ESSENTIAL p-DIMENSION OF THE NORMALIZER OF A MAXIMAL TORUS

MARK L. MacDONALD

Abstract. We compute the exact value for the essential p-dimension of the normalizer of a split maximal torus for most simple connected linear algebraic groups. These values give new upper bounds on the essential p-dimension of some simple groups, including some exceptional groups.

For each connected simple algebraic group, we also give an upper bound on the essential p-dimension of any torus contained in that group. These results are achieved by a detailed case-by-case analysis.

Introduction

Let p be a prime, k a field of characteristic not p (an assumption we make on all base fields), and let G be a split simple algebraic group over k. For us a *simple algebraic group* is connected, linear, and has no proper connected normal subgroups. Then one can ask what is the essential p-dimension of the normalizer of a split maximal torus in G, $\mathrm{ed}(N;p)$? This question was answered in [MR09] for $G = PGL_n$. Their main motivation came from the upper bound $\mathrm{ed}(G;p) \leq \mathrm{ed}(N;p)$. In the present paper we give exact values for $\mathrm{ed}(N;p)$ for most split simple algebraic groups G. These results are consistent with Reichstein's conjecture (see [Re10]). In some cases we obtain new bounds on $\mathrm{ed}(G;p)$. We also obtain upper bounds for the essential p-dimension of any torus inside a given (not necessarily split) simple algebraic group (see Theorem 1.7).

The four Tables in this paper summarize our main results, which follow from a detailed case-by-case analysis. In the remainder of this introduction, we explain how these tables give new information about essential dimension.

0.1. **Essential dimension of normalizers.** The essential dimension (resp. essential p-dimension) of an algebraic group G over a field k is a non-negative integer invariant, denoted by $\mathrm{ed}_k(G)$ (resp. $\mathrm{ed}_k(G;p)$). Roughly speaking, it is the number of independent parameters needed to specify a G-torsor up to isomorphism (resp. and allowing for prime to p field extensions). In recent years, much work has gone into computing these numbers (see [Re10] for a recent survey).

Let $T \subset G$ be a split maximal torus in a simple algebraic group over a field k. Let $N = N_G(T)$ be its normalizer, then $N/T \cong W = W(R)$ the Weyl group of the root system R of G.

For p any prime, computing $\mathrm{ed}(N;p)$ is roughly equivalent to computing the symmetric p-rank, $\mathrm{SymRank}(\phi;p)$, of the Weyl group action on the characters of a split maximal torus (see Definition 1.1). We will now explain how to find the exact value of, or at least the best bounds for $\mathrm{ed}(N;p)$.

Every split simple algebraic group G has an entry in Table I, II, or III (with the exception of Remark 2.3). For a prime p, the pair (G,p) occurs in the Tables iff the representation ${}^1\hat{T}$ has symmetric p-rank strictly bigger than the rank of T. So if the pair (G,p) does not occur in the Tables, then by Theorem 1.9 we have $\mathrm{ed}(N;p) = \mathrm{ed}(W;p)$. The essential p-dimensions of the Weyl groups are evaluated in Table IV.

If the pair (G,p) has an entry in one of these Tables, and the final column of this entry contains a "y", then by Corollory 1.11 we have that $\mathrm{ed}(N;p) = \mathrm{SymRank}({}^1\hat{T};p) - \dim(T)$. The only remaining possibility is that the final column of this entry contains an "n", in which case the exact value for $\mathrm{ed}(N;p)$ is not always known; see Theorem 1.9 for upper and lower bounds, and the final section for a discussion of individual cases.

This work extends the results of [MR09], where $\mathrm{ed}(N;p)$ was computed for $G = PGL_n$, which appears in Table I as the cases ${}^1A^{+1}_{p^r-1}$ and ${}^1A^{+1}_{p^rs-1}$ (using notation of 1.2).

0.2. **New upper bounds for** $\mathrm{ed}(G;p)$**.** By [Se02, III.4.3 Lemma 6][1] together with [BF03, Lemma 1.3] we have

$$\mathrm{ed}(G;p) \leq \mathrm{ed}(N;p).$$

In some cases this bound is sharp, such as $G = SO_{2n+1}$, $p = 2$, but in other cases the inequality is known to be strict. Nevertheless, it sometimes provides the best known upper bound for $\mathrm{ed}(G;p)$. In the following cases, the best bounds which had previously been written down were also bounds for the absolute essential dimension, given in [Le04]. For the classical groups:

$$\mathrm{ed}(PSO_{2n};2), \mathrm{ed}(PSp_{2n};2) \leq \begin{cases} 4\cdot 2^r(s-1) & \text{for } n = 2^r s, s > 1, \\ n^2 & \text{for } n = 2^r. \end{cases}$$

For n odd we already knew $\mathrm{ed}(PSp_{2n};2) = n+1$, [Mac08]. Let E_n denote the split adjoint group of type E_n, then we have:

$$\begin{array}{llll} \mathrm{ed}(E_6;3) \leq 21 & \mathrm{ed}(2E_7;2) \leq 33 & \mathrm{ed}(E_7;2) \leq 57 \\ \mathrm{ed}(E_8;2) \leq 120 & \mathrm{ed}(E_8;3) \leq 73. \end{array}$$

1. Preliminaries

The *rank* of a free $\mathbb{Z}$-module L is defined to be the minimal size of a generating subset of L. If F is a finite group which acts on L (in other words $\phi : F \to \mathrm{GL}(L)$ is an integral representation), then we can define the *symmetric rank*.

$$\mathrm{SymRank}(\phi) := \min\{ \text{ size of an } F\text{-invariant subset of } L \text{ which is generating}\}.$$

For example, if F is the Weyl group of some irreducible root system R, and ϕ is the induced action on the root lattice L, then $\mathrm{SymRank}(\phi) = |R_0|$, the number of roots of minimal length. This follows from a case-by-case analysis as in [Le04]. Notice that the Weyl group acts transitively on the minimal length roots.

In the present paper we will be interested in the p-local version of this invariant, for a prime p. We will say a subset $\Lambda \subset L$ is *p-generating* if it generates a $\mathbb{Z}$-submodule

[1] This Lemma assumes the base field is perfect, but in our case this assumption can be dropped.

X_Λ whose rank is $\operatorname{rank} L$, and whose index (defined as $|L/X_\Lambda|$) is prime to p. Choose a Sylow p-subgroup $\Gamma \subset F$.

Definition 1.1. The *symmetric p-rank* of ϕ is defined as

$$\operatorname{SymRank}(\phi; p) := \min\{ \text{ size of a } \Gamma\text{-invariant subset of } L \text{ which is } p\text{-generating}\}.$$

Notice that this number depends only on the integral representation ϕ, and the prime p, and not on the choice of Sylow p-subgroup (since all Sylow subgroups are conjugate). Clearly we have

$$\operatorname{rank}(\phi) \leq \operatorname{SymRank}(\phi; p) \leq \operatorname{SymRank}(\phi) \leq |F| \operatorname{rank}(\phi).$$

1.2. **Lattices.** A *lattice* is often defined as a free $\mathbb{Z}$-module with a positive-definite bilinear form. In the present paper, all lattices come from some irreducible root system, as the root lattice, the weight lattice, or as some intermediate lattice (see [Bou68], [Hu92]). Notice that different root systems may produce isomorphic lattices.

Given an irreducible root system R, its group of automorphisms obeys $A(R) = W(R) \rtimes \operatorname{Aut}(D)$, where $W(R)$ is the Weyl group and $\operatorname{Aut}(D)$ is the group of graph automorphisms of the Dynkin diagram. If L is some lattice associated to R, then $A(R)$ has an induced action on L.

Let M_r denote the (unique) subgroup of $\operatorname{Aut}(D)$ of order r. We will imitate the notation of [Ti66] for the following integral representation, given by the restriction of the induced $A(R)$ action

$$ {}^rL := \phi : W \rtimes M_r \to \operatorname{GL}(L). \tag{1.3}$$

1.3If L is a root lattice of type A, D, or E, then L^{+d} will denote an intermediate lattice in which L has index d (this is unique, except for type D, and $d = 2$, see Section 3). This follows the notation of [CS88].

We find it convenient to embed our lattices L inside a real vector space, with a fixed orthonormal basis $\{\epsilon_i\}$.

1.4. **Algebraic tori.** An *(algebraic) torus* over a field k is an algebraic group T such that $T_{\text{sep}} := T \times \operatorname{Spec}(k_{\text{sep}})$ is isomorphic to some copies of the multiplicative group $\mathbb{G}_m$ (see [Vo98] or [Bo92]). A torus which is isomorphic to $\mathbb{G}_m^n$ over k will be called *split*. Any torus becomes split after a finite Galois extension K. For any torus T defined over k, let $A_T := \operatorname{Gal}(K/k)$, where K is a minimal Galois splitting field of T. Then A_T is well-defined, and it is called the *decomposition group* of T. A_T naturally acts on the character module $\hat{T} = \operatorname{Hom}(T(K), K^*)$, and we can associate the *Galois representation* $\psi_T : A_T \to \operatorname{GL}(\hat{T})$. The main result from [LMMR10b, Cor. 5.1] is that

$$\operatorname{ed}(T; p) = \operatorname{SymRank}(\psi_T; p) - \dim T. \tag{1.5}$$

A torus T whose character representation obeys $\operatorname{SymRank}(\psi_T) = \dim(T)$ is called *quasi-split*. If we can choose a maximal torus $T \subset G$ which is (quasi-)split, then G is said to be (quasi-)split. We also know that $\operatorname{ed}(T) \leq \operatorname{SymRank}(\psi_T) - \dim T$, but equality does not always hold (there are non-quasi-split tori with $\operatorname{ed}(T) = 0$).

1.6. **Tori in algebraic groups; generic tori.** Let $T \subset G$ be a maximal torus in a simple algebraic group. Then any element of the decomposition group A_T acts on $\hat{T}$ by preserving the root system R of G_{sep}. In other words, $A_T \subset A(R)$. Notice that the integral representation ${}^r\hat{T}$ from (1.3) is independent of whether T splits, and depends only on G_{sep} and r.

Theorem 1.7. *Let $T_0 \subset G$ be any torus in a simple algebraic group over k, and let $r = |\operatorname{Aut}(D)|$ for the Dynkin diagram associated to the root system of G_{sep}. Choose a maximal torus T which contains T_0. Then*

$$\operatorname{ed}(T_0; p) = \operatorname{SymRank}(\psi_{T_0}; p) - \dim(T_0) \leq \operatorname{SymRank}({}^r\hat{T}; p) - \dim(T_0).$$

Moreover, if $\operatorname{char}(k) = 0$ then there exists a field extension K/k and a "generic" maximal torus $T_0 \subset G_K$ which achieves this upper bound.

Proof. We can choose a Sylow p-subgroup $\Gamma_0 \subset A_{T_0}$ contained in a Sylow p-subgroup $\Gamma \subset A(R)$. Then a Γ-invariant p-generating subset of $\hat{T}$ induces a Γ_0-invariant p-generating subset of $\hat{T}_0$, as required.

Now we will show that the upper bound is achieved for generic tori. Given a quasi-split maximal torus $T \subset G$, with N its normalizer, then the variety G/N may be thought of as the variety of maximal tori in G, and we can construct the tautological fibration $S \to G/N$. The fibre over a point $x \in G/N$ is a maximal torus $S_x \subset G_{k(x)}$. The fibre over the generic point is called the *generic torus*, and we will denote it $T_{\text{gen}} \subset G_{k(G/N)}$. Voskresenskii showed that, for $\operatorname{char}(k) = 0$, we have $A_{T_{\text{gen}}} \cong W(R) \rtimes A_T$ [Vo88, Theorem 2].

We can choose a quasi-split maximal torus $T \subset G_{k'}$ for some field extension k'/k, such that $r := |A_T| = |\operatorname{Aut}(D)|$. By (1.5) we have $\operatorname{ed}_K(T_{\text{gen}}; p) = \operatorname{SymRank}({}^r\hat{T}; p) - \dim(T)$ for $K = k'(G/N)$. Hence the upper bound is achieved for $T_0 = T_{\text{gen}}$. □

Theorem 1.7 gives us motivation to compute the symmetric p-rank of the $A(R)$-action on the character lattices; the results can be found in Tables I, II, and III.

1.8. **Normalizers of split tori.** A representation $\phi : N \to \operatorname{GL}(V)$ is said to be *p-faithful* (resp. *p-generically free*), if $\ker(\phi)$ is finite of order prime to p, and ϕ descends to a faithful (resp. generically free) representation of $N/\ker(\phi)$.

For the remainder of this section we will assume $T \subset G$ is a split maximal torus in a simple algebraic group over k, and $N = N_G(T)$, and $W = W(R) \cong N/T$, where R is the root system of G. Also, H will denote a Sylow p-subgroup of W.

Theorem 1.9. *Let $T \subset G$ be a maximal and split torus over k, let N be its normalizer, and ${}^1\hat{T}$ the representation of the Weyl group from* (1.3)*. Then we have the lower bounds:*

$$\max\{\operatorname{SymRank}({}^1\hat{T}; p) - \dim(T), \operatorname{ed}(W; p)\} \leq \operatorname{ed}(N; p)$$

We also have the upper bound:

$$\operatorname{ed}(N; p) \leq \operatorname{SymRank}({}^1\hat{T}; p) - \dim(T) + \operatorname{ed}(W; p).$$

In particular, if $\operatorname{SymRank}({}^1\hat{T}; p) = \dim(T)$ then $\operatorname{ed}(N; p) = \operatorname{ed}(W; p)$.

