LONGER NILPOTENT SERIES FOR CLASSICAL UNIPOTENT SUBGROUPS

JOSHUA MAGLIONE

Abstract. In studying nilpotent groups, the lower central series and other variations can be used to construct an associated $\mathbb{Z}^+$-graded Lie ring, which is a powerful method to inspect a group. Indeed, the process can be generalized substantially by introducing $\mathbb{N}^d$-graded Lie rings. We compute the adjoint refinements of the lower central series of the unipotent subgroups of the classical Chevalley groups over the field $\mathbb{Z}/p\mathbb{Z}$ of rank d. We prove that, for all the classical types, this characteristic filter is a series of length $\Theta(d^2)$ with nearly all factors having p-bounded order.

1. Introduction

The connection between p-groups and Lie rings has long been known and continues to be a symbiotic relationship. Indeed, in [5], Lazard proves that, for a series of a group G,

$$G = G_1 \geq G_2 \geq \cdots \geq G_n \geq G_{n+1} = 1,$$

if $[G_i, G_j] \leq G_{i+j}$ for all $i, j \geq 1$, then there is an associated graded Lie ring to the series given by

$$L = \bigoplus_{i=1}^{n} G_i/G_{i+1}.$$

J. B. Wilson weakened the hypothesis of Lazard's statement by replacing series with filters, and proved filters still have an associated graded Lie ring [10]. A filter ϕ is a function from a pre-ordered commutative monoid (see Definition 2.1) $(M, \prec)$ into the set of normal subgroups of G satisfying

$$(\forall m, n \in M) \qquad [\phi_m, \phi_n] \leq \phi_{m+n} \quad \text{and} \quad m \prec n \text{ implies } \phi_m \geq \phi_n.$$

Filters produce lattices of normal subgroups, and in the case where $(M, \prec)$ is totally ordered, the filter is a series.

A notable feature of filters is their ease of refinement. Given a filter from M into the normal subgroups of G, one can insert new subgroups into the lattice and generate a new filter. Wilson gives a few locations to search for new subgroups to add to filters, one of which is the adjoint refinement, which uses ring theoretic properties stemming from the graded Lie ring product.

The length of the adjoint filter, the filter stabilized by the adjoint refinement, seems difficult to predict without considering specific examples. Therefore, we work with the well known family of unipotent subgroups of classical groups, e.g. the group of upper unitriangular matrices. Surprisingly, we find something new. We compute the adjoint refinements of the lower central series of the unipotent subgroups of these groups over the field $\mathbb{Z}/p\mathbb{Z}$. After the refinement process stabilizes, we find

Date: March 10, 2015.

that the factors of this new filter are very small. Moreover, the subgroups of this filter are totally ordered, so we obtain a characteristic series. The length of the adjoint series is largely unchanged under most quotients, so this seemingly narrow case of examples is a great place to start understanding these filters on a wide range of families of p-groups.

Theorem 1.1. *If $U = \langle x_r(t) : r \in \Phi^+, t \in \mathbb{Z}/p\mathbb{Z}\rangle$ is a subgroup of the Chevalley group $A_d(\mathbb{Z}/p\mathbb{Z})$ for $p \geq 3$ (i.e. the group of upper unitriangular matrices), then all of the (nontrivial) factors of the series stabilized by the adjoint refinement process have order p or p^2.*

For comparison, the usual lower central series (which is equal to the lower central exponent p series) has large factors, many of order approximately p^d. When investigating the action of $\mathrm{Aut}(U)$ on U, Theorem 1.1 puts a large constraint on the possible actions of the automorphism group. Indeed, in the computations for isomorphism or automorphism testing, a reduction in the order of the first factor alone can greatly reduce the algorithm run time [3]. For example, the automorphism group of the first factor of the lower central series of U is $\mathrm{GL}(d, p)$. However, for the series of Theorem 1.1, the automorphism group of the first factor is $\mathrm{GL}(e, p)$, where e is either 1 or 2. For unipotent subgroups of other classical Chevalley groups, we get a similar outcome.

Theorem 1.2. *Let p be a prime with $p \geq 3$. Let $U = \langle x_r(t) : r \in \Phi^+, t \in \mathbb{Z}/p\mathbb{Z}\rangle$ be a unipotent subgroup of a classical Chevalley group over $\mathbb{Z}/p\mathbb{Z}$ with Lie rank d. There exists a characteristic series of U whose length is $\Theta(d^2)$ and whose factors have constant order (except possibly a constant number of factors). Furthermore, the associated Lie algebra, $L(\alpha)$ is $\mathbb{N}^m$-graded, where m is either $\lceil d/2\rceil$ or $\lfloor d/2\rfloor$.*

Corollary 1.3. *Let U and m be as in Theorem 1.2. Then U/U' has an $\mathrm{Aut}(U)$ invariant series of length m. There is at most one factor with dimension 1, and if U is of type D, then there is a factor of dimension 3. All other factors have dimension 2.*

As usual with these groups, the case $p = 2$ requires additional care. Modest changes need to be made for characteristic two and are addressed in Remark 4.17, at the end of Section 4. In addition, we have exclusively used the field $\mathbb{Z}/p\mathbb{Z}$, but we expect similar results for arbitrary finite fields. In this case, the order of the factors depends on the size of the field. For comments on how to generalize this approach to arbitrary finite fields, see Remark 4.18 at the end of Section 4.

