)(1+X^5+X^{10})$

TABLE 1. The functions $Q_w(X)$ for a Coxeter element w

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

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

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

Type B_ℓ**:** The permutation action of $W(\mathrm{B}_\ell)$ on its roots is isomorphic to the action of $W(\mathrm{C}_\ell)$ on its roots, so the same argument works.

Types D_ℓ**:** Identify W with the elements of $W(\mathrm{C}_\ell)$ such that $\prod_{i=1}^{\ell}(iw) > 0$ and consider Φ to consist of the roots $\varepsilon e_i - \delta e_j$ with $\varepsilon,\delta \in \{\pm1\}$, $i,j = 1,\dots,\ell$ and $i \neq j$. We can take $w_c = (1,2,\dots,\ell-1,-1,-2,\dots,-\ell+1)(\ell,-\ell)$ and $\alpha = \varepsilon e_i - \delta e_j$. Once again $m \geq \ell/2$ if $i,j \neq \ell$. If $i = \ell$, $j \neq \ell$, then $\alpha {w_c}^m = (-1)^m \varepsilon e_\ell - \delta e_{j+m}$ 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 Φ 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 $1 - X^a$ appears more than twice in these polynomials and $q \geq 3$, it follows by Lemma 6.2 that $Q_{w_c}(1/q) \geq (1 - 1/q)^4$.

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 of rank greater than one. If W is classical with rank at least 7 then there is a reflection nonderangement*

Type	c	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8
A_1	2	1							
A_2	2	1	2						
B_2	8	4	0						
G_2	4	3	4						
A_3	8	2	4	0					
B_3	8	1	2	2					
A_4	6	1	2	0	2				
B_4	12	1	1	4	0				
D_4	16	5	8	0	0				
F_4	36	3	1	6	0				
A_5	8	1	1	2	4	0			
B_5	16	1	0	0	4	2			
D_5	16	3	5	2	4	0			
A_6	10	1	0	0	4	0	2		
B_6	20	1	0	0	2	5	0		
D_6	24	3	5	3	4	0	0		
E_6	36	3	0	3	2	6	0		
E_7	60	3	0	0	2	10	0	0	
E_8	108	3	0	0	0	0	4	9	0

TABLE 2. The constants c and c_i for small rank and exceptionals

w such that

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

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

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

with the constants c and c_i listed in Table 2.

Proof. Fix a root β. Assume β is short (resp. long) for Cartan type B_ℓ (resp. C_ℓ). Let $\Phi_\beta = \{\gamma \in \Phi \mid \langle \gamma, \beta^\star \rangle = 0\}$. Then Φ_β is a subsystem of W and, except in type D_4, it has at most two irreducible components. Let Φ'_β be the irreducible summand of Φ_β of maximal rank. Let s_β be the reflection in β and let w_β 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 $s_1s_2s_1s_3s_2s_1s_4s_2s_1s_3s_2$. (Here s_i is the ith simple reflection, with the numbering given in [Bou75].) These elements are all reflection nonderangements.

First we prove that

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

for the classical types of rank at least 7.

Type A_ℓ: Assume $\beta = e_1 - e_2$. Then Φ_β has type $A_{\ell-2}$, and so orbits within Φ_β contribute at most $\frac{\ell-2}{q^{(\ell-2)/2}}$ to the sum, as in the previous proof. If $\alpha \notin \Phi_\beta$, then

A_1	$1-X$
A_2	$1-X^3$
A_3	$(1-X)(1-X^3)(1+X^2)$
A_ℓ $(\ell>3)$	$\prod_{i\in\{1,\ldots,\ell+1\}\setminus\{2,\ell-1\}}(1-X^i)$
$\mathrm{B}_2,\mathrm{C}_2$	$(1-X)^2(1+X^2)$
$\mathrm{B}_3,\mathrm{C}_3$	$(1-X)(1-X^2)(1-X^6)$
$\mathrm{B}_4,\mathrm{C}_4$	$(1-X)(1-X^3)(1-X^4)(1-X^8)$
$\mathrm{B}_\ell,\mathrm{C}_\ell$ $(\ell>4)$	$(1-X)(1-X^{\ell-2})^{(3-(-1)^\ell)/2}\prod_{i\in\{2,\ldots,\ell\}\setminus\{\ell-1\}}(1-X^{2i})$
D_4	$(1-X)^2(1+X^6)(1+X^2)^2$
D_5	$(1-X)^3(1-X^5)(1-X^6)(1+X^2)(1+X^4)$
D_6	$(1-X)^3(1-X^3)(1-X^6)(1-X^{10})(1+X^2)^2(1+X^4)$
D_ℓ $(\ell>6)$	$(1-X)^3\prod_{i\in\{\ell-3,\ell\}}(1-X^i)\prod_{i\in\{4,\ldots,\ell-1\}\setminus\{\ell-3\}}(1-X^{2i})\times$ $(1+X^2)(1+X^2+X^4)$
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	$(1-X)^2\prod_{i\in\{6,12,14,20,24,30\}}(1-X^i)\times$ $(1+X^2)(1+X^4)(1+X^3+X^6)$

TABLE 3. The functions $Q_w(X)$

$\alpha=\pm(e_i-e_j)$ 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_ℓ **with** β **short:** Assume $\beta=e_1-e_2$. Then Φ_β has type $\mathrm{B}_{\ell-1}$, and so the orbits within Φ_β contribute at most $\frac{\ell-1}{q^{(\ell-1)/2}}$. If $\alpha\notin\Phi_\beta$, then $\alpha=\varepsilon e_i-\delta e_j$ 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_ℓ **with** β **long:** This is similar to type B_ℓ, with the short roots and long roots exchanged.