For the values of $\mathrm{SymRank}({}^1\hat{T};p)$ see Tables I,II, and III, and for $\mathrm{ed}(W;p)$ see Table IV. Notice that $\mathrm{ed}(N;p)>0$ iff p divides the order of W.

Proof of lower bounds in Theorem 1.9. Firstly, notice that $\mathrm{ed}(W;p)\leq\mathrm{ed}(N;p)$ follows from the surjection $H^1(k,N)\to H^1(k,W)$ for quasi-split groups (see [Gi04, Thm. 5.1] or [Ra04]).

For a Sylow p-subgroup $H\subset W$, let N_H denote the preimage of H in N. Then by [MR09, Lemma 4.1] we have that $\mathrm{ed}(N_H;p)=\mathrm{ed}(N;p)$. From [LMMR10a, Thm. 1.3(a)] we know there is a p-faithful $(N_H)_{\mathrm{alg}}$-representation V, defined of over an algebraic closure, such that $\dim(V)-\dim(T)\leq\mathrm{ed}_k(N_H;p)$. Such a representation is also a p-faithful T_{alg}-representation. Decompose $V=\oplus_{\lambda\in\Lambda}V_\lambda$ into weight spaces of T_{alg}, where $\Lambda\subset\hat{T}$ is the set of non-trivial weights. Now Λ is p-generating (since V is p-faithful), and it is invariant under H. Therefore $\mathrm{SymRank}({}^1\hat{T};p)\leq|\Lambda|\leq\dim(V)$, as required. □

We will prove the upper bound of Theorem 1.9 by constructing a generically free representation from a subset of $\hat{T}$. Let $\phi:F\to\mathrm{GL}(L)$ be a representation of a finite group, and let $\Lambda\subset L$ be an F-invariant subset. The following condition on Λ will ensure generic freeness in Lemma 1.10(iii).

(K_F): The kernel of the F-map $\mathbb{Z}[\Lambda]\to L$ is faithful as an F-module.

Fix a Sylow p-subgroup $H\subset W$, and let $N_H\subset N$ be its preimage under $\pi:N\to W$. The following construction slightly generalizes [MR09, Section 3], where only the case when N_H is a semi-direct product was considered.

Lemma 1.10. *Let T be a split torus over k, and let $\Lambda\subset\hat{T}$ be a finite H-invariant subset. Then there is an N_H-representation, V_Λ, obeying the following properties.*

(i) V_Λ has a basis $\{v_\lambda\}_{\lambda\in\Lambda}$, on which T acts by $tv_\lambda=\lambda(t)v_\lambda$,
(ii) Λ is p-generating iff V_Λ is p-faithful,
(iii) Λ is p-generating and satisfies (K_H) iff V_Λ is p-generically free.

Proof. Choose a set of representatives $\{\lambda_i\}\subset\Lambda$, one for each H-orbit; let $H_i:=\mathrm{Stab}_H(\lambda_i)$, and let N_i be the preimage of H_i in N_H. Now consider the irreducible G-representation $L(\lambda_i)$ of highest weight λ_i [Ja87, II 2.4]. Since elements of N permute the weight spaces of any representation, we can define $V_i:=L(\lambda_i)_{\lambda_i}$, a one-dimensional N_i-representation (see [Ja87, II 2.4 Prop. (b)]). This is defined over k because λ_i is (since T is split). Then define

$$V_\Lambda:=\oplus_i\,\mathrm{ind}_{N_i}^{N_H}(V_i).$$

For each i, the corresponding summand has a basis $\{v_\lambda\}_{\lambda\in H\cdot\lambda_i}$, where T acts as in (i).

For (ii), let M be the kernel of the representation $N_H\to\mathrm{GL}(V_\Lambda)$ defined above; notice that $M\subset T$. Also, $T\to\mathrm{GL}(V_\Lambda)$ factors through $\mathrm{Diag}(X_\Lambda)$, which acts faithfully on V_Λ. So by the anti-equivalence Diag, we see that $M\cong\mathrm{Diag}(\hat{T}/X_\Lambda)$. Therefore M is order prime to p iff Λ is p-generating.

To show (iii), first assume that Λ is generating. In this case, we know from [MR09, Lemma 3.3][2] that Λ satisfies (K_H) iff V_Λ is generically free. By (ii), the general case now follows. □

Proof of Thm. 1.9. All that remains is the upper bound; we want to construct a p-generically free representation of N_H of the right dimension (by [LMMR10a, Section 1]). Given a Sylow p-subgroup $H \subset W$, we can choose an H-invariant p-generating subset of minimal size $|\Lambda| = \mathrm{SymRank}({}^1\hat{T}; p)$. By Lemma 1.10 this gives us a p-faithful N_H-representation, V_Λ. Let V be a faithful H-representation of dimension $\mathrm{ed}(W; p)$ (which is possible by [KM08], extending the base field if necessary). Then, as in [MR09, Lemma 3.2], $V_\Lambda \times V$ is a p-generically free N_H-representation, and thus we have the required upper bound on $\mathrm{ed}(N; p) = \mathrm{ed}(N_H; p)$. □

Corollary 1.11. *Let $T \subset G$ be a split maximal torus, N its normalizer, and $H \subset W$ a Sylow p-subgroup. If a minimal H-invariant p-generating subset of $\hat{T}$ satisfies condition (K_H), then we have* $\mathrm{ed}(N; p) = \mathrm{SymRank}({}^1\hat{T}; p) - \dim(T)$.

Proof. By Lemma 1.10 we have an N_H-representation of dimension $\mathrm{SymRank}({}^1\hat{T}; p)$ which is p-generically free. The result now follows from the lower bound of Theorem 1.9 and [LMMR10a, Section 1]. □

For $F \subset A(R)$, we will now give a useful condition on an F-invariant subset $\Lambda \subset \hat{T}$ which will imply the condition (K_F). We will say that $\lambda_0 \in \Lambda$ is Λ-*independent* if for any $\lambda_0 \neq \lambda_1 \in \Lambda$ we can choose coefficients $a_\lambda \in \mathbb{Z}$ such that $\sum_{\lambda \in \Lambda} a_\lambda \lambda = 0 \in \hat{T}$ with $a_{\lambda_0} \neq 0$ and $a_{\lambda_1} = 0$.

Lemma 1.12. *Let $\Lambda \subset \hat{T}$ be an F-invariant subset, such that* $\mathrm{rank}(X_\Lambda) = \mathrm{rank}\,\hat{T}$. *If λ is Λ-independent, and $h \in F$, then $h \cdot \lambda$ is also Λ-independent. If every $\lambda \in \Lambda$ is Λ-independent, then Λ satisfies (K_F).*

Proof. The first statement is clear.

Assume every $\lambda \in \Lambda$ is Λ-independent. Take an $h \in F$ which acts trivially on the kernel of $\mathbb{Z}[\Lambda] \to \hat{T}$. For every linear dependency $\sum_{\lambda \in \Lambda} a_\lambda \lambda = 0 \in \hat{T}$, F permutes the elements $\{\lambda | a_\lambda \neq 0\}$. By assumption, this implies h fixes every $\lambda \in \Lambda$. The span of Λ is full rank, and $\hat{T}$ is a faithful F-module, so $\mathbb{Z}[\Lambda]$ is a faithful F-module, hence $h = 1$. □

Lemma 1.13. *Let $\phi : F \to \mathrm{GL}(L)$ be an integral representation of a finite group, and let $L' \subset L$ be an index prime to p sublattice (of equal rank). Then* $\mathrm{SymRank}(\phi; p) = \mathrm{SymRank}(\phi|_{L'}; p)$. *Also, if $\Gamma \subset F$ is a Sylow p-subgroup, then a minimal Γ-invariant p-generating subset of L satisfies (K_Γ) iff such a subset of L' satisfies (K_Γ).*

Proof. Firstly notice that if Λ is a minimal Γ-invariant p-generating subset of L', then Λ is also p-generating for L; so $\mathrm{SymRank}(\phi; p) \leq \mathrm{SymRank}(\phi|_{L'}; p)$. Now let Λ be a minimal Γ-invariant p-generating subset of L. If we multiply every element in Λ by the index $c = |L/L'|$, then $c\Lambda$ is Γ-invariant p-generating subset of L'. The final sentence of the Lemma now follows because $\ker(\mathbb{Z}[\Lambda] \to L)$ is a faithful Γ-module iff $\ker(\mathbb{Z}[c\Lambda] \to L')$ is. □

[2]They assume N_H is a semi-direct product of T and H, but an identical proof works in general.

2. Type A_n

We will view the lattice A_n as the $\mathbb{Z}$-submodule of $\mathrm{Span}_{\mathbb{Z}}(\{\epsilon_i\}_{i=1}^{n+1})$ of elements whose coordinates sum to zero. The Weyl group $W(A_n)$ is the symmetric group on $n+1$ letters, which acts by permuting the coordinates ϵ_i. Negation is an outer automorphism of order 2.

This A_n is the character lattice of a maximal torus in PGL_{n+1}. To obtain the weight lattice, and the other intermediate lattices, let $m|n+1$, and then adjoin the following vector:

$$v_m := \frac{1}{m}(1,\cdots,1) - (0,\cdots,0,1,\cdots 1). \tag{2.1}$$

Here the last $\frac{n+1}{m}$ coordinates in the second summand are 1's, so that the sum of the coordinates of v_m is zero. Define A_n^{+m} to be the span of A_n together with v_m. In particular A_n^{+1} is the root lattice, and $A_n^{+(n+1)}$ is the weight lattice.

We may define an isomorphism $A_n^{+m}/A_n^{+1} \cong \mathbb{Z}/m\mathbb{Z}$ by sending v_m to $1 \in \mathbb{Z}/m\mathbb{Z}$. Then, for any $\lambda \in A_n^{+m}$, we will denote by $g(\lambda) \in \mathbb{Z}/m\mathbb{Z}$ its projection to the quotient module, and we sometimes call this the *glue part*. Now one may check the following.

Lemma 2.2. *For $\lambda \in A_n^{+m}$, we have*

$$\lambda = \frac{g(\lambda)}{m}(1,\cdots,1) + (a_1,\cdots,a_{n+1}),$$

such that $a_i \in \mathbb{Z}$ and $\sum a_i = -g(\lambda)\frac{n+1}{m}$.

For the rest of this section we will write $n = p^r s - 1$, for s not divisible by p (and possibly equal to 1). Table I summarizes our computations of $\mathrm{SymRank}(\phi;p)$ for A_n-type representations (using the notation as in 1.2). In this table we assume $s \neq 1$, and that it is not divisible by p. The (K) column states whether the choice of minimal p-generating Γ-invariant subset satisfies (K_Γ). Also, SU_{n+1} denotes the quasi-split (and not split) simply connected simple group of type A_n (see [Ti66, p. 55]).

Remark 2.3. For $t|s$ and $k \leq r$, we have that $A_{p^r s-1}^{+p^k t} \subset A_{p^r s-1}^{+p^k}$ is a sublattice of index t, and hence prime to p. By Lemma 1.13, we have reduced to considering lattices with $t = 1$, because $\mathrm{SymRank}({}^1A_{p^r s-1}^{+p^k};p) = \mathrm{SymRank}({}^1A_{p^r s-1}^{+p^k t};p)$.

The Sylow p-subgroup $H_r := W(A_{p^r-1})^{(p)}$ is given by an iterated wreath product of cyclic p-groups, as in [MR09]. The H_r-action on $\mathbb{R}^{p^r}$ naturally partitions the p^r coordinates into blocks of size p^i, for $0 \leq i \leq r$. We will call these p^i-*blocks*, and we may consider them as elements of $\mathbb{R}^{p^i}$; for each i the number of p^i-blocks is p^{r-i}.

The H_r-action restricted to a single p^i-block is given by the $H_i := W(A_{p^i-1})^{(p)}$-action on $\mathbb{R}^{p^i}$. Two p^i-blocks are *equivalent* if there is an element of H_i that maps one into the other. We will say a p^i-block is j-*stable* if every p^j-block ($0 \leq j \leq i$) is equivalent to each other. We will call such a block *scalar* if it is 0-stable. If the coordinates are all integers, then we can consider the related terms mod p; for example, scalar mod p means all the coordinates are congruent mod p.