The paper is organized as follows. We discuss the definition of a filter and necessary information in Section 2. In Section 3, we give a method to compute an adjoint refinement. In Section 4, we prove our main results, Theorem 1.1 and Theorem 1.2.

1.1. **Notation.** We let $\mathbb{N}$ and $\mathbb{Z}^+$ denote the set of nonnegative integers and positive integers respectively. For a set S, we denote the power set of S by 2^S. For a group G and for $x, y \in G$, we let $[x, y]$ denote $x^{-1}y^{-1}xy$. In general, we define $[x_1] = x_1$ and $[x_1, x_2, ..., x_n, x_{n+1}] = [[x_1, ..., x_n], x_{n+1}]$. If $H, K \leq G$, then $[H, K] = \langle [h, k] : h \in H, k \in K\rangle$. We use the same recursive notation for subgroups of G as we do for elements of G. Throughout the paper, p is a prime, and $\mathbb{Z}_p$ denotes the field $\mathbb{Z}/p\mathbb{Z}$.

We adopt the same notation for root systems and Chevalley groups as provided by Carter in [2, Chapters 2 – 4]. That is, we let Φ denote a system of roots. Define an ordering of the roots and let Φ^+ and Φ^- denote the positive and negative roots respectively. Let Π be the set of fundamental roots of Φ, and let $\{h_r : r \in \Pi\} \cup \{e_s : s \in \Phi\}$ be a Chevalley basis for the Lie algebra $\mathfrak{g}$ over $\mathbb{C}$ for some Cartan decomposition.

The Chevalley group of type $\mathfrak{g}$ over $\mathbb{Z}_p$, denoted $\mathfrak{g}(p)$, is the group of automorphisms of the Lie algebra $\mathfrak{g}_{\mathbb{Z}_p} = \mathfrak{g} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \langle x_r(t) : r \in \Phi, t \in \mathbb{Z}_p\rangle$, where $x_r(t) = \exp(t \text{ ad } e_r)$. The root subgroup of $r \in \Phi$ is $X_r = \langle x_r(t) : t \in \mathbb{Z}_p\rangle$. The maximal unipotent subgroups of $\mathfrak{g}(p)$ are all conjugate to the group $U = \langle X_r : r \in \Phi^+\rangle$, so in our proofs we take $U = \langle X_r : r \in \Phi^+\rangle$. Note that unipotent subgroups stay the same in all the classical groups, including special and projective, so we do not need to be specific.

2. Filters

Since Theorem 1.1 and Theorem 1.2 use a filter generation algorithm, we summarize the necessary ideas from [10, Section 3] for the sake of completeness.

Defintion 2.1. *A* pre-order $\prec$ *on a commutative monoid, M, is a reflexive and transitive relation, and for all $k, \ell, m, n \in M$, if $k \prec \ell$ and $m \prec n$, then $k+m \prec \ell+n$.*

Defintion 2.2. *A* filter *of G is a function $\phi : M \to 2^G$ such that for all $m, n \in M$, $\phi_m = \phi(m)$ is a subgroup of G,*

$$[\phi_m, \phi_n] \le \phi_{m+n} \qquad \textit{and} \qquad m \prec n \textit{ implies } \phi_m \ge \phi_n.$$

We remark that filters $\phi : \mathbb{N} \to 2^G$, with $\phi_0 = G$, are exactly the *N-series* introduced by Lazard [5]. From the definition of a filter, $\phi_m \trianglelefteq G$ for all $m \in M$.

Every filter induces a new filter $\partial\phi : M \to 2^G$ given by

$$\partial\phi_m = (\partial\phi)_m = \prod_{s \in M-\{0\}} \phi_{m+s} = \langle \phi_{m+s} : s \in M - \{0\}\rangle.$$

It follows that for each $m, n \in M$,

$$[\partial\phi_m, \phi_n] = \prod_{s\in M-\{0\}} [\phi_{m+s}, \phi_n] = \prod_{s\in M-\{0\}} \phi_{m+s+n} \le \prod_{s\in M-\{0\}} \phi_n \cap \phi_{m+s} \le \phi_{m+n}.$$

In particular, $[\partial\phi_m, \phi_m] \le \phi_m$; thus, $\partial\phi_m \trianglelefteq \phi_m$. For $m \in M$, let

$$L_m = \phi_m/\partial\phi_m. \tag{2.3}$$

Thus, by [10, Theorem 3.3], the abelian group,

$$L(\phi) = \bigoplus_{m\in M} L_m, \tag{2.4}$$

is a Lie ring with product on the homogeneous components

$$(\forall x \in \phi_s, \forall y \in \phi_t) \qquad [\partial\phi_s x, \partial\phi_t y] = \partial\phi_{s+t}[x, y]. \tag{2.5}$$

Note that if ϕ is a filter such that ϕ produces an N-series of G, then $\partial\phi$ is also an N-series and $\partial\phi_m = N_{m+1}$. In that case, $L(\phi)$ is the Lie ring described by Lazard cf. [5, Theorem 2.1].