Type D_ℓ**:** Assume $\beta=e_1-e_2$. Then Φ_β has type $\mathrm{D}_{\ell-2}\,\mathrm{A}_1$ and Φ'_β is the subsystem of type $\mathrm{D}_{\ell-2}$. So the orbits within Φ'_β contribute at most $\frac{\ell-2}{q^{(\ell-1)/2}}$ to the sum. If $\alpha\notin\Phi'_\beta$, then $\alpha=\varepsilon e_i-\delta e_j$ 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. The constant c is just $|C_W(w)|$. The functions $Q_w(X)$ are given in Table 3. Applying Lemma 6.2, 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 $W(\Phi'_\beta)$ has order h_β, and the centraliser of w in W has order $2h_\beta\leq 4\ell$. The required result now follows from the first inequality of Proposition 6.1. □

```
SplitMaximalToralSubalgebra := function(L, Z)
  repeat
    let H/Z = MaximalToralSubalgebra(L/Z)               O(ℓ^6 log(q))
    if H is split then return H                          O(ℓ^7 log(q))
    let F = GeneralisedRoots(L/Z, H/Z)                   O(ℓ^7 log(ℓ) log^2(q))
    if there exists f ∈ F with deg(f) = 1 then
      let M/Z := ⟨φ((L/Z)_f + (L/Z)_{f_-})⟩              O(ℓ^6 log(q))
    elif there exists f ∈ F with deg(f) = 2 and f = f_- then
      let M/Z := ⟨φ((L/Z)_f⟩                             O(ℓ^6 log(q))
      if dim(M/Z) ≠ 3 then
        find α in Φ_f over k_2                           O(ℓ log^2(q))
        let M/Z = ⟨φ((L/Z)_α + (L/Z)_{-α})⟩              O(ℓ^6 log(q))
    end if
  until M is defined                                     O(ℓ log(ℓ)) times
  let H = SplitMaximalToralSubalgebra(M, φ(Z(M/Z)))
  let C = φ(C_{L/Z}(H)) and Z = φ(Z(C/Z))
  let K = Z
  for M in Components(C, H) do
    let K = K + SplitMaximalToralSubalgebra(M, Z)
  end for
  return K
end function
```

ALGORITHM 10. Finding a split maximal toral subalgebra

Finally we are in a position to give an analysis of our algorithm. We refer to Algorithm 10, a version of Algorithm 8 which searches for maximal toral subalgebras corresponding to reflection nonderangements. As discussed in Subsection 6.2, finding f with $\deg(f) = 1$, or $\deg(f) = 2$ and $f = f_-$ is equivalent to the corresponding Weyl group element being a reflection nonderangement. When $\deg(f) = 2$ and $f = f_-$, we have always found in practice that M/Z is of type A_1, and so has dimension 3. We do not have a proof of this however, so it is necessary to check and then decompose over the field extension k_2 in the unlikely event that we get a larger subalgebra.

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 $O(n^3\ell^6 \log^2(\ell)\log^2(q))$.*

Proof. Before calling Algorithm 10, we compute the centre of L, which takes time $O((n+\ell^2)^3 \log(q))$. Using Algorithm 7, we can assume G is simple. As indicated in Algorithm 10, the computations within the main loop take time $O(\ell^7 \log(\ell)\log^2(q))$.

By Proposition 6.6, if G is classical with rank at least 7, we obtain a split toral subalgebra M 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,

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

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 $\mathrm{D}_4(5)$. But for any fixed Lie algebra, it is easily seen that there is a nonzero chance of the algorithm working, since there is a chance that the toral subalgebra found by Algorithm 5 is already split. We have now 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/ℓ.