For $s \geq 1$ not divisible by p, we may partition the coordinates of $\mathbb{R}^{p^r s}$ into s different p^r-blocks. We choose a Sylow p-subgroup $H := W(A_{p^r s-1})^{(p)}$, such that H restricted

ϕ	G	p	Conditions	SymRank$(\phi;p)$	(K)
${}^1A^{+p^k}_{p^r-1}$	$\frac{SL_{p^r}}{\mu_{p^{r-k}}}$	$\neq 2$	$1 \leq k = r$	p^r	n
			$1 \leq k \leq r-1$	$p^{2r-1}+p^k$	y
			$k = 0, r \geq 2$	p^{2r-1}	y
			$k = 0, r = 1$	$p^{2r-1} = p$	n
${}^1A^{+2^k}_{2^r-1}$	$\frac{SL_{2^r}}{\mu_{2^{r-k}}}$	2	$1 \leq k = r$	2^r	n
			$2 \leq k = r-1$	$2^{2r-2}+2^k$	y
			$1 = k = r-1$	$2^{2r-2}+2^k = 6$	n
			$1 \leq k \leq r-2$	$2^{2r-1}+2^k$	y
			$k = 0, r \geq 2$	2^{2r-1}	y
			$k = 0, r = 1$	$2^{2r-1} = 2$	n
${}^2A^{+2^k}_{2^r-1}$	$\frac{SU_{2^r}}{\mu_{2^{r-k}}}$	2	$2 \leq k = r$	2^{r+1}	y
			$2 \leq k \leq r-1$	$2^{2r-1}+2^{k+1}$	y
			$1 = k \leq r-2$	$2^{2r-1}+2$	y
			$1 = k = r-1$	$2^{2r-2}+2^k = 6$	n
			$k = 0, r \geq 2$	2^{2r-1}	y
${}^1A^{+p^k}_{p^rs-1}$	$\frac{SL_{p^rs}}{\mu_{p^{r-k}s}}$	any	$1 \leq k = r$	$p^r s$	n
			$1 \leq k \leq r-1$	$p^{2r}(s-1)+p^k$	y
			$k = 0, r \geq 1$	$p^{2r}(s-1)$	y
${}^2A^{+2^k}_{2^rs-1}$	$\frac{SU_{2^rs}}{\mu_{2^{r-k}s}}$	2	$1 \leq k = r$	$2^{r+1}s$	y
			$1 \leq k \leq r-1$	$2^{2r+1}(s-1)+2^{k+1}$	y
			$k = 0, r \geq 1$	$2^{2r+1}(s-1)$	y
			$k = 0 = r$	$2^{2r+1}(s-1) = 2(s-1)$	n

TABLE I. A_n lattices

to any p^r-block is given by H_r (see [MR09]); so that $(H_r)^s \subset H$. For $s = 1$, we have $(H_r)^s = H$.

We will consider a map $\Sigma : \mathbb{R}^{p^r s} \to \mathbb{R}^{p^{r-1}s}$, whose i^{th} coordinate is given by the sum of the coordinates of the i^{th} p-block. We will abuse notation slightly and write compositions of such maps as $\Sigma^i : \mathbb{R}^{p^r s} \to \mathbb{R}^{p^{r-i}s}$. In particular, if $s = 1$, then Σ^r is simply the sum of all coordinates.

Lemma 2.4. *Let $\lambda \in \mathbb{R}^{p^r s}$, where s is not divisible by p. For any $0 \leq i \leq r$, we have*

$$|(H_r)^s \lambda| \geq |\Sigma^i((H_r)^s \lambda)| \cdot |(H_i)^{p^{r-i}s} \lambda|.$$

Proof. Notice that $(H_i)^{p^{r-i}s}$ stabilizes the fibers of Σ^i. The result follows. □

Lemma 2.5. *Let $\lambda \in \mathbb{R}^{p^r s}$, where s is not divisible by p. If λ contains a non-scalar p^k-block ($k \leq r$), then $|(H_r)^s \lambda| \geq p^{r-k+1}$.*

Proof. First we prove the lemma for $k = 1$. Assume there is a non-scalar p-block, say B_1. For all $1 \leq i \leq r$, let B_i be the unique p^i-block which contains B_1.

To get a lower bound on the number of non-scalar p-blocks, start with the block B_1, which is non-scalar. If B_2 is 1-stable, then we know there are at least p non-scalar p-blocks, since the other p-blocks in B_2 must also be non-scalar. Similarly, for each i

such that B_i is not $(i-1)$-stable, we get another factor of p. Let m be the number of indices $1 \le i \le r$ for which B_i is $(i-1)$-stable. Then there are at least p^m non-scalar p-blocks in λ.

Now we also have $r-m-1$ indices $i \ge 2$ for which the p^{i-1}-blocks in B_i are not equivalent. For such an i, the p inequivalent blocks in B_i are cyclically permuted by $\mathbb{Z}/p \subset (H_r)^s$, and have different images under Σ^1. Now we can apply Lemma 2.4 to get

$$|(H_r)^s\lambda| \ge |\Sigma^1((H_r)^s\lambda)| \cdot |(H_1)^{p^{r-1}s}\lambda| \ge p^{r-m-1}p^{p^m} \ge p^{r-m-1}p^{m+1} = p^r.$$

Here we have used the inequality $p^m \ge m+1$, which is valid for $m \ge 0$ and $p \ge 2$. This proves the $k=1$ case.

Now assume λ contains a non-scalar p^k-block. If $k=1$, then we have already shown the result, so assume every p-block is scalar. Then $|(H_r)^s\lambda| = |\Sigma^1((H_r)^s\lambda)| = |(H_{r-1})^s\Sigma^1(\lambda)|$, and $\Sigma(\lambda)$ contains a non-scalar p^{k-1}-block. So, by induction, $|(H_r)^s\lambda| \ge p^{(r-1)-(k-1)-1} = p^{r-k-1}$. □

Lemma 2.6. *Let $p=2$ and $k \ge 2$. For then any $\lambda \in A^{+2^k}_{2^r s-1}$ such that s and $g(\lambda)$ are both odd, we have $-\lambda \notin H \cdot \lambda$. In other words, the $(H \times \mathbb{Z}/2)$-orbit of λ is strictly bigger than the H-orbit.*

Proof. This is simply because $g(h\lambda) \equiv g(\lambda) \bmod 2^k$, but $g(-\lambda) \equiv -g(\lambda) \not\equiv g(\lambda) \bmod 2^k$. □

Lemma 2.7. *Let $\lambda \in A^{+p^k}_{p^r s-1}$, with s not divisible by p, and $g(\lambda) \not\equiv 0$ mod p.*

(i) Then $|H\lambda| \ge p^k$.
(ii) If $p=2$, and either $k \ge 2$ or $s > 1$ then $|(H \times \mathbb{Z}/2)\lambda| \ge 2^{k+1}$.

Proof. By Lemma 2.2, we have $\lambda = \frac{g(\lambda)}{p^k}(1, \cdots, 1) + (a_1, \cdots, a_{p^r s})$, such that $\sum a_i = -g(\lambda)p^{r-k}s$, and $a_i \in \mathbb{Z}$. Here $\sum a_i$ is not divisible by p^{r-k+1}, so there is a p^{r-k+1}-block which is non-scalar, and hence by Lemma 2.5 we have $|H\lambda| \ge p^{r-(r-k+1)+1} = p^k$.

The $p=2$, $k \ge 2$ case now follows, because the $(H \times \mathbb{Z}/2)$-orbit has order a power of 2, and is strictly bigger than the H-orbit, by Lemma 2.6.

For $p=2$, $s>1$, we have the H_r-orbit of some 2^r-block is at least 2^k. For any other 2^r-block, this copy of H_r acts trivially, but since $g(\lambda) \not\equiv 0 \bmod 2$, negation acts non-trivially, hence increasing the $(H \times \mathbb{Z}/2)$-orbit size by a factor of 2. □

Lemma 2.8. *Assume $\lambda \in A_{p^m s-1}$.*

(i) If $s=1$ and $\Sigma^{m-1}(\lambda) \not\equiv 0$ mod p, then $|H\lambda| \ge p^{2m-1}$.
(ii) If $s>1$ not divisible by p, and $\Sigma^m(\lambda) \not\equiv 0$ mod p, then $|(H_m)^s\lambda| \ge p^{2m}$. If also $p=2$, then $|((H_m)^s \times \mathbb{Z}/2)\lambda| \ge 2^{2m+1}$.

Proof. For (i) notice that $\Sigma^{m-1}(\lambda)$ is non-scalar, and therefore $|\Sigma^{m-1}(H\lambda)| = p$.

Since the sum of the coordinates is zero, there are two p^{m-1}-blocks whose coordinates sums are not divisible by p, and hence each contain a non-scalar p-block. Now combine Lemma 2.4 and Lemma 2.5 to see

$$|H\lambda| \ge |\Sigma^{m-1}(H\lambda)| \cdot |(H_{m-1})^p\lambda| \ge p(p^{m-1})(p^{m-1}) = p^{2m-1}.$$

For (ii), similar to case (i), there must be two p^m-blocks each containing a non-scalar p-block. So by Lemma 2.5, we have $|(H_m)^s\lambda| \geq (p^m)(p^m) = p^{2m}$.

For $p = 2$, notice $(H_m)^s$ acts trivially on $\Sigma^m(\lambda)$, but negation acts non-trivially, hence increasing the orbit size by a factor of two. □

Remark 2.9. Part (i) is also proved in [MR09].

Given a set of elements S in $\mathbb{Z}^N$, and a number $x \in \mathbb{Z}$, the notation $S = x$ (resp. $S \equiv x \bmod p$) will mean that every coordinate of every element in S is equal to (resp. congruent mod p to) the number x.

Lemma 2.10. *Let $\lambda \in A^{+p^k}_{p^r s-1}$, with s not divisible by p, and $1 \leq k \leq r-1$.*

(i) Assume $s = 1$. If $\Sigma^{r-1}(\lambda) \not\equiv 0$ mod p and $\Sigma^k(\lambda) \not\equiv g(\lambda)$ mod p, then $|H\lambda| \geq p^{2r-1}$.

(ii) Assume $s > 1$. If $\Sigma^r(\lambda) \not\equiv 0$ mod p, then $|(H_r)^s\lambda| \geq p^{2r}$. If also $p = 2$, then $|((H_r)^s) \times \mathbb{Z}/2)\lambda| \geq 2^{2r+1}$.

Proof. From Lemma 2.2 we can write any p^k-block as $B = \frac{g(\lambda)}{p^k}(1, \cdots, 1) + (b_1, \cdots, b_{p^k})$, where $b_i \in \mathbb{Z}$. By our assumptions, there must be at least two p^k-blocks B_1, B_2 in λ that are not sent to $g(\lambda)$ mod p, under Σ^k. In other words, $g(\lambda) + \sum b_i \not\equiv g(\lambda) \bmod p$. In particular, the p-blocks inside B_i are not all scalar. Therefore we can apply Lemma 2.5 to see $|H_k B_i| \geq p^k$.

For (i), since $\Sigma^k(\lambda) \in A_{p^{r-k}-1}$, from Lemma 2.8(i), we see $|\Sigma^k(H\lambda)| \geq p^{2(r-k)-1}$. Now apply Lemma 2.4:

$$|H\lambda| \geq |\Sigma^k(H\lambda)| \cdot |(H_k)^{p^{r-k}}\lambda| \geq p^{2(r-k)-1}(p^k)(p^k) = p^{2r-1}.$$

For (ii), similarly by Lemma 2.8(ii), we see $|\Sigma^k((H_r)^s\lambda)| \geq p^{2(r-k)}$. Therefore, by Lemma 2.4:

$$|(H_r)^s\lambda| \geq |\Sigma^k((H_r)^s\lambda)| \cdot |(H_k)^{p^{r-k}s}\lambda| \geq p^{2(r-k)}(p^k)(p^k) = p^{2r}.$$

Finally, for $p = 2$, notice $(H_r)^s$ acts trivially on $\Sigma^r(\lambda)$, but negation acts non-trivially, hence increasing the orbit size by a factor of two. □

2.11. **Case ${}^1A^{+p^k}_{p^r-1}$, $p \neq 2$ or $p = 2$.** The arguments for $p = 2$ and $p \neq 2$ are mostly the same, so we consider them simultaneously. We use the Sylow subgroup $H = H_r$, as defined above.

Lemma 2.12. *Let $\Lambda \subset A^{+p^k}_{p^r-1}$ be H-invariant and p-generating, with $1 \leq k \leq r-1$. Then there are distinct H-orbits, $\Delta_0, \Delta_1 \subset \Lambda$ such that $\Sigma^{r-1}(\Delta_0) \not\equiv 0$ mod p and $g(\Delta_1) \not\equiv 0$ mod p, such that one of the two orbits obeys $\Sigma^{r-1}(\Delta_i) \not\equiv g(\Delta_i)$ mod p.*

Proof. Consider the map

$$\pi : (\frac{1}{p^r}\mathbb{Z})^{p^r} \to (\mathbb{Z}/p)^p \times \mathbb{Z}/p$$
$$\lambda \mapsto (\Sigma^{r-1}(\lambda), g(\lambda)) \bmod p.$$

Then $\pi(A^{+p^k}_{p^{r-1}})$ is a rank p abelian group. Therefore, if Λ is p-generating, $\pi(\Lambda)$ is also a rank p abelian group. But any H-orbit has image under π either rank $p-1$ or rank 1. H-orbits whose image have rank 1 come from elements whose image under Σ^{r-1} have equal coordinates mod p.

So we can choose two orbits in Λ such that the two together generate a rank p image under the map π. Therefore one of the two orbits obeys $\Sigma^{r-1}(\Delta_i) \not\equiv g(\Delta_i) \bmod p$.

At least one of these two orbits has non-trivial glue part, $g(\Delta_i)$; choose one and call it Δ_1, and the other one Δ_0. At least one of the two orbits must obey $\Sigma^{r-1}(\Delta_i) \not\equiv 0 \bmod p$. If Δ_0 obeys this condition, then we are done.

Otherwise, Δ_0 has image rank 1, and therefore it has non-trivial glue part. Now by swapping the names of Δ_0 and Δ_1, we have found the required pair of orbits. □

We will say that a pair of orbits Δ_0, Δ_1 from Lemma 2.12 *can be swapped* if $\Sigma^{r-1}(\Delta_1) \not\equiv 0 \bmod p$, and $g(\Delta_0) \not\equiv 0 \bmod p$. In this case we may relabel Δ_0 as Δ_1, and vice versa.