Suppose $\mathcal{S}$ generates M as a monoid, and $0 \in \mathcal{S}$. Let $\mathcal{G} = \mathcal{G}(M, \mathcal{S})$ be the (directed) Cayley graph whose vertices are M and whose labeled edge set is $\{m \xrightarrow{s} n : m + s = n, s \in \mathcal{S}\}$. Furthermore, let $\mathcal{G}_m^n$ denote the set of all paths, $\mathbf{t}$, from

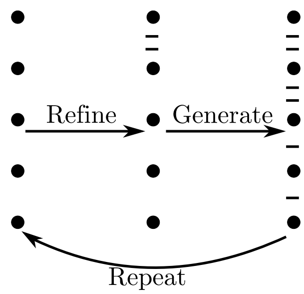

FIGURE 1. Iterating the adjoint refinement process.

vertex m to vertex n in $\mathcal{G}$. We write a path $\mathbf{t}$ as a sequence of edge labels the path traverses. That is, for each $s_i \in \mathcal{S}$, $\mathbf{t} = (s_1, ..., s_k)$ where $m + s_1 + \cdots + s_k = n$. Suppose $\pi : \mathcal{S} \to 2^G$ is a function, and for simplicity, we denote $[\pi_{s_1}, ..., \pi_{s_k}]$ by $[\pi_{\mathbf{t}}]$ if $\mathbf{t} = (s_1, ..., s_k)$. Define a new function $\bar{\pi} : M \to 2^G$ by

$$\bar{\pi}_m = \prod_{\mathbf{t} \in \mathcal{G}_0^m} [\pi_{\mathbf{t}}]. \tag{2.6}$$

We close this section with sufficient conditions on M, $\mathcal{S}$ and π so that $\bar{\pi}$ is a filter.

Defintion 2.7. *A* generalized refinement monoid $(M, \prec)$ *is a commutative preordered monoid with minimal element* 0 *and if* $m \prec n$ *and* $n = \sum_{i=1}^{r} n_i$*, then there exists* $m_i \prec n_i$ *where* $m = \sum_{i=1}^{r} m_i$*.*

Theorem 2.8 (Wilson [10, Theorem 3.9])**.** *Suppose* $(M, \prec)$ *is a generalized refinement monoid and* $0 \in \mathcal{S} \subset M$ *is an interval closed generating set of* M*. If* $\pi : \mathcal{S} \to 2^G$ *is an order reversing function into the set of normal subgroups of* G*, then* $\bar{\pi}$ *is a filter.*

3. Constructing the Stable Adjoint Series

For Theorems 1.1 and 1.2, we will use the adjoint series introduced by Wilson [10, Section 4]. To produce the adjoint series (or *α-series*), we iterate a refinement process until it stabilizes. There are two major steps in computing the adjoint series: finding the new subgroups to add at the top of the series and generating the lower terms of the series. The former is nearly independent from the latter, so we can find all the new subgroups that get added to the top section (successively) before we start to generate the lower terms. This is essentially how we approach our investigation of the adjoint series in Section 4. Figure 1 gives a visualization of the basic process.

We begin by describing how we obtain new subgroups. Let $\phi : (\mathbb{N}, \leq) \to 2^G$ be a filter, and set $\alpha_n^{(1)} = \phi_n$ for all $n \in \mathbb{N}$. In our construction, we use the lower central series of G as our initial filter, which is indexed by $\mathbb{Z}^+$. This allows for the opportunity to record operators (e.g. the holomorph of G) at the top of the filter, ϕ_0, even though we presently take ϕ_0 to be G. We define the $\alpha^{(1)}$-series to be the filter $\alpha^{(1)} : \mathbb{N} \to 2^G$, and in general, the $\alpha^{(k)}$-series is a filter $\alpha^{(k)} : (\mathbb{N}^k, \prec) \to 2^G$ inductively produced as follows, where $\prec$ is the lexicographic order.

As established in Section 2, if $n \in \mathbb{N}^k$, then $L_n^{(k)} = \alpha_n^{(k)}/\partial\alpha_n^{(k)}$ is a homogenous component of the associated $\mathbb{N}^k$-graded Lie algebra $L(\alpha^{(k)})$ cf. (2.3) and (2.4). To obtain the $\alpha^{(k+1)}$-series from the $\alpha^{(k)}$-series for $k \geq 1$, we use the graded product map $\circ : L_s^{(k)} \times L_t^{(k)} \to L_{s+t}^{(k)}$ given by communtation in G cf. (2.5).