Since

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

we can choose a such that

$$\left(1 - \frac{C}{\ell}\right)^{a\ell} \leq \frac{1}{e^4}$$

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

$$\left(1 - \frac{C}{\ell}\right)^{a\ell\log(\ell)} \leq \left(\frac{1}{e^4}\right)^{\log(\ell)} = \frac{1}{\ell^4}.$$

Clearly the depth of recursion is at most ℓ, which contributes a further factor of ℓ to our timing. The ranks of all the subalgebras in all the calls at a particular depth sum to at most ℓ, so the total number of recursive calls is at most ℓ^2. Hence the overall probability of success is at least

$$\left(1 - \frac{1}{\ell^4}\right)^{\ell^2} \geq \left(1 - \frac{1}{2\ell^2}\right)^{\ell^2} \geq \frac{1}{2}.$$

Hence Algorithm 10 takes Las Vegas time $O(\ell^9 \log^2(\ell) \log^2(q))$. Combining this with the preprocessing time of $O((n + \ell^2)^3 \log(q))$, 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 $O(n^3\ell^6 \log^2(\ell) \log^2(q))$.*

Proof. The time taken to find a split maximal toral subalgebra clearly dominates the time for Algorithm 9. □

We can easily decompose G into simple subgroups, since we know its root datum. Hence, combining this corollary with Proposition 4.3, we see that the algorithm for Lang's Theorem takes Las Vegas time

$$O(n^3\ell^6 \log^2(\ell) \log^2(q) + n^8 r^2 s^2 \log^2(q)),$$

which is easily simplified to the expression in Theorem 1.2.

References

[Bab97] László Babai, *Randomization in group algorithms: conceptual questions*, Groups and computation, II (New Brunswick, NJ, 1995), Amer. Math. Soc., Providence, RI, 1997, pp. 1–17.

[Bou75] N. Bourbaki, *Éléments de mathématique*, Hermann, Paris, 1975, Fasc. XXXVIII: Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées, Actualités Scientifiques et Industrielles, No. 1364.

[Car72] Roger W. Carter, *Simple groups of Lie type*, John Wiley & Sons, London-New York-Sydney, 1972, Pure and Applied Mathematics, Vol. 28.

[Car93] ———, *Finite groups of Lie type*, John Wiley & Sons Ltd., Chichester, 1993, Conjugacy classes and complex characters, Reprint of the 1985 original, A Wiley-Interscience Publication.

[CLG97] Frank Celler and C. R. Leedham-Green, *Calculating the order of an invertible matrix*, Groups and computation, II (New Brunswick, NJ, 1995), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 28, Amer. Math. Soc., Providence, RI, 1997, pp. 55–60. MR MR1444130 (98g:20001)

[CMT04] Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor, *Computing in groups of Lie type*, Math. Comp. **73** (2004), 1477–1498.

[dGIR96] Willem de Graaf, Gábor Ivanyos, and Lajos Rónyai, *Computing Cartan subalgebras of Lie algebras*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 5, 339–349. MR 98m:17001

[GH97] S. P. Glasby and R. B. Howlett, *Writing representations over minimal fields*, Comm. Algebra **25** (1997), no. 6, 1703–1711. MR 98c:20019

[Gro02] Larry C. Grove, *Classical groups and geometric algebra*, Graduate Studies in Mathematics, vol. 39, American Mathematical Society, Providence, RI, 2002. MR MR1859189 (2002m:20071)

[Hog82] G. M. D. Hogeweij, *Almost-classical Lie algebras. I, II*, Nederl. Akad. Wetensch. Indag. Math. **44** (1982), no. 4, 441–452, 453–460. MR MR683531 (84f:17007)

[Hum67] James E. Humphreys, *Algebraic groups and modular Lie algebras*, Memoirs of the American Mathematical Society, No. 71, American Mathematical Society, Providence, R.I., 1967. MR 36 #169

[Hum75] ———, *Linear algebraic groups*, Springer-Verlag, New York, 1975, Graduate Texts in Mathematics, No. 21.

[Hum78] ———, *Introduction to Lie algebras and representation theory*, Springer-Verlag, New York, 1978, Second printing, revised. MR 81b:17007

[Jac62] Nathan Jacobson, *Lie algebras*, Interscience Publishers (a division of John Wiley & Sons), New York-London, 1962, Interscience Tracts in Pure and Applied Mathematics, No. 10.

[Leh92] G. I. Lehrer, *Rational tori, semisimple orbits and the topology of hyperplane complements*, Comment. Math. Helv. **67** (1992), no. 2, 226–251. MR 93e:20065

[Leh98] ———, *The cohomology of the regular semisimple variety*, J. Algebra **199** (1998), no. 2, 666–689. MR MR1489931 (98k:20080)

[LN97] Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn. MR 97i:11115

[Mül03] Peter Müller, *Algebraic groups over finite fields, a quick proof of Lang's theorem*, Proc. Amer. Math. Soc. **131** (2003), no. 2, 369–370 (electronic). MR 2003i:20088

[Ryb99] A. J. E. Ryba, *A new method for recognising groups of lie type*, Seminar given a Groups and Computation III, Ohio State University, June 15–19, 1999.

[Sel67] George B. Seligman, *Some results on Lie p-algebras*, Bull. Amer. Math. Soc. **73** (1967), 528–530. MR MR0219585 (36 #2664)

[Spr98] T. A. Springer, *Linear algebraic groups*, second ed., Birkhäuser Boston Inc., Boston, MA, 1998.

[SV00] Tonny A. Springer and Ferdinand D. Veldkamp, *Octonions, Jordan algebras and exceptional groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000. MR MR1763974 (2001f:17006) [vzGG03] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, second ed., Cambridge University Press, Cambridge, 2003. MR MR2001757 (2004g:68202)