Lemma 2.13. *Given a pair of H-orbits, Δ_0 and Δ_1 from Lemma 2.12, one of the following two conditions is satisfied (possibly after swapping Δ_0 and Δ_1):*

(a) $\Sigma^k(\Delta_0) \not\equiv g(\Delta_0)$ mod p.
(b) $\Sigma^k(\Delta_0) \equiv g(\Delta_0)$ mod p, $k = r-1$, and $\Sigma^{r-1}(\Delta_1) = 0$.

Proof. Assume that such a pair doesn't obey (a), even after swapping the roles of Δ_0 and Δ_1, if possible. We must show the pair obeys (b).

So we have that $\Sigma^k(\Delta_0) \equiv g(\Delta_0) \bmod p$. Notice that if $k < r-1$, then this would imply $\Sigma^{r-1}(\Delta_0) \equiv 0 \bmod p$, a contradiction. So we have $k = r-1$, and therefore $g(\Delta_0) \not\equiv 0 \bmod p$.

Now we know by Lemma 2.12 that $\Sigma^{r-1}(\Delta_1) \not\equiv g(\Delta_1)$, and so (by assumption), Δ_0 and Δ_1 can't be swapped. Therefore $\Sigma^{r-1}(\Delta_1) \equiv 0 \bmod p$. Now this implies $\Sigma^{r-1}(\Delta_1) = 0$, and so we are done. □

Lemma 2.14. *Let $\lambda \in A^{+p^k}_{p^{r-1}}$ with $k = r-1 \neq 0$, such that $\Sigma^{r-1}(\lambda) = 0$ and $g(\lambda) \not\equiv 0$ mod p. Then $|H\lambda| \geq p^{p(r-1)}$.*

Proof. Write $\lambda = \frac{g(\lambda)}{p^{r-1}}(1, \cdots, 1) + (a_1, \cdots, a_{p^r})$, as in Lemma 2.2. Consider the p^{r-1}-blocks of λ. Since $\Sigma^{r-1}(\Delta_1) = 0$, we sum the coordinates of the first p^{r-1}-block to get $\sum a_i = -g \not\equiv 0 \bmod p$. In particular, each p^{r-1}-block contains a p-block which is not scalar. So by Lemma 2.5, the H_{r-1}-orbit of each p^{r-1}-block is at least p^{r-1}, and therefore by Lemma 2.4, we have $|H\lambda| \geq |(H_{r-1})^p\lambda| \geq (p^{r-1})^p$, as required. □

Corollary 2.15. *Let $\Lambda \subset A^{+p^k}_{p^{r-1}}$ be H-invariant and p-generating, with $1 \leq k \leq r-1$. Then $|\Lambda| \geq \min\{p^{2r-1} + p^k, p^{p(r-1)} + p^k\}$.*

Proof. By Lemma 2.12 we can find two orbits Δ_0 and Δ_1, which obey either case (a) or (b) from Lemma 2.13. In case (a), we have $|\Delta_0| \geq p^{2r-1}$ by Lemma 2.10, and $|\Delta_1| \geq p^k$ by Lemma 2.7. In case (b) we have $|\Delta_0| \geq p^k$ by Lemma 2.7, and $|\Delta_1| \geq p^{p(r-1)}$ by Lemma 2.14. □

Theorem 2.16. *Let $\Lambda \subset A^{+p^k}_{p^{r-1}}$ be H-invariant and p-generating. Then*

$$|\Lambda| \geq \begin{cases} p^r & 1 \leq k = r \\ p^{2r-2} + p^k & 1 \leq k = r-1, p = 2 \\ p^{2r-1} & k = 0 \\ p^{2r-1} + p^k & \text{otherwise} \end{cases}$$

Moreover, there exist Λ such that these bounds are achieved.

Proof. For $1 \leq k = r$, we must have an element λ such that $g(\lambda) \not\equiv 0 \bmod p$, so the lower bound follows from Lemma 2.7. Let $\Lambda = H \cdot v_{p^r}$, where v_{p^r} is defined in (2.1). This set is p-generating and H-invariant, and has size p^r; so the bound is achieved.

For $p = 2$ and $k = r-1$, notice this is the only case where the quantity $p^{p(r-1)} + p^k$ is less than the quantity $p^{2r-1} + p^k$, from Corollory 2.15. To see this bound is achieved, take $\Delta_0 = H \cdot v_{2^k}$, where v_{p^k} is defined in (2.1); then Δ_0 has size 2^{r-1}. Also let $\Delta_1 = H \cdot (\sum_{i=1}^{2^r} \frac{1}{2^{r-1}} \epsilon_i - \epsilon_1 - \epsilon_{1+2^{r-1}})$, where the two 2^k-blocks are equivalent; this orbit has size $2^{r-1}2^{r-1}$. One checks that $\Lambda = \Delta_0 \coprod \Delta_1$ generates the lattice, so the lower bound is achieved.

The $k = 0$ bound follows from Lemma 2.8. The bound is achieved by choosing $\Lambda = H \cdot \lambda$ for

$$\lambda := (\underbrace{1, 0, \cdots, 0}_{p^{r-1}\text{-block}}, \underbrace{-1, 0, \cdots, 0}_{p^{r-1}\text{-block}}, 0, \cdots, 0) = \epsilon_1 - \epsilon_{1+p^{r-1}}\,. \tag{2.17}$$

This is the same choice as in [MR09, 6 and 7].

For all other cases, by Corollory 2.15 we have $|\Lambda| \geq p^{2r-1} + p^k$. To see this bound is achieved, take λ as in (2.17). Then $\Delta_0 = H \cdot \lambda$ has size p^{2r-1}, as in the $k = 0$ case. Now take $\Delta_1 = H \cdot v_{p^k}$, which has size p^k. One checks that $\Lambda = \Delta_0 \coprod \Delta_1$ generates the lattice. □

Now we show when the choices from the proof of Theorem 2.16 satisfy (K_H). Firstly, the choice for $1 \leq k = r$ does not satisfy (K_H), since the only linear relation among the elements of Λ is that they all sum to zero.

For the $p = 2, 1 \leq k = r-1$ case, let $\sigma := \frac{1}{2^{r-1}} \sum_{i=1}^{2^r} \epsilon_i$, and assume $r \geq 3$. Then we have the following equations among elements of Λ:

$$(\sigma - \epsilon_1 - \epsilon_{1+2^{r-1}}) + (\sigma - \epsilon_i - \epsilon_{i+2^{r-1}}) - (\sigma - \epsilon_i - \epsilon_{1+2^{r-1}}) - (\sigma - \epsilon_1 - \epsilon_{i+2^{r-1}}) = 0$$
$$(\sigma - \epsilon_1 - \epsilon_2) + (\sigma - \epsilon_{j+2^{r-1}} - \epsilon_{j+1+2^{r-1}}) - (\sigma - \epsilon_1 - \epsilon_{j+2^{r-1}}) - (\sigma - \epsilon_2 - \epsilon_{j+1+2^{r-1}}) = 0.$$

These equations are valid for $i = 2, 3$ and $j = 1, 3$ (here we have used that $r \geq 3$). They show that $(\sigma - \epsilon_1 - \epsilon_{1+2^{r-1}})$ is Λ-independent, and that $(\sigma - \epsilon_1 - \epsilon_2)$ is Λ-independent. So by Lemma 1.12 we see that (K_H) is satisfied. For $r = 2$, one checks that (K_H) is not satisfied.

For $k = 0$, let $\gamma \in H$ be the order p permutation given by sending $\epsilon_i \mapsto \epsilon_{i+p^{r-1}}$, where $\epsilon_{i+p^r} = \epsilon_i$. Assume $r \geq 2$, and consider the following relations among elements

of Λ:

$$(\epsilon_1 - \epsilon_j) + (\epsilon_2 - \epsilon_{j+1}) - (\epsilon_2 - \epsilon_j) - (\epsilon_1 - \epsilon_{j+1}) = 0 \tag{2.18}$$

$$(\epsilon_1 - \epsilon_j) + \gamma(\epsilon_1 - \epsilon_j) + \cdots + \gamma^{p-1}(\epsilon_1 - \epsilon_j) = 0. \tag{2.19}$$

Here $j = 1 + p^{r-1}$. This shows $(\epsilon_1 - \epsilon_j)$ is Λ-independent, and hence by Lemma 1.12 it satisfies (K_H). For $r = 1$, (K_H) is not satisfied.

In all other cases, we can argue as follows. Let $\sigma = \frac{1}{p^k}\sum_{i=1}^{p^r} \epsilon_i$, and let γ be as in the $k = 0$ case. Then consider the following equations:

$$(\sigma - \sum_{i=1}^{p^{r-k}} \epsilon_i) - (\sigma - \sum_{i=1}^{p^{r-k}} \gamma^j \epsilon_i) + \sum_{i=1}^{p^{r-k}} (\epsilon_i - \gamma^j \epsilon_i) = 0 \tag{2.20}$$

$$(\sigma - \sum_{i=1}^{p^{r-k}} \epsilon_i) - (\sigma - \sum_{i=1}^{p^{r-k}} \epsilon_{i+p^{r-k}}) + \sum_{i=1}^{p^{r-k}} (\epsilon_i - \gamma\, \epsilon_1) - \sum_{i=1}^{p^{r-k}} (\epsilon_{i+p^{r-k}} - \gamma\, \epsilon_1) = 0. \tag{2.21}$$

If $p \geq 3$ then we can use $j = 1, 2$ in the first equation. The second equation is only valid if $k \geq 2$, in which case it is different from the first. So for $p \geq 3$ or $k \geq 2$ we have show that $(\sigma - \sum_{i=1}^{p^{r-k}} \epsilon_i)$ is Λ-independent. In the only remaining case, $p = 2$ and $k = 1$ we also have the following equation, which shows Λ-independence:

$$(\sigma - \sum_{i=1}^{2^{r-1}} \epsilon_i) + (\sigma - \sum_{i=1}^{2^{r-1}} \epsilon_{i+2^{r-1}}) = 0. \tag{2.22}$$

We already know $(\epsilon_1 - \epsilon_{1+p^{r-1}})$ is Λ-independent from the $k = 0$ case (notice that $r = 1$ doesn't occur in the present case). So our choice of Λ satisfies (K_H), by Lemma 1.12.

2.23. **Case ${}^2A^{+2^k}_{2^r-1}$, $p = 2$.** As above we will use the notation $H := H_r = W(A_{2^r-1})^{(2)}$, and let $\Gamma = H \times \mathbb{Z}/2$, where the generator for $\mathbb{Z}/2$ is the outer automorphism on the lattice given by negation.

For $k = 0$ or 1, one checks that (for each value of r) the Λ from Theorem 2.16 is invariant under negation, so the value $\mathrm{SymRank}(\phi; 2)$ is unchanged from the ${}^1A^{+2^k}_{2^r-1}$ case. Furthermore, the condition (K_Γ) is equivalent the condition (K_H), by Lemma 1.12.

For $k \geq 2$, by Lemma 2.7 any λ in the lattice with $g(\lambda)$ odd has Γ-orbit size at least 2^{k+1}. Now we can modify the proof of Theorem 2.16 to obtain the desired lower bounds. Furthermore, these bounds are achieved by taking the Γ-orbits of the same elements as in Theorem 2.16 (instead of just the H-orbits). Also (K_H) implies (K_Γ) by Lemma 1.12. Now Λ contains negatives of elements, so we get relations of the form $\lambda + (-\lambda) = 0$, which ensures that in the case $k = r$ condition (K_Γ) is satisfied.

2.24. **Case ${}^1A^{+p^k}_{p^r s-1}$, with $s > 1$ not divisible by p.** We will use $H := W(A_{p^r s-1})^{(p)}$ as described near the start of this section. We will also denote $\sigma := \frac{1}{p^k}\sum_{i=1}^{p^r s} \epsilon_i$.

Lemma 2.25. *Let $\Lambda \subset A_{p^r s-1}^{+p^k}$ be p-generating, with $1 \leq k \leq r$, and $s > 1$ not divisible by p. Then either $\Sigma^r(\Lambda)$ contains at least s elements whose reduction mod p is not the scalar zero, or $\Sigma^r(\Lambda)$ contains $s-1$ such elements, as well as one whose glue part is not zero mod p.*

Proof. Consider the the map

$$\pi : (\frac{1}{p^r}\mathbb{Z})^{p^r s} \to (\mathbb{Z}/p)^s \times \mathbb{Z}/p$$
$$\lambda \to (\Sigma^r(\lambda), g(\lambda)) \bmod p.$$

The image $\pi(A_{p^r s-1}^{+p^k})$ is a rank s abelian group, so for Λ to be p-generating, $\pi(\Lambda)$ must generate a rank s group, and in particular the image contains s generators. At most one of these generators is zero mod p on the $(\mathbb{Z}/p)^s$ component. This proves the lemma. □

Theorem 2.26. *Let $\Lambda \in A_{p^r s-1}^{+p^k}$ be H-invariant and p-generating, where $s > 1$ is not divisible by p. Then*

$$|\Lambda| \geq \begin{cases} p^r s & 1 \leq k = r \\ p^{2r}(s-1) + p^k & 1 \leq k \leq r-1 \\ p^{2r}(s-1) & k = 0 \end{cases}$$

Moreover, in each case there exists a Λ such that these bounds are achieved.