Defintion 3.1. *The* adjoint ring of $\circ$ *is*

$$\operatorname{Adj}(\circ) = \Big\{(f,g) \in End\left(L_s^{(k)}\right) \times End\left(L_t^{(k)}\right)^{op} : \forall u \in L_s^{(k)}, \forall v \in L_t^{(k)}, uf \circ v = u \circ gv\Big\}.$$

This is our source of new (characteristic) subgroups. Another characterization of the adjoint ring of $\circ$ is to define it as the ring for which $\circ$ factors through $\otimes_{\operatorname{Adj}(\circ)} : L_s^{(k)} \times L_t^{(k)} \to L_s^{(k)} \otimes_{\operatorname{Adj}(\circ)} L_t^{(k)}$ uniquely. This latter characterization implies that the properties of $\operatorname{Adj}(\circ)$ influence the properties of $\circ$, and hence commutation in G. See [9, Section 2] for further details on adjoints.

We choose $(s,t) \in \mathbb{N}^k \times \mathbb{N}^k$ to be the lex least pair where the Jacobson radical of $\operatorname{Adj}(\circ)$ is nontrivial. Let J be the Jacobson radical of $\operatorname{Adj}(\circ)$, and let $J^0 = \operatorname{Adj}(\circ)$. Recursively define $J^{i+1} = J^i J$ for all $i \in \mathbb{N}$. For all $i \in \mathbb{N}$, define H_i so that $\alpha_s^{(k)} \geq H_i \geq \partial\alpha_s^{(k)}$ and

$$H_i/\partial\alpha_s^{(k)} = L_s^{(k)} J^i. \tag{3.2}$$

If $J = 0$, then we get no new subgroups. If $J = 0$ for each $(s,t) \in \mathbb{N}^k \times \mathbb{N}^k$, then the $\alpha^{(k)}$-series has no nontrivial adjoint refinement.

To incorporate these new subgroups into a filter, we first obtain a generating set for $\mathbb{N}^{k+1}$ which includes the indices of the new subgroups. Let

$$\mathcal{S}_{k+1} = \{(n,i) \in \mathbb{N}^k \times \mathbb{N} : n \preceq s\}, \tag{3.3}$$

so that $\mathcal{S}_{k+1}$ is interval closed and generates $\mathbb{N}^{k+1}$. For $(n,i) \in \mathbb{N}^k \times \mathbb{N}$, define

$$\pi_n^i = \begin{cases} \alpha_n^{(k)} & \text{if } n \prec s, \\ H_i & \text{if } n = s. \end{cases} \tag{3.4}$$

Observe that π is a function from $\mathcal{S}_{k+1}$ into the normal subgroups of G (which is totally ordered with respect to $\prec$ the lexicographic order) which satisfies the conditions of Theorem 2.8. Thus, $\bar{\pi} : \mathbb{N}^{k+1} \to 2^G$ is a filter, and we set $\alpha^{(k+1)} = \bar{\pi}$. We refer to the filter $\alpha^{(k+1)}$ as the $\alpha^{(k+1)}$-series.

We show that the adjoint series is a characteristic series.

Proposition 3.5. *If the initial filter, $\phi : \mathbb{N} \to 2^G$, is a characteristic series, then the adjoint series of G is a characteristic series.*

To prove the proposition, we show that $\operatorname{Aut}(G)$ acts on $\operatorname{Adj}(\circ)$ via conjugation. From [7, Proposition 3.8], $\operatorname{Aut}(G)$ maps into the *pseudo-isometries* of $\circ$, which are defined to be

$$\Psi\operatorname{Isom}(\circ) = \left\{(h,\hat{h}) \in \operatorname{Aut}\left(L_s^{(k)}\right) \times \operatorname{Aut}\left(L_{2s}^{(k)}\right) : xh \circ hy = (x \circ y)\hat{h}\right\}.$$

The pseudo-isometries of $\circ$ act on $\operatorname{Adj}(\circ)$ by conjugation as the following lemma proves.

Lemma 3.6. $\Psi\operatorname{Isom}(\circ)$ *acts on* $\operatorname{Adj}(\circ)$ *by*

$$(f,g)^{(h,\hat{h})} = (h^{-1}fh, hgh^{-1}) \in \operatorname{Adj}(\circ),$$

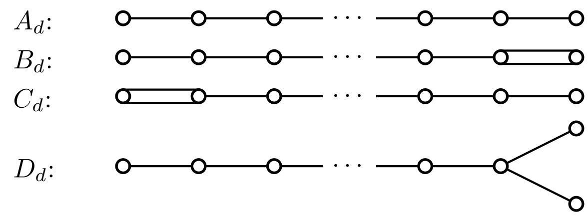

FIGURE 2. The Dynkin diagrams for the different classical types of root systems.

for $(f, g) \in \mathrm{Adj}(\circ)$ *and* $(h, \hat{h}) \in \Psi\,\mathrm{Isom}(\circ)$. *Furthermore, this action is faithful.*