Proof. For $k = r$, assume Λ is p-generating. We can apply Lemma 2.25 and get s elements of Λ which obey either $\Sigma^r(\lambda) \not\equiv 0 \bmod 2$ or $g(\lambda) \not\equiv 0 \bmod 2$. If the latter, then by Lemma 2.7 we have $|(H_r)^s\lambda| \geq p^r$. If $g(\lambda) = 0 \bmod 2$, then $\lambda \in A_{2^r s-1}^{+2^{k-1}}$, and we can apply Lemma 2.10 we see $|(H_r)^s\lambda| \geq p^{2r} > p^r$. Since $(H_r)^s$ acts trivially on $\Sigma^r(\Lambda)$, we get that $|\Lambda| \geq p^r s$. To see this value is achieved, choose $\Lambda = \{\sigma - s\,\epsilon_i\}_{i=1}^{p^r s}$.

For $1 \leq k \leq r-1$, we combine Lemma 2.25 and Lemma 2.7 and Lemma 2.10 to get $|\Lambda| \geq \min\{p^{2r}s, p^{2r}(s-1) + p^k\} = p^{2r}(s-1) + p^k$.

To show this is achieved, consider the set:

$$\Lambda_0 = \bigcup_{1 \leq i \leq p^r < j \leq p^r s} \{\epsilon_i - \epsilon_j\}. \tag{2.27}$$

This set is H-invariant, and has $p^{2r}(s-1)$ elements. All that remains is to find an element with $g(\lambda_1) \not\equiv 0 \bmod p$ whose orbit is p^k. Since we have assumed the first p^r-block is a big block, then $\lambda_1 = \sigma - s\sum_{i=1}^{p^{r-k}} \epsilon_i$ is such an element. So $\Lambda = \Lambda_0 \cup H\lambda_1$ will do.

For $k = 0$, as in Lemma 2.25, we can find $s-1$ distinct non-zero elements in $\Sigma^r(\Lambda)$, and by Lemma 2.10 each has $(H_r)^s$-orbit size at least p^{2r}. Since $(H_r)^s$ acts trivially on $\Sigma^r(\Lambda)$, we have shown the lower bound. To see is achieved, use $\Lambda = \Lambda_0$ from (2.27) above. □

Remark 2.28. The $k = 0$ case was also covered in [MR09, 8].

Now we will determine when these choices satisfy (K_H). For $1 \leq k = r$, the condition is not satisfied.

For $k = 0$, similar to the $k = 0$ case when $s = 1$, we define $\gamma \in H$ by sending $\epsilon_i \mapsto \epsilon_{i+p^{r-1}}$, unless i is divisible by p^r, in which case $\epsilon_i \mapsto \epsilon_{i+p^{r-1}-p^r}$. This γ has order p. Now for $r \geq 1$, the equation (2.18) is valid if we instead use $j = 1 + ip^r$, for any $1 \leq i \leq s-1$. If $s \geq 3$ then we get at least two equations, which show that $(\epsilon_1 - \epsilon_j)$ is Λ-independent for each of these j; furthermore Λ is the union of the H-orbits of these elements. If $s = 2$, then $p \geq 3$, so we can modify equation (2.18) to get our second equation. In either case, by Lemma 1.12, we have shown (K_H) is satisfied. Notice that for $r = 0$ we have $\mathrm{SymRank}(\phi; p) = s - 1 = \mathrm{rank}(\phi)$.

Finally, for $1 \leq k \leq r-1$, by using the argument from the $k = 0$ case we see that every element of Λ_0 is Λ-independent. Similar to the $s = 1$ case, if we insert a factor of s to all of the summation signs in equations (2.20),(2.21),(2.22), then an identical argument goes through. So (K_H) is satisfied.

2.29. **Case ${}^2A^{+2^k}_{2^r s-1}$, with $s > 1$ odd, and $p = 2$.** Let $\Gamma = (H \times \mathbb{Z}/2)$. The lower bounds for the size of Γ-invariant 2-generating subsets of the lattice are the same as Theorem 2.26, except that negation adds another factor of two by Lemma 2.7 and Lemma 2.10.

To see they are achieved, simply take the Λ used in Theorem 2.26 together with their negatives. Notice that (K_H) implies (K_Γ). Furthermore, when $1 \leq k = r$, by considering the equations $(\lambda) + (-\lambda) = 0$, we see that every element of Λ is Λ-independent, and hence that (K_Γ) is satisfied by Lemma 1.12. For $0 = k = r$, we have that Λ consists of $s - 1$ linearly independent elements together with their negatives, and hence (K_Γ) is not satisfied.

3. Type D_n

Let us describe the lattices of type D_n, following the notation of [CS93]. Denote by I_n the $\mathbb{Z}$-module with (orthonormal) basis $\epsilon_1, \cdots, \epsilon_n$. It has an index 2 submodule, $D_n = \{\sum \mathrm{c}_i \epsilon_i \,|\, \sum \mathrm{c}_i \text{ is even. }\}$. We construct the module D_n^{+4} by taking the span of I_n together with $\frac{1}{2}\sum \epsilon_i$. Finally, for n even, $D_n^{+2} \subset D_n^{+4}$ is the index 2 submodule of elements whose coefficients sum to an even integer.

The action of the Weyl group $W(D_n) = (\mathbb{Z}/2)^{n-1} \rtimes S_n$ on D_n is given by S_n permuting the vectors ϵ_i, and $(\mathbb{Z}/2)^{n-1}$ making an even number of sign changes on $\{\epsilon_i\}$. We have an outer automorphism given by negating only ϵ_1. When $n = 4$ there is also an outer automorphism of order 3, which is a phenomenon known as triality. The following table summarizes the possible situations. The column ϕ uses notation as from 1.2, and G is a corresponding split group. For the rest of this section, $n = 2^r s$ where s is odd.

Unless the lattice is D_4, the primes $p \neq 2$ do not appear in the table. This is because in these cases the size n set $\Lambda = \{\epsilon_i\}$ is Sylow invariant, and generates a sublattice of index a power of 2, so $\mathrm{SymRank}(\phi; p)$ is the rank of the lattice.

We have $n = 2^r s$ where s is odd, and we use the notation $(H_r)^s \subset H \subset S_{2^r s}$ as defined near the start of Section 2. Then for $p = 2$, our Sylow subgroup Γ is either $(\mathbb{Z}/2)^{n-1} \rtimes H$ or $(\mathbb{Z}/2)^n \rtimes H$.

ϕ	G	p	Conditions	SymRank$(\phi;p)$	(K)
${}^1D_n$	PSO_{2n}	2	$n=2^r s,\ s>1$	$2^{2r+2}(s-1)$	y
			$n=2^r\geq 4$	2^{2r}	y
${}^2D_n$	PSp_{2n}	2	$n=2^r s,\ s>1$	$2^{2r+2}(s-1)$	y
			$n=2^r\geq 4$	2^{2r}	y
${}^1D_n^{+2}$	$HSpin_{2n}$	2	$n\geq 6$	2^{n-1}	y
${}^1I_n$	SO_{2n}	2	$n\geq 4$	$2n$	n
${}^2I_n$	Sp_{2n}, SO_{2n+1}	2	$n\geq 2$	$2n$	n
${}^1D_n^{+4}$	$Spin_{2n}$	2	$n\geq 5$ odd	2^{n-1}	y
			$n\geq 4$ even	$2^{n-1}+2^{r+1}$	y
${}^2D_n^{+4}$	$Spin_{2n+1}$	2	$n\geq 2$	2^n	y
${}^3D_4$	F_4	3		9	y

TABLE II. D_n lattices (which includes groups of types B_n and C_n)

3.1. **Case ${}^1D_{2^r s}$ or ${}^2D_{2^r s}$, with $s>1$ odd.** We consider both the cases simultaneously. Consider the map $\pi : D_{2^r s}\to(\mathbb{Z}/2)^s$ given by $\pi(\lambda)=\Sigma^r(\lambda) \bmod 2$. For $\Lambda\subset D_{2^r s}$ to be 2-generating, we need $\pi(\Lambda)$ to be of rank $s-1$. Let $\lambda\in\Lambda$ be such that $\pi(\lambda)$ is one of the $s-1$ generators. Since $\pi(\lambda)$ is non-trivial, $\Sigma^r(\lambda)$ must contain at least two non-trivial coordinates, and hence λ contains at least two 2^r-blocks both of which contain a non-scalar 2-block. Now by Lemma 2.5, the H_r-orbits of each of these 2^r-blocks is at least 2^r. Also, $\Sigma^r((\mathbb{Z}/2)^{n-1}\lambda)$ is at least size 4, since we can change the signs of either of these blocks (even in the case $r=0$). Finally, $(\mathbb{Z}/2)^n\rtimes(H_r)^s$ acts trivially on $\pi(D_{2^r s})$, and so we have $|\Lambda|\geq 4(2^r)(2^r)(s-1)=2^{r+2}(s-1)$.

To see this bound is achieved, notice the following set is $((\mathbb{Z}/2)^n\rtimes H)$-invariant and generating:

$$\Lambda=\bigcup_{1\leq i\leq 2^r<j\leq n}\{\pm\epsilon_i\pm\epsilon_j\}.$$

To see this satisfies condition (K_Γ), we use Lemma 1.12. Let us consider $\epsilon_1+\epsilon_{2^r+1}\in\Lambda$. Then we have

$$(\epsilon_1+\epsilon_{2^r+1})+(-\epsilon_1+\epsilon_{2^r+1})+(\epsilon_1-\epsilon_{2^r+2})+(-\epsilon_1-\epsilon_{2^r+2})=0$$
$$(\epsilon_1+\epsilon_{2^r+1})+(-\epsilon_1-\epsilon_{2^r+1})=0$$

So $\epsilon_1+\epsilon_{2^r+1}$ is Λ-independent. A similar argument can be used on the other elements of Λ.

3.2. **Case ${}^1D_{2^r}$ or ${}^2D_{2^r}$, with $r\geq 2$.** We consider both the cases simultaneously. Consider the map $\pi : D_{2^r}\to(\mathbb{Z}/2)^2$ given by $\pi(\lambda)=\Sigma^{r-1}(\lambda) \bmod 2$. For $\Lambda\subset D_{2^r}$ to be 2-generating, we need $\pi(\Lambda)$ to contain a non-trivial element. Let $\lambda\in\Lambda$ be such that $\pi(\lambda)$ is non-trivial. Therefore both 2^{r-1}-blocks in λ contain a non-scalar 2-block. Now by Lemma 2.5, the H_{r-1}-orbits of each of these 2^{r-1}-blocks is at least 2^{r-1}. Also, $\Sigma^{r-1}((\mathbb{Z}/2)^{2^{r-1}}\lambda)$ is at least size 4, since we can change the signs of either of these blocks (even in the case $r=0$). Finally, $(\mathbb{Z}/2)^{2^{r-1}}\rtimes H_{r-1}$ acts trivially on $\pi(D_{2^r})$, and so we have $|\Lambda|\geq 4(2^{r-1})(2^{r-1})=2^{2r}$.

This lower bound is achieved by choosing:

$$\Lambda = \bigcup_{1\leq i\leq 2^{r-1}<j\leq 2^r} \{\pm\epsilon_i \pm \epsilon_j\}.$$

This Λ satisfies (K_Γ), which can be seen by using a similar argument to the $s > 1$ case to show $\epsilon_1 + \epsilon_{2^{r-1}+1}$ is Λ-independent.

3.3. **Case ${}^1D_n^{+2}$, and $n \geq 6$ even.** For $\Lambda \subset D_n^{+2}$ to be 2-generating, there must be a $\lambda \in \Lambda$, all of whose coefficients of ϵ_i are half-integers. In other words, $c_i \in \frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$; and in particular are non-zero. By considering how the coefficients change sign, the Γ-orbit of such an element is at least of size 2^{n-1}.

To ease notation, define $\sigma := \frac{1}{2}\sum_{i=1}^n \epsilon_i$. For $n \equiv 0 \bmod 4$, this bound is achieved by choosing $\Lambda = \Gamma\cdot\sigma$; for $n \equiv 2 \bmod 4$, this bound is achieved by choosing $\Lambda = \Gamma\cdot(\sigma - \epsilon_1)$.

These both satisfy (K_Γ); we will only consider the $n \equiv 0 \bmod 4$ case, because the other case is similar. We have the following two equations.

$$\sigma + (\sigma - \epsilon_1 - \epsilon_2 - \epsilon_3 - \epsilon_4) - (\sigma - \epsilon_1 - \epsilon_2) - (\sigma - \epsilon_3 - \epsilon_4) = 0$$
$$\sigma + (-\sigma) = 0.$$

Therefore, for $n \geq 5$, we have that σ is Λ-independent, and thus Λ satisfies (K_Γ), by Lemma 1.12.

3.4. **Case ${}^1I_n$, and $n \geq 4$.** Λ must contain n linearly independent elements of I_n, and for even n, Γ sends these to their negatives, so $|\Lambda| \geq 2n$. For odd n, if every element of Λ has at least one coordinate zero, then they are also all sent to their negatives. Otherwise, there is an element of Λ whose coordinates are all non-zero. The Γ-orbit of such an element is at least 2^{n-1}. For $n \geq 4$, we have $|\Lambda| \geq 2^{n-1} \geq 2n$. This lower bound is achieved by choosing $\Lambda = \{\pm\epsilon_i\}$. The condition (K_Γ) is not satisfied; the sign changes act trivially on the kernel of $\mathbb{Z}[\Lambda] \to \hat{T}$.

3.5. **Case ${}^2I_n$, and $n \geq 2$.** Λ must have n linearly independent elements of I_n, together with their negatives, and therefore $|\Lambda| \geq 2n$. This lower bound is achieved by choosing $\Lambda = \{\pm\epsilon_i\}$. As in the case ${}^1I_n$, the condition (K_Γ) is not satisfied;

3.6. **Case ${}^1D_n^{+4}$, and $n \geq 5$ odd.** To be 2-generating, Λ must contain an element all of whose coefficients are half-integers, and in particular are non-zero. The Γ-orbit of such an element is at least of size 2^{n-1}.

Let $\sigma := \frac{1}{2}\sum_{i=1}^n \epsilon_i$. Since n is odd, this bound is achieved by $\Lambda = \Gamma\cdot\sigma = \{\frac{1}{2}(\pm\epsilon_1 \cdots \pm \epsilon_n)\}$, where each element has an even number of minus signs. Notice that the generated lattice, X_Λ, contains ϵ_1, something which is not true for n even. To see that (K_Γ) is satisfied, we can use the first equation in the ${}^1D_n^{+2}$ case, but not the second, since the negatives are not in Λ. Since $n \geq 5$, we can also use the following equation:

$$\sigma + (\sigma - \epsilon_1 - \epsilon_2 - \epsilon_3 - \epsilon_5) - (\sigma - \epsilon_2 - \epsilon_5) - (\sigma - \epsilon_1 - \epsilon_3) = 0.$$

Then we see σ is Λ-independent, and by Lemma 1.12 we are done.

3.7. **Case ${}^1D_n^{+4}$, and $n \geq 4$ even.** Consider the map $\pi : D_n^{+4} \to \mathbb{Z}/2 \times \mathbb{Z}/2$ given by sending λ to its coordinate sum mod 2, and its projection $D_n^{+4}/I_n \cong \mathbb{Z}/2$. Then π is surjective, and Γ acts trivially on the image, so for any 2-generating subset Λ we have that $\pi(\Lambda)$ generates $(\mathbb{Z}/2)^2$.

Notice that for any λ whose projection to D_n^{+4}/I_n is non-trivial, in other words its coordinates consist of half-integers, then all of its coefficients are non-zero. In particular, $|\Gamma\lambda| \geq 2^{n-1}$.

Now assume λ is such that its coordinates sum to an odd number. If its coordinates are half-integers, then we know $|\Gamma\lambda| \geq 2^{n-1} \geq 2^{r+1}$, so assume they are integers. We know one of its 2^r-blocks sum to an odd number (where $n = 2^r s$, for s odd), and hence this 2^r-block contains a non-scalar 2-block. By Lemma 2.5, we know $|H\lambda| \geq 2^r$. Finally, notice that the number of positive odd coefficients does not equal the number of negative odd coefficients (since there are an odd number of them), so $-\lambda \notin H\lambda$, and therefore $|\Gamma\lambda| \geq 2^{r+1}$.

This shows that $|\Lambda| \geq 2^{n-1} + 2^{r+1}$.

Finally, this bound is achieved by $\Lambda = (\Gamma \cdot \sigma) \cup \{\pm\epsilon_i \,|1 \leq i \leq 2^r\}$. To see this satisfies (K_Γ), consider the equations

$$(\epsilon_1) + (\epsilon_2) + \cdots + (\epsilon_n) + 2(\sigma) = 0$$
$$(\epsilon_1) + (-\epsilon_1) = 0, \qquad \sigma + (-\sigma) = 0.$$

This shows σ and ϵ_i are Λ-independent. By Lemma 1.12 we are done.

3.8. **Case ${}^2D_n^{+4}$, and $n \geq 2$.** For $\Lambda \subset D_n^{+4}$ to be 2-generating, it must contain an element all of whose coefficients of ϵ_i are half-integers, and hence non-zero. The $(\mathbb{Z}/2)^n$-orbit of such an element is of size at least 2^n, and therefore $|\Lambda| \geq 2^n$.

This lower bound is achieved by $\Lambda = \Gamma \cdot \sigma = \{\frac{1}{2}(\pm\epsilon_1 \cdots \pm\epsilon_n)\}$. Let us check that it satisfies (K_Γ). Let $\sigma = \frac{1}{2}\sum_{i=1}^n \epsilon_i$; then we have the two equations

$$\sigma + (\sigma - \epsilon_1 - \epsilon_2) + (-\sigma + \epsilon_1) + (-\sigma + \epsilon_2) = 0$$
$$\sigma + (-\sigma) = 0.$$

Therefore σ is Λ-independent, and thus Λ satisfies (K_Γ), by Lemma 1.12.

3.9. **Case ${}^3D_4$, and $p = 3$.** Since $|W(D_4)^{(3)}| \cdot 3 = |W(F_4)^{(3)}|$, and the root system of D_4 is contained in that of F_4, we may work with the root lattice of F_4, together with its Weyl group action. Let $\tilde{\alpha} = 2\alpha_1 + 4\alpha_2 + 3\alpha_3 + 2\alpha_2$ be the highest root in F_4. Then we have a subroot system $A_2 \times A_2 \subset F_4$ generated by $\{\alpha_1, \alpha_2\}$ and $\{\alpha_4, -\tilde{\alpha}\}$. These copies of A_2 each have a copy of $\mathbb{Z}/3$ is their Weyl groups, so we will use this choice for our Sylow 3-subgroup $\Gamma := (\mathbb{Z}/3)^2 \subset W(F_4)$.

Notice that any 3-generating subset must contain an element λ whose coefficient of α_3 (written in root coordinates) is not a multiple of 3; in particular such an element is in neither copy of A_2, and hence $|\Gamma \cdot \lambda| = 9$.

Indeed, take $\Lambda = \Gamma \cdot \alpha_3$. We can choose generators $\{a, b\}$ for each copy of $\mathbb{Z}/3$ such that $a\alpha_3 = \alpha_3 + 2\alpha_2$ and $b\alpha_3 = \alpha_3 + \alpha_4$. Then notice the equations

$$\alpha_3 + a^i b^i \alpha_3 - a^i \alpha_3 - b^i \alpha_3 = 0, \quad \text{for } i = 1, 2.$$

This shows that α_3 is Λ-independent, and hence by Lemma 1.12 we see Λ satisfies (K_Γ).

4. Exceptional Type

We will use E_n to denote both the root lattice of E_n as well as the split adjoint group of type E_n. We consider the exceptional groups at every prime which divides the order of the Weyl group, but we only include in the table the cases where $\mathrm{SymRank}(\phi;p) > \dim(\phi)$.

ϕ	G	p	$\mathrm{SymRank}(\phi;p)$	(K)
${}^2A_2$	G_2	2	4	n
${}^1A_2$	G_2	3	3	n
${}^2D_4$	F_4	2	16	y
${}^3D_4$	F_4	3	9	y
${}^1E_6$	E_6	2	16	y
${}^2E_6$	${}^2E_6$	2	32	y
${}^1E_7$	E_7	2	64	y
${}^1E_7^{+2}$	$2E_7$	2	40	y
${}^1E_8$	E_8	2	128	y
${}^1E_6$	E_6	3	27	y
${}^1E_6^{+3}$	$3E_6$	3	27	y
${}^1E_7$	E_7	3	27	y
${}^1E_8$	E_8	3	81	y
${}^1E_8$	E_8	5	25	y

Table III. Exceptional lattices

We can find the G_2 and F_4 cases in the A_n and D_n tables.

For the $p = 2$ cases, we will use the description of the E_6, E_7 and E_8 root lattices given in [Bou68, p.213-220] or [Hu92], and often write them in these coordinates.

4.1. **Case ${}^1E_8$ and $p = 2$.** We have $E_8 = D_8^{+2}$, and $W(D_8) \subset W(E_8)$. Let H' be the usual Sylow 2-subgroup of $W(D_8)$, and choose a Sylow 2-subgroup $H' \subset H'' \subset W(E_8)$, so that $|H''| = 2^{14}$. Notice that the 248 roots of E_8 decompose into H'-orbits of size 128, 64, 32, and 16. Since the H''-orbits must have sizes which are powers of 2, these are also H''-orbits.

Explicitly, using the usual coordinates for D_8^{+2}, we can choose $\Lambda = \{\frac{1}{2}(\pm 1, \cdots, \pm 1)\}$ with an even number of minus signs. Here $\Gamma = H''$, so Λ is a Γ-invariant subset which generates the lattice. Therefore $128 \geq \mathrm{SymRank}(E_8;2) \geq \mathrm{SymRank}(D_8^{+2};2) = 128$. This Λ satisfies (K_Γ) for the same reason as the ${}^1D_8^{+2}$ case, above.

4.2. **Case ${}^1E_7$ and $p = 2$.** Defining $H'' \subset W(E_8)$ as above, consider the H''-orbit of $\alpha = (0,0,0,0,0,0,1,1)$ of size 16. By defining the E_7 lattice as elements of E_8 which are orthogonal to α, we have $W(E_7) = W(E_8)_\alpha$, the elements fixing α ([Hu92,

Thm. 1.12(d)]). Furthermore, we can choose $\Gamma = H''_\alpha$ as a Sylow 2-subgroup of $W(E_7)$, because it has order $2^{14}/16 = |W(E_7)^{(2)}|$.

Consider the $H'_\alpha \subset \Gamma$ action on the 126 roots of E_7. They decompose into H'_α-orbits of size 64, 32, 16, 8, 4 and 2. Since the 126 roots are preserved by the Γ, these must also be Γ-orbits. In particular, the 64 element set $\Lambda = \Gamma \cdot \frac{1}{2}(1,-1,1,1,1,1,1,-1)$ generates the E_7 lattice, so $\mathrm{SymRank}(E_7;2) \geq 64$. Indeed this is minimal, because any 2-generating subset must contain an element whose coefficients are all in $\frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$, and $(\mathbb{Z}/2)^6 \subset \Gamma$ has trivial stabilizer of such an element.

This Λ satisfies (K_Γ) by using a similar argument to the ${}^1D_8^{+2}$ case, above.

4.3. **Case ${}^1E_7^{+2}$ at $p = 2$.** E_7^{+2} is the span of the root lattice E_7 together with $\frac{1}{2}(1,1,1,1,1,1,0,0)$, and the Γ action is the same as the E_7 case. The 56 elements in E_7^{+2} of length 3/2 decompose into H'_α-orbits of size 36, 16, and 8. Therefore these are also $\Gamma = H''_\alpha$-orbits. We take the union of two of these orbits, $\Lambda = \Gamma\cdot\frac{1}{2}(1,1,1,1,1,1,0,0) \cup \Gamma\cdot\frac{1}{2}(0,0,0,0,0,2,1,-1)$ which is of size $40 = 32+8$. One checks that this generates the lattice. To see it is minimal, notice Λ must contain an element whose first 6 coordinates are half-integers (which has Γ-orbit at least size 32) and an element whose last two coordinates are half integers (which has Γ-orbit at least size 8). Alternatively, notice that as lattices $E_7^{+2} = A_7^{+4}$, and we can embed $W(A_7) \rtimes \mathbb{Z}/2 \subset W(E_7)$. This implies $40 = \mathrm{SymRank}({}^2A_7^{+4};2) \leq \mathrm{SymRank}({}^1E_7^{+2};2) \leq 40$.

To see our choice of Λ satisfies (K_Γ), notice that $\frac{1}{2}(1,1,1,1,1,1,0,0)$ is Λ-independent by a similar argument to the ${}^1D_n^{+2}$ case. We have the following relations of elements in Λ:

$$\begin{aligned}
&\frac{1}{2}(0,0,0,0,0,2,1,-1) + \frac{1}{2}(0,0,0,0,0,-2,1,-1) \\
&+ \frac{1}{2}(0,0,0,0,2,0,-1,1) + \frac{1}{2}(0,0,0,0,-2,0,-1,1) = 0 \\
&\frac{1}{2}(0,0,0,0,0,2,1,-1) + \frac{1}{2}(0,0,0,0,0,-2,-1,1) = 0.
\end{aligned}$$

Therefore $\frac{1}{2}(0,0,0,0,0,2,1,-1)$ is Λ independent, and by Lemma 1.12, we are done.

4.4. **Case ${}^1E_6$ at $p = 2$.** Using the labellings as in [Bou68, p.218], the E_6 simple roots $\alpha_2, \cdots, \alpha_6$ form a root system of type D_5, so $W(D_5) \subset W(E_6)$. In fact, $|W(E_6)^{(2)}| = |W(D_5)^{(2)}| = 2^7$, so we get a description of the Sylow action of E_6. In coordinates, we have $\alpha_1 = \frac{1}{2}(1,-1,-1,-1,-1,-1,-1,1)$, and Γ only changes the first 5 coordinates, so the Γ-orbit of α_1 is of size 16. Furthermore, this orbit generates the E_6 lattice. It is minimal, because any 2-generating subset of E_6 must contain an element whose coefficients are all in $\frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$, and such an element has orbit size at least 16.

$\Lambda = \Gamma \cdot \alpha_1$ is the set $\{\frac{1}{2}(\pm1,\pm1,\pm1,\pm1,\pm1,-1,-1,1)\}$, where each element has an even number of minus signs. Therefore (K_Γ) is satisfied, by using a similar argument to the ${}^1D_5^{+4}$ case.