Proof. Let $x, y \in L_{e_1}^{(k)}$. It follows that $\Psi\,\mathrm{Isom}(\circ)$ acts on $\mathrm{Adj}(\circ)$ as

$$xh^{-1}fh \circ y = (xh^{-1}f \circ h^{-1}y)\hat{h} = (xh^{-1} \circ gh^{-1}y)\hat{h} = x \circ hgh^{-1}y.$$

It follows that this action is faithful because h and $\hat{h}$ are automorphisms cf. [7, Proposition 4.16]. □

Proof of Proposition 3.5. By [7, Proposition 3.8], $\mathrm{Aut}(G)$ maps into $\Psi\,\mathrm{Isom}(\circ)$. Therefore, by Lemma 3.6, $\mathrm{Aut}(G)$ acts on $\mathrm{Adj}(\circ)$ by conjugation. Furthermore, since J is the intersection of all maximal ideals in $\mathrm{Adj}(\circ)$, it follows that the action of $\mathrm{Aut}(G)$ fixes J. Thus, J^i is fixed by the action of $\mathrm{Aut}(G)$ for every $i \in \mathbb{Z}^+$. Therefore, $L_{e_1}^{(k)}J^n$ is characteristic, and hence, π_n is characteristic for $n \in \mathbb{N}^{k+1}$, provided $\alpha^{(k)}_{(n_1,\dots,n_k)}$ is characteristic. Since ϕ_m is characteristic for $m \in \mathbb{N}$, it follows by induction that each term in the $\alpha^{(k+1)}$-series is characteristic. □

4. The Stable Adjoint Refinement of Classical Unipotent Groups

In this section we prove Theorems 1.1 and 1.2. Most of our work goes into proving Theorem 1.1; we will see that Theorem 1.2 follows from the proof of Theorem 1.1. Recall that the adjoint series is a refinement of some other (characteristic) series. Let $U \leq \mathfrak{g}(p)$ be a unipotent subgroup. Our initial series is the lower central series and we denote the k^{th} term of the series by $\gamma_k(U)$ or γ_k. We let $\gamma_0(U) = U$, so that $\mathbb{N}$ indexes our filter. Let $\circ$ be the graded product map given in (2.5).

For details on Chevalley groups, root systems, and Lie algebras see [2]. Recall the Chevalley commutator formula

Theorem 4.1 (Chevalley)**.** *Let* $u, t \in \mathbb{Z}_p$ *and* $s, r \in \Phi$. *Then for each* $i, j > 0$ *with* $ir + js \in \Phi$, *there exists constants* C_{ijrs} *such that*

$$[x_s(u), x_r(t)] = \prod_{i,j>0} x_{ir+js}(C_{ijrs}(-t)^i u^j) \tag{4.2}$$

where the product is taken in increasing order of $i + j$.

The details for the constants C_{ijrs} can be found in [2, p. 77]. We denote the fundamental roots, p_i, to be consistent with the Dynkin diagram for $\mathfrak{g}$. That is, p_1 is connected to p_2, p_2 is connected to both p_1 and p_3, and so on. The Dynkin diagrams for different types of root systems are given in Figure 2. We choose an ordering of the fundamental roots Π so that $p_i \prec_\Pi p_j$ if $i < j$. Thus, if (r, s) is an extra-special pair of roots (i.e. $r + s \in \Phi$, $0 \prec_\Pi r \prec_\Pi s$ and for all $r_1 + s_1 = r + s$, $r \preceq_\Pi r_1$), then $[e_r, e_s] = -(v + 1)e_{r+s}$; cf. [2, p. 58].

Note that for every $r \in \Phi^+$, we can write

$$r = p_{i_1} + \cdots + p_{i_k}, \tag{4.3}$$

for (not necessarily distinct) $p_{i_j} \in \Pi$. Thus, we may talk about the *height* of each (positive) root r denoted $h(r)$ which is the sum of the integer coefficients of r when written as in (4.3). We say a root subgroup X_r has height m if $h(r) = m$. Let U_m denote the subgroup generated by all X_r such that $h(r) \geq m$. As the next lemma states, these subgroups almost always coincide with the lower central series of U.

Lemma 4.4 (Spitznagel [6, Theorem 1])**.** *Let U be a maximal unipotent subgroup of a classical Chevalley group over $\mathbb{Z}_p$. If U is of type B or C and $p = 2$, then $\gamma_2(U) \neq U_2 = \langle X_r : h(f) \geq 2, r \in \Phi^+\rangle$. Otherwise, $\gamma_m(U) = U_m$ for all m.*

Because of Lemma 4.4, we assume $p \geq 3$ for types B and C. Some comments about when $p = 2$ are given at the end of the section, see Remark 4.17. From Lemma 4.4, it follows that $L_i^{(1)} = U_i/U_{i+1}$ is the quotient containing all root subgroups of height i. Since there are exactly d fundamental roots, $L_1^{(1)} \cong \mathbb{Z}_p^d$. Furthermore, since there are exactly $d-1$ positive roots with height 2, $L_2^{(1)} \cong \mathbb{Z}_p^{d-1}$. Therefore, $\circ$ may be regarded as an alternating $\mathbb{Z}_p$-bilinear map, $\circ : \mathbb{Z}_p^d \times \mathbb{Z}_p^d \to \mathbb{Z}_p^{d-1}$.