4.5. **Case ${}^2E_6$, and $p = 2$.** The Γ-action here is that same as the ${}^1E_6$ case, together with the outer automorphism given by negation. As in that case, there must be an element in Λ with half-integer coordinates, and the orbit of such an element is at least

size 32. This is achieved by considering the Γ-orbit of α_1, which is size 32, and this orbit spans E_6.

One sees $\Lambda = \Gamma \cdot \alpha_1$ satisfies (K_Γ) by a similar argument to the ${}^2D_5^{+4}$ case.

4.6. **Cases ${}^1E_6$,${}^1E_7$, and ${}^1E_8$, at $p = 3$.** We recall the description of the Sylow 3-subgroups $W(E_6)^{(3)} = W(E_7)^{(3)}$ and $W(E_8)^{(3)}$ from [Ch06, 4]. We have a sub-root system $A_2 \times (A_2)^3 \subset A_2 \times E_6 \subset E_8$, and there are 5 order three generators $\{a, b, c, d, e\} \subset W(E_8)^{(3)}$. We will now describe the action of these generators on the roots $\alpha_1, \cdots, \alpha_8$.

The extended Dynkin diagram of E_6, with highest root α_{E_6}, has a symmetry of order 3; d acts on these roots via this rotation, by sending α_6 to $-\alpha_{E_6}$ to α_1 to α_6, etc. a, b, c each cyclically permute the roots in their own copy of A_2; so a cyclically permutes $\{\alpha_3, \alpha_1, -\alpha_1 - \alpha_3\}$; and then $b = dad^{-1}$, $c = dbd^{-1}$.

Now a, b, c, d act trivially on α_8, and e acts trivially on $\alpha_1, \cdots, \alpha_6$. e cyclically permutes $\{\alpha_8, -\alpha_0, \alpha_0 - \alpha_8\}$, where α_0 is the highest root of E_8. So all that remains is to describe the action of a, b, c, d, e on α_7. One checks that: $a\alpha_7 = \alpha_7$, $b\alpha_7 = \alpha_7 + \alpha_6 + \alpha_5$, $c\alpha_7 = \alpha_7 + \alpha_{E_6} - \alpha_2$, $d\alpha_7 = \alpha_{E_7} - \alpha_1$, $e\alpha_7 = \alpha_7 + \alpha_8$. Here α_{E_7} is the highest root of E_7 with respect to the simple roots $\alpha_1, \cdots, \alpha_7$.

With this complete description, one may check the following

Lemma 4.7. *Let $\lambda = \sum_i \lambda_i \alpha_i \in \mathbb{R}^8$ be a vector in the vector space spanned by the roots of E_8, so $\lambda_i \in \mathbb{R}$. Then*

(i) $a\lambda = \lambda$ *iff* $\lambda_4 = 3\lambda_1$ *and* $\lambda_3 = 2\lambda_1$.
(ii) $b\lambda = \lambda$ *iff* $3\lambda_5 = 2\lambda_4 + 3\lambda_7$ *and* $3\lambda_6 = \lambda_4 + 2\lambda_7$.
(iii) $c\lambda = \lambda$ *iff* $\lambda_7 = \lambda_2$ *and* $\lambda_4 = 2\lambda_2$.
(iv) $d\lambda = \lambda$ *iff* $\lambda_1 = \lambda_6 = 0$ *and* $\lambda_2 = \lambda_3 = \lambda_5$.
(v) $e\lambda = \lambda$ *iff* $\lambda_7 = \lambda_8 = 0$.

Corollary 4.8. *Let $\lambda = \sum_i \lambda_i \alpha_i$ be an element of the E_8 lattice, so $\lambda_i \in \mathbb{Z}$. Then*

(i) If $\lambda_4 \not\equiv 0$ mod 3, then $|\langle a, b\rangle \lambda| = 9$.
(ii) If $\lambda_7 \not\equiv 0$ mod 3, then $|W(E_7)^{(3)}\lambda| \geq 27$ and $|W(E_8)^{(3)}\lambda| \geq 81$.
(iii) If $\lambda_4 \not\equiv 0$ mod 3 and $\lambda_7 = \lambda_8 = 0$, then $|W(E_6)^{(3)}\lambda| \geq 27$.

Proof. Part (i) follows from 4.7. For Part (ii), assume $\lambda_7 \not\equiv 0$ mod 3. Notice that the coefficient of α_4 in $d\lambda$ is $\lambda_4 + \lambda_7$ mod 3. So we can act on λ with d until its α_4 coefficient is not divisible by 3. Then we can apply Part (i) to see $|\langle a, b, d\rangle \lambda| \geq 27$. Also e must increase the orbit size further, so $|\langle a, b, d, e\rangle \lambda| \geq 81$.

Finally, for Part (iii), we can rewrite such a λ in the basis $\{\alpha_1, \alpha_3, \alpha_5, \alpha_6, \alpha_2, -\beta\}$, we see all 6 coefficients must be in $\frac{1}{3}\mathbb{Z}\backslash\mathbb{Z}$, and in particular are non-zero. So 4.7 implies $|W(E_6)^{(3)}\lambda| \geq 27$ as required. □

This corollory immediately gives the desired lower bounds for $\mathrm{SymRank}(\phi; 3)$. To see these bounds are achieved, take $\Lambda_{E_6} := W(E_6)^{(3)}\alpha_4$, $\Lambda_{E_7} := W(E_7)^{(3)}\alpha_7$, and $\Lambda_{E_8} := W(E_8)^{(3)}\alpha_7$. Then $|\Lambda_{E_6}| = 27$, $|\Lambda_{E_7}| = 27$ and $|\Lambda_{E_8}| = 81$, where each of these sets generate the E_6, E_7, and E_8 lattices respectively.

Finally we will check these sets satisfy (K_Γ). Consider the following relations among elements of Λ_{E_6}:

$$\alpha_4 + (\alpha_4 + \alpha_3 + \alpha_5) - (\alpha_4 + \alpha_3) - (\alpha_4 + \alpha_5) = 0$$
$$\alpha_4 + (\alpha_4 + \alpha_3 + \alpha_1 + \alpha_2) - (\alpha_4 + \alpha_3 + \alpha_1) - (\alpha_4 + \alpha_2) = 0.$$

This shows α_4 is Λ_{E_6}-independent, and hence by Lemma 1.12, we are done the E_6 case.

Consider the following relations among elements of Λ_{E_7}:

$$\alpha_7 + (\alpha_7 + \alpha_6 + \beta - \alpha_2) - (\alpha_7 + \alpha_6) - (\alpha_7 + \beta - \alpha_2) = 0$$
$$\alpha_7 + (\alpha_7 + \alpha_6 + \alpha_5 + \alpha_{E_6}) - (\alpha_7 + \alpha_6 + \alpha_5) - (\alpha_7 + \alpha_{E_6}) = 0.$$

This shows α_7 is Λ_{E_7}-independent, and also Λ_{E_8}-independent. So by Lemma 1.12, we are done.

4.9. **Case ${}^1E_6^{+3}$, at $p = 3$.** We will write elements of the lattice E_6^{+3} in coordinates of $\{\alpha_1, \alpha_3; \alpha_6, \alpha_5; -\alpha_{E_6}, \alpha_2\}$, corresponding to the three "arms" of the extended Dynkin diagram of E_6. Then the lattice E_6 is additively generated by these 6 linearly independent vectors together with $\alpha_4 = \frac{1}{3}(-1, -2; -1, -2; -1, -2)$, and E_6^{+3} is generated by E_6 together with $v := \frac{1}{3}(1, 2; 0, 0; -1, -2)$.

Observe that for any element, written in coordinates as above, $\lambda = (\lambda_1, \lambda_2; \lambda_3, \lambda_4; \lambda_5, \lambda_6) \in E_6^{+3}$ we must have: $\lambda_1 + \lambda_2$, $\lambda_3 + \lambda_4$, $\lambda_5 + \lambda_6$ are all integers, and also $\lambda_1 + \lambda_3 + \lambda_5$, $\lambda_2 + \lambda_4 + \lambda_6$ are both integers. These observations imply that if λ has a non-integral first coordinate, then the second coordinate is also non-integral and different from the first. Furthermore, either both λ_3, λ_4 are non-intergral or both λ_5, λ_6 are non-integral. Such a λ must exist in a 3-generating subset, and one checks that its $W(E_6)^{(3)}$-orbit is at least size 27. This shows the lower bound. To see this bound is achieved, notice that $\Lambda = W(E_6)^{(3)} \cdot v$ is size 27 and generates the lattice.

Let us check Λ satisfies (K_Γ). Notice the following relations in Λ:

$$v + acv + a^2c^2v = 0,$$
$$v + dv + d^2v = 0.$$

This shows v is Λ-independent, so by Lemma 1.12, we are done.

4.10. **Cases ${}^1E_6$, ${}^1E_7$, and ${}^1E_8$, at $p = 5$.** Choose $A_4 \subset E_6$ generated by $\{\alpha_3, \alpha_4, \alpha_5, \alpha_6\}$. We can choose a Sylow 5-subgroup $\Gamma := W(A_4)^{(5)} = W(E_6)^{(5)}$. Then Γ fixes the highest root α_{E_6}, and sends α_1 to $\alpha_1 + \alpha_i$ for $i \in \{3, 4, 5, 6\}$. So $\Lambda := \Gamma \cdot \alpha_1 \cup \{-\alpha_{E_6}\}$ is Sylow invariant, and generates an index 2 sublattice in E_6 (since the α_2 coefficient of the highest root is 2). Thus $\mathrm{SymRank}(\phi; 5) = \dim(E_6)$.

For E_7, similarly we can choose $A_4 \subset E_7$ generated by the simple roots $\{\alpha_4, \alpha_5, \alpha_6, \alpha_7\}$, and then we have the Sylow 5-subgroup $\Gamma := W(A_4)^{(5)} \cong W(E_7)^{(5)}$, which fixes α_1 and the highest root α_{E_7}. Furthermore, Γ sends α_3 to $\alpha_3 + \alpha_i$ for $i \in \{4, 5, 6, 7\}$. Then $\Lambda := \Gamma \cdot \alpha_3 \cup \{\alpha_1, \alpha_{E_7}\}$ is Sylow invariant, and it generates an index 2 sublattice in E_7. Thus $\mathrm{SymRank}(\phi; 5) = \dim(E_7)$.

For E_8 we choose a sublattice $A_4 \times A_4 \subset E_8$ generated by $\{\alpha_1, \alpha_3, \alpha_4, \alpha_2\}$ together with $\{\alpha_6, \alpha_7, \alpha_8, \alpha_0\}$, where α_0 is the highest root of E_8. We have $\Gamma := W(A_4)^{(5)} \times W(A_4)^{(5)} \cong W(E_8)^{(5)}$, but the sublattice is index 5. Indeed, any 5-generating subset

$\Lambda \subset E_8$ must contain an element whose coefficient of α_5 (when written in the basis of simple roots) is not divisible by 5. One checks that such an element has Γ-orbit size 25. This bound is achieved with $\Lambda := \Gamma \cdot \alpha_5$.

Let us check that Λ satisfies (K_Γ). We can choose generates σ_1, σ_2 of the two copies of $W(A_4)^{(5)} \cong \mathbb{Z}/5$ such that $\sigma_1\alpha_5 = \alpha_5 + \alpha_2 + \alpha_4$, and $\sigma_2\alpha_5 = \alpha_5 + \alpha_6$. With the choices we have:

$$\alpha_5 + \sigma_1\sigma_2\alpha_5 - \sigma_1\alpha_5 - \sigma_2\alpha_5 = 0,$$
$$\alpha_5 + \sigma_1^2\sigma_2^2\alpha_5 - \sigma_1^2\alpha_5 - \sigma_2^2\alpha_5 = 0.$$

So α_5 is Λ-independent, and hence by Lemma 1.12 we are done.

4.11. **Cases ${}^1E_7$ and ${}^1E_8$, at $p = 7$.** Take $A_6 \subset E_7 \subset E_8$ generated by $\{\alpha_1, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7\}$, and then take $\Gamma := W(A_6)^{(7)} = W(E_7)^{(7)} = W(E_8)^{(7)}$. Then Γ sends the highest root α_{E_7} to $\alpha_{E_7} + \alpha_i$, and sends α_8 to $\alpha_8 + \alpha_i$ for any $i \in \{1, 3, 4, 5, 6, 7\}$. So $\Lambda_{E_7} := \Gamma \cdot \alpha_{E_7}$ generates an index 2 sublattice in E_7, and $\Lambda_{E_8} := \Gamma \cdot \alpha_8$ generates an index 2 sublattice in E_8. So in both cases the symmetric 7-rank is equal to the rank.

5. Loose ends

Given a pair (G, p) of a split simple algebraic group and a prime p, which does not appear in Tables I, II, or III, we have $\mathrm{ed}(N; p) = \mathrm{ed}(W; p)$, by Theorem 1.9. For completeness, we will compute $\mathrm{ed}(W; p)$ for all Weyl groups of irreducible root systems at all primes p. Then we will consider the individual cases of pairs (G, p) which have an entry in the Tables, but the (K) column contains an "n"; in other words the cases not covered by Corollory 1.11.

5.1. **Essential p-dimension of the Weyl groups.** In Table IV we list all values $\mathrm{ed}(W(R); p)$ for primes p. Though not directly related to this paper, we also we list value of $\mathrm{ed}(W(R)) = \mathrm{ed}(W(R); 0)$ when it is known, assuming $\mathrm{char}\, k \neq 2$ (see Remark 5.2 for further discussion).