We construct the structure constants $M_\mathfrak{g}$ (Gram matrix) of $\circ$ for the classical types $\mathfrak{g}$, i.e. for all $u, v \in \mathbb{Z}_p^d$, $u \circ v = uM_\mathfrak{g}v^t$. Observe that for type A,

$$[x_{p_i}(s), x_{p_j}(t)] = \begin{cases} x_{p_i+p_j}(st) & \text{if } (p_i, p_j) \text{ is extra special,} \\ x_{p_i+p_j}(-st) & \text{if } (p_j, p_i) \text{ is extra special,} \\ 0 & \text{otherwise.} \end{cases} \tag{4.5}$$

Define $\varphi_1 : L_1 \to \mathbb{Z}_p^d$ by $\varphi_1(\gamma_2 x_{p_i}(t)) = te_i$, and define $\varphi_2 : L_2 \to \mathbb{Z}_p^{d-1}$ by $\varphi_2(\gamma_3 x_{p_i+p_j}(t)) = te_{j-1}$, provided $i < j$. Note that both φ_1 and φ_2 are vector space isomorphisms. Thus, by (4.5), the structure constants matrix for $A_d(p)$ is

$$M_A = \begin{bmatrix} 0 & e_1 & & & \\ -e_1 & 0 & e_2 & & \\ & -e_2 & 0 & \ddots & \\ & & \ddots & \ddots & e_{d-1} \\ & & & -e_{d-1} & 0 \end{bmatrix}. \tag{4.6}$$

Lemma 4.7. *Let $M_\mathfrak{g}$ be the structure constants for $\circ$ of $\mathfrak{g}(p)$. Then $M_\mathfrak{g}$ has the same shape as the Cartan matrix of the root system of type $\mathfrak{g}$.*

Proof. This follows from the Chevalley commutator formula (4.2). ∎

Hence, the structure constant matrices M_B and M_C are equal to M_A, provided they are the same rank. Finally, for type D, we have

$$M_D = \begin{bmatrix} 0 & e_1 & & & & \\ -e_1 & 0 & \ddots & & & \\ & \ddots & \ddots & e_{d-3} & & \\ & & -e_{d-3} & 0 & e_{d-2} & e_{d-1} \\ & & & -e_{d-2} & 0 & 0 \\ & & & -e_{d-1} & 0 & 0 \end{bmatrix}. \tag{4.8}$$

Now we compute the adjoint rings of these bilinear maps. By Lemma 4.7, the adjoint rings for M_A, M_B, and M_C are the same, but the adjoint ring for M_D is different. For each $i \in \{1, ..., d-1\}$, let $M_i \in \mathrm{M}_d(\mathbb{Z}_p)$ to be the matrix with 1 in the $(i, i+1)$ entry, -1 in the $(i+1, i)$ entry, and 0 elsewhere. Similarly, let $N \in \mathrm{M}_d(\mathbb{Z}_p)$ be the matrix with 1 in the $(d-2, d)$ entry and -1 in the $(d, d-2)$ entry, and 0 elsewhere. Therefore, $M_A = \sum_{i=1}^{d-1} e_i M_i$ and $M_D = \sum_{i=1}^{d-2} e_i M_i + e_{d-1} N$. It follows that

$$\mathrm{Adj}\,(M_1) = \left\{ \left(\begin{bmatrix} w & x & * \\ y & z & * \\ 0 & 0 & * \end{bmatrix}, \begin{bmatrix} z & -x & * \\ -y & w & * \\ 0 & 0 & * \end{bmatrix} \right) : w,x,y,z \in \mathbb{Z}_p \right\} \text{ and}$$

$$\mathrm{Adj}\,(N) = \left\{ \left(\begin{bmatrix} * & 0 & * & 0 \\ * & w & * & x \\ * & 0 & * & 0 \\ * & y & * & z \end{bmatrix}, \begin{bmatrix} * & 0 & * & 0 \\ * & z & * & -x \\ * & 0 & * & 0 \\ * & -y & * & w \end{bmatrix} \right) : w,x,y,z \in \mathbb{Z}_p \right\}.$$

Note that we can obtain M_i from M_1 by applying a permutation. Applying such a permutation also permutes the adjoint ring, and therefore

$$\mathrm{Adj}\,(M_i) = \left\{ \left(\begin{bmatrix} * & 0 & 0 & * \\ * & w & x & * \\ * & y & z & * \\ * & 0 & 0 & * \end{bmatrix}, \begin{bmatrix} * & 0 & 0 & * \\ * & z & -x & * \\ * & -y & w & * \\ * & 0 & 0 & * \end{bmatrix} \right) : w,x,y,z \in \mathbb{Z}_p \right\}.$$

Observe that $\mathrm{Adj}\,(M_A) = \mathrm{Adj}\left(\sum_{i=1}^{d-1} e_i M_i\right) = \bigcap_{i=1}^{d-1} \mathrm{Adj}\,(M_i)$. For $x, y, z \in \mathbb{Z}_p$, let $D(x, y) \in \mathrm{M}_d(\mathbb{Z}_p)$ denote the diagonal matrix with diagonal $(x, y, x, y, ...)$, $Q_A(x, y) = xE_{12} + yE_{(d-1)d}$, and $Q_D(x, y, z) = xE_{12} + yE_{(d-2)(d-1)} + zE_{(d-2)d}$. Thus,

$$\begin{aligned} \mathrm{Adj}\,(M_A) &= \{(D(w,x) + Q_A(y,z), D(x,w) - Q_A(y,z)) : w,x,y,z \in \mathbb{Z}_p\} \\ \mathrm{Adj}\,(M_D) &= \{(D(v,w) + Q_D(x,y,z), D(w,v) - Q_D(x,y,z)) : v,w,x,y,z \in \mathbb{Z}_p\}. \end{aligned}$$

Now we describe the Jacobson radical of the adjoint rings of M_A and M_D; denote the radicals J_A and J_D respectively. If $d \geq 3$ (or $d \geq 4$ for type D as D_3 and A_3 are the same root systems), then

$$J_A = \{(Q_A(y,z), -Q_A(y,z)) : y,z \in \mathbb{Z}_p\} \tag{4.9}$$

$$J_D = \{(Q_D(x,y,z), -Q_D(x,y,z)) : x,y,z \in \mathbb{Z}_p\}. \tag{4.10}$$

Otherwise (if $d \leq 2$), the adjoint ring of the forms

$$[0] \quad \text{and} \quad \begin{bmatrix} 0 & e_m \\ -e_m & 0 \end{bmatrix}$$

is $\mathbb{Z}_p$ and $\mathrm{M}_2(\mathbb{Z}_p)$ (resp.), which both have trivial Jacobson radical. Note that $J_A^2 = J_D^2 = 0$. Thus we get at most one new subgroup at the top of the series corresponding to $L_1 J_A$ (or $L_1 J_D$). In fact, the new subgroup is

$$H_1 = \begin{cases} \langle X_{p_1}, X_{p_d}, \gamma_2 \rangle & \text{if type } A, B, \text{ or } C, \\ \langle X_{p_1}, X_{p_{d-1}}, X_{p_d}, \gamma_2 \rangle & \text{if type } D, \end{cases} \tag{4.11}$$

and $H_i = \gamma_2$ for all $i \geq 2$ c.f. (3.2).

For each iteration of the computation, we use the bilinear map, given by commutation, from the first nonzero factor of the $\alpha^{(k)}$-series. This bilinear map depends on U/H_1 and $\gamma_2/\partial\gamma_2$. We remark that the quotient $\gamma_2/\partial\gamma_2$ in the second iteration contains all root subgroups X_r with $h(r) = 2$ where both $r - p_1, r - p_d \notin \Phi^+$ (additionally $r - p_{d-1} \notin \Phi^+$ if type D). Note that if $\widetilde{U}$ is the unipotent subgroup of $A_{d-2}(p)$ ($A_{d-3}(p)$ if type D), then commutation in U/H_1 is the same as commutation in $\widetilde{U}/\gamma_2(U)$ (up to relabeling). Thus, the structure constants for $* : U/H_1 \times U/H_1 \to \gamma_2(U)/\partial\gamma_2(U)$, is given by (4.6) for all types, except the structure constants have smaller dimension:

$$M_* = \begin{bmatrix} 0 & e_2 & & \\ -e_2 & 0 & \ddots & \\ & \ddots & \ddots & e_{d-2} \\ & & -e_{d-2} & 0 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 0 & e_2 & & \\ -e_2 & 0 & \ddots & \\ & \ddots & \ddots & e_{d-3} \\ & & -e_{d-3} & 0 \end{bmatrix}.$$

If U is the unipotent subgroup of the classical group $\mathfrak{g}(p)$, then after the first iteration the structure constants matrix of commutation is given by (4.6), except with smaller dimension. Thus, for the subsequent iterations, we cut the dimension by two and the structure constants matrix is similar to (4.6). This proves the following proposition since each iteration adds a dimension to the monoid which indexes the associated Lie algebra.