R	$p=0$	$p=2$	$p=3$	$p=5$	$p=7$	$p \geq 11$
A_n	??	$\lfloor \frac{n+1}{2} \rfloor$	$\lfloor (n+1)/p \rfloor$			
B_n	n	n	$\lfloor n/p \rfloor$			
C_n	n	n	$\lfloor n/p \rfloor$			
D_n (n odd)	$n-1$	$n-1$	$\lfloor n/p \rfloor$			
D_n (n even)	n	n	$\lfloor n/p \rfloor$			
E_6	??	4	3	1	0	0
E_7	7	7	3	1	1	0
E_8	8	8	4	2	1	0
F_4	4	4	2	0	0	0
G_2	2	2	1	0	0	0

Table IV. Essential dimensions of Weyl groups, $\mathrm{ed}(W; p)$

We know $\mathrm{ed}(S_n; p)$ is the floor of n/p, by [MR09, Cor. 4.2]. So for $p \neq 2$, this gives values in the A_n, B_n, C_n, and D_n cases. For $p = 2$, notice $W(B_n) = W(C_n)$ contains $(\mathbb{Z}/2)^n$, and hence has essential 2-dimension at least n (and therefore equal to n). For $W(D_n)$, we have $\mathrm{ed}((\mathbb{Z}/2)^{n-1} \rtimes S_n; 2)$ is $n-1$ for n odd (has a faithful $n-1$ dimensional representation, and contains $(\mathbb{Z}/2)^{n-1}$, which has essential 2-dimension $n-1$), and $\mathrm{ed}(W(D_n); 2) = n$ for n even (see [MR10, Prop. 5.2]).

For the exceptional groups, only the primes 2 and 3 require explanation, and we leave the F_4 and G_2 cases to the reader. At $p = 2$, we have that $W(D_8) \subset W(E_8)$, and there is a faithful 8-dimensional representation of $W(E_8)$, so $\mathrm{ed}(W(E_8); 2) = 8$. We have $W(D_5)^{(2)} \cong W(E_6)^{(2)}$, and so $\mathrm{ed}(W(E_6); 2) = 4$.

The hardest case is E_7. We have that $W(E_7)$ contains $W(D_6)$, so $6 \leq \mathrm{ed}(W(E_7); 2) \leq 7$. Let $\Gamma = W(E_7)^{(2)}$, and one can check (for example, with a computer algebra program), that the centre of Γ is isomorphic to $(\mathbb{Z}/2)^3$, and that the intersection of the centre with $[\Gamma, \Gamma]$ is the group $(\mathbb{Z}/2)^2$. So we can apply [MR10, Theorem 1.2] to see that $\mathrm{ed}(\Gamma; 2)$ is odd. Therefore, it is $\mathrm{ed}(W(E_7); 2) = 7$.

For $p = 3$, one sees that $W(E_6)^{(3)} \cong S_9^{(3)}$, and hence $\mathrm{ed}(W(E_7); 3) = \mathrm{ed}(W(E_6); 3) = \lfloor 9/3 \rfloor = 3$. And $W(E_8)^{(3)} \cong \mathbb{Z}/3 \times W(E_6)^{(3)}$, so $\mathrm{ed}(W(E_8); 3) = 4$.

For the absolute essential dimension, that is $\mathrm{ed}(W; 0) := \mathrm{ed}(W)$, notice that for D_n for n even, B_n, C_n, E_8, E_7, F_4, and G_2, we have that $\mathrm{ed}(W(R); 2) \leq \mathrm{ed}(W) \leq \mathrm{rank}(R) = \mathrm{ed}(W(R); 2)$. We also know that, for n odd, $\mathrm{ed}(W(D_n)) = n - 1$, by [FF08, Theorem 5.4].

For the standard representation of $W(E_6)$, negation is not in the Weyl group, so $\mathrm{ed}(W(E_6)) \leq 6 - 1$ ([BF03, Cor. 6.18]). But the best lower bound we have is given by $\mathrm{ed}(W(E_6); 2)$, and hence $4 \leq \mathrm{ed}(W(E_6)) \leq 5$.

Remark 5.2. Computing $\mathrm{ed}(W(A_n))$ is a well-known open problem, and was one of the motivations behind the definition of essential dimension in [BR97]. The values $\mathrm{ed}(W(A_n))$ have only been computed for small values of n. For $n = 1, 2, 3, 4$, and 5 the values are 1,1,2,2, and 3, respectively (assuming $\mathrm{char}\, k = 0$; see [BR97]). Recently Duncan has shown $\mathrm{ed}(W(A_6)) = 4$ (see [Du10], which also contains the most recent bounds for larger n). The only other case where $\mathrm{ed}(W(R))$ is unknown for an irreducible root system is $\mathrm{ed}(W(E_6))$, which could be 4 or 5.

5.3. **Cases when (K_Γ) is not satisfied.** The following are the split simple algebraic groups which appear in Table I, II, or III, and have an "n" in the (K) column. In these cases, the best known upper bound for $\mathrm{ed}(N; p)$ comes from Theorem 1.9. The best lower bound comes from either Theorem 1.9, or $\mathrm{ed}(G; p) \leq \mathrm{ed}(N; p)$. In some cases the upper and lower bounds do not match, and hence the essential p-dimension of the normalizer is still not known exactly.

5.4. **Case SL_n.** Here Theorem 1.9 gives us $\lfloor n/p \rfloor \leq \mathrm{ed}(N; p) \leq 1 + \lfloor n/p \rfloor$.

5.5. **Case PGL_p.** The upper bound from Theorem 1.9 is $\mathrm{ed}(N; p) \leq 2$, and we also know that $\mathrm{ed}(PGL_p; p) = 2$ (see [RY00, Lemma 8.5.7]), which gives a lower bound. Hence $\mathrm{ed}(N; p) = 2$ in this case.

5.6. **Case SL_4/μ_2.** The upper bound from Theorem 1.9 gives $\mathrm{ed}(N;2) \leq 6-3+2 = 5$. We also know that $\mathrm{ed}(SL_4/\mu_2;2) = 4$, where the lower bound follows from the non-triviality of a cohomological invariant defined on SL_4/μ_2-torsors (see [RST06]). So $4 \leq \mathrm{ed}(N;p) \leq 5$.

5.7. **Case SO_{2n}.** For n odd, the upper bound from Theorem 1.9 gives $\mathrm{ed}(N;2) \leq 2n-n+(n-1) = 2n-1$, and we know that $\mathrm{ed}(SO_{2n};2) = 2n-1$. So $\mathrm{ed}(N;2) = 2n-1$. But for n even, $\mathrm{ed}(W;2) = n$, so we only know that $2n-1 \leq \mathrm{ed}(N;2) \leq 2n$.

5.8. **Case SO_{2n+1}.** The upper bound of Theorem 1.9 gives $\mathrm{ed}(N;2) \leq 2n-n+n = 2n$, and we know that $\mathrm{ed}(SO_{2n+1};2) = 2n$, and hence $\mathrm{ed}(N;2) = 2n$.

5.9. **Case Sp_{2n}.** From Theorem 1.9 we have that $n \leq \mathrm{ed}(N;2) \leq 2n-n+n = 2n$.

5.10. **Case G_2.** For $p = 2$, the upper bound from Theorem 1.9 gives $\mathrm{ed}(N;2) \leq 4-2+2 = 4$, and we know that $\mathrm{ed}(G_2;2) = 3$. So $3 \leq \mathrm{ed}(N;2) \leq 4$. For $p = 3$, Theorem 1.9 gives us $1 \leq \mathrm{ed}(N;3) \leq 3-2+1 = 2$.

Remark 5.11. The only case where the upper and lower bounds differ by more than 1 is $G = Sp_{2n}$. The only cases where $\mathrm{ed}(G;p) \leq \mathrm{ed}(N;p)$ is not an improvement to the lower bound given in Theorem 1.9, are $G = SL_n$ and $G = Sp_{2n}$, both of which have trivial essential dimension.

Remark 5.12. One can now check that for the cases considered in this section, even if we chose a different minimal p-generating Γ-invariant $\Lambda \subset \hat{T}$, it could never satisfy (K_Γ). This isn't obvious a priori; for example, in Section 3 we chose a subset $\Lambda \subset A_8^{+3}$ which generates the lattice, is $W(A_8)^{(3)}$-invariant, is size 30 (and hence minimal), and then we verified that Λ satisfied (K_Γ). Yet there exists another subset $\Lambda' \subset A_8^{+3}$ which is generating, Γ-invariant, and size 30, which does *not* satsify (K_Γ).

Acknowledgements

I would like to thank Zinovy Reichstein for several useful discussions, as well as Nicole Lemire and Philippe Gille for their comments. I'd also like to thank Aurel Meyer and Roland Lötscher for their corrections and comments.

References

[Bou68] N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre, Ch. 4-6*, Hermann, Paris (1968).

[BF03] G. Berhuy, G. Favi, *Essential dimension: a functorial point of view (after A. Merkurjev).* Doc. Math. 8 (2003), 279-330.

[Bo92] A. Borel, *Linear algebraic groups.* Second edition. Graduate Texts in Mathematics, 126. Springer-Verlag, New York, (1991).

[BR97] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group.* Compositio Math. 106 (1997), no. 2, 159-179.

[Ch06] V. Chernousov, *Another proof of Totaro's theorem on E_8-torsors.* Canad. Math. Bull. 49 (2006), no. 2, 196-202.

[CS93] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York (1993).

[CS88] J.H. Conway, N.J.A. Sloane, *Low-dimensional lattices. I. Quadratic forms of small determinant*, Proc. Roy. Soc. London Ser. A 418 (1988), no. 1854, 17-41.

[Du10] A. Duncan, *Essential dimensions of A_7 and S_7*. Math. Res. Lett. 17 (2010), no. 2, 263-266.

[FF08] G. Favi, M. Florence, *Tori and essential dimension.* J. Algebra 319 (2008), no. 9, 3885-3900.

[Gi04] P. Gille, *Type des tores maximaux des groupes semi-simples*, J. Ramanujan Math. Soc. 19 (2004), no. 3, 213-230.

[Hu92] J.E. Humphreys, *Reflection groups and Coxeter groups*, Cambridge Studies in Advanced Mathematics, 29. Cambridge University Press, Cambridge (1992).

[Ja87] J.C. Jantzen, *Representations of algebraic groups.* Pure and Applied Mathematics, 131. Academic Press, Inc., Boston, MA (1987).

[KM08] N.A. Karpenko, A.S. Merkurjev, *Essential dimension of finite p-groups.* Invent. Math. 172 (2008), no. 3, 491-508.

[Le04] N. Lemire, *Essential dimension of algebraic groups and integral representations of Weyl groups.*, Transform. Groups 9 (2004), no. 4, 337-379.

[LMMR10a] R. Lötscher, M.L. MacDonald, A. Meyer, Z. Reichstein, *Essential p-dimension of algebraic tori*, Preprint http://www.math.uni-bielefeld.de/LAG/man/363.html

[LMMR10b] R. Lötscher, M.L. MacDonald, A. Meyer, Z. Reichstein, *Essential dimension of algebraic tori*, Preprint: http://www.math.uni-bielefeld.de/LAG/man/399.html

[Mac08] M.L. MacDonald, *Cohomological invariants of odd degree Jordan algebras*, Math. Proc. Cambridge Philos. Soc. 145 (2008), no. 2, 295-303.

[MR09] A. Meyer, Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra Number Theory 3 (2009), no. 4, 467-487.

[MR10] A. Meyer, Z. Reichstein, *Some Consequences of the Karpenko-Merkurjev Theorem.* Documenta Math. Extra Volume: Andrei A. Suslin's Sixtieth Birthday (2010) 445-457.

[Ra04] M.S. Raghunathan, *Tori in quasi-split-groups,* J. Ramanujan Math. Soc. 19 (2004), no. 4, 281-287.

[Re10] Z. Reichstein. *Essential dimension*, ICM proceedings, (2010), to appear. Preprint: http://www.mathematik.uni-bielefeld.de/LAG/man/393.html

[RY00] Z. Reichstein, B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties.* With an appendix by János Kollár and Endre Szabó. Canad. J. Math. 52 (2000), no. 5, 1018-1056.

[RST06] M. Rost, J.-P. Serre, J.-P. Tignol, *La forme trace d'une algèbre simple centrale de degré 4.* C. R. Math. Acad. Sci. Paris 342 (2006), no. 2, 83-87.

[Se02] J.-P. Serre. *Galois cohomology.* Translated from the French by Patrick Ion and revised by the author. Corrected reprint of the 1997 English edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, (2002).

[Ti66] J. Tits, *Classification of algebraic semisimple groups.* 1966 Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965) pp. 33-62 Amer. Math. Soc., Providence, R.I., (1966)

[Vo88] V.E. Vosrekenskii, *Maximal tori without effect in semisimple algebraic groups*, Mat. Zametki **44** (1988), no. 3, 309-318, 410; English translation in Math. Notes **44** (1988), no. 3-4, 651-655 (1989)

[Vo98] V.E. Voskresenskii, *Algebraic groups and their birational invariants.* Translated from the Russian manuscript by Boris Kunyavskii. Translations of Mathematical Monographs, 179. American Mathematical Society, Providence, RI (1998).