Proposition 4.12. *The associated Lie algebra of the adjoint series is $\mathbb{N}^m$-graded, with $m = \lceil \frac{d}{2} \rceil$ (types A, B, or C) or $m = \lfloor \frac{d}{2} \rfloor$ (type D).*

Because the bilinear maps essentially stay the same, we can easily list the top of the adjoint series. Let H_1 be defined as in (4.11) and $H_k = \langle X_{p_k}, X_{p_{d-k+1}}, H_{k-1} \rangle$ for $k \geq 2$ (if type D, then $H_k = \langle X_{p_k}, X_{p_{d-k}}, H_{k-1} \rangle$). With m given by Proposition 4.12,

$$U \geq H_{m-1} \geq \cdots \geq H_1 \geq \gamma_2 \geq \cdots \geq \gamma_c \geq 1, \tag{4.13}$$

without filter generation. Observe that if U is of type A, B, or C, then

$$|U/H_{m-1}| = \begin{cases} p & \text{if } 2 \nmid d, \\ p^2 & \text{if } 2 \mid d, \end{cases}$$

and $|H_{k+1}/H_k| = |H_1/\gamma_2| = p^2$, for $1 \leq k \leq m-2$. On the other hand, if U is of type D, then

$$|U/H_{m-1}| = \begin{cases} p^2 & \text{if } 2 \nmid d, \\ p & \text{if } 2 \mid d, \end{cases}$$

$|H_{k+1}/H_k| = p^2$, for $1 \leq k \leq m-2$, and $|H_1/\gamma_2| = p^3$. Therefore, Corollary 1.3 follows.

Now we investigate the lower terms of the adjoint series of these unipotent groups. Currently, the series in (4.13) has $\Theta(d)$ terms and it may not be a filter. To get

$\Theta(d^2)$ terms, we must generate a filter with the series in (4.13). Let $\mathcal{S}_m = \{n \in \mathbb{N}^m : n \prec 2e_1\}$. We recursively define a function $\pi_m : \mathcal{S}_m \to 2^G$. Let $\pi_2 : \mathcal{S}_2 \to 2^G$ where

$$\pi_2(n,i) = \begin{cases} \gamma_1 & \text{if } (n,i) \preceq (1,0), \\ H_1 & \text{if } (n,i) = (1,1), \\ \gamma_2 & \text{otherwise.} \end{cases}$$

Thus, for $k \geq 3$, let $\pi_k : \mathcal{S}_k \to 2^G$ where

$$\pi_k(n,i) = \begin{cases} \pi_{k-1}(n) & \text{if } (n,i) \preceq (e_1,0), \\ H_{k-1} & \text{if } (n,i) = (e_1,1), \\ H_{k-2} & \text{otherwise.} \end{cases}$$

To be consistent with the established notation, let $\pi_m = \pi$.

Because of the lexicographic ordering, it is possible to have an infinite number of indices correspond to the same image under α. That is, for $n \in \mathbb{N}^m$, the cardinality of $\{n' \in \mathbb{N}^m : \alpha_{n'} = \alpha_n\}$ need not be finite. It is even possible for the previous set to include elements with different n_1 values. Thus when referring to a term in the α-series, we use the smallest (lex) index $(n_1, ..., n_m)$, where n_1 is as large as possible. In the case of the last term in the series, we let n_1 equal one plus the class of U.

To get the lower terms, we must generate them via (2.6), so for all $n \in \mathbb{N}^m$,

$$\alpha_n = \alpha_n^{(m)} = \bar{\pi}_n = \prod_{\mathbf{t} \in \mathcal{G}_0^n} [\pi_{\mathbf{t}}].$$

Note that the terms of the commutator subgroups are equal to either U, H_i, or γ_2. The following lemma states that we don't need to run through all $\mathbf{t} \in \mathcal{G}_0^n$.

Lemma 4.14. *Let $k \geq 2$ and $n = (n_1, ..., n_k)$ where $n_i \in \mathbb{N}$. Then*

$$\alpha_n^{(k)} = \prod_{\mathbf{t}} [\pi_{\mathbf{t}}] \gamma_{n_1+1},$$

where the product runs through all paths, $\mathbf{t}$, of length n_1 from $\mathcal{G}_0^n$.

Proof. Recall that $\mathcal{S}_k = \{n \in \mathbb{N}^k : n \prec 2e_1\}$. Therefore,

$$\alpha_n^{(k)} \geq [\pi_{e_1}, ..., \pi_{e_1}, \pi_{(0,n_2,...,n_k)}] = \gamma_{n_1+1} = \gamma_{n_1+1},$$

so every path of length at least $n_1 + 1$ from $\mathcal{G}_0^n$ is already contained in $\alpha_n^{(k)}$. Since $(n_1, 0, ..., 0) \preceq n$, it follows that $\gamma_{n_1} \geq \alpha_n^{(k)}$, so the statement follows. □

From Lemma 4.14, it follows that, for a fixed $n \in \mathbb{N}^m$, the entries and their multiplicities (the number of occurrences) of the commutator $[\pi_{\mathbf{t}}]$ are completely determined. Indeed, for $n = (n_1, ..., n_m)$ and for all commutators n_1 entries, the entry H_i must have multiplicity n_{i+1}. Because $\mathbb{N}^k$ is a commutative monoid, we get every possible order of terms in the commutator.

In the following theorem, we examine the multiset of entries from $[\pi_{\mathbf{t}}]$. These multisets are partially ordered under component inclusion. That is, for multisets $\mathcal{A}$ and $\mathcal{B}$, where $|\mathcal{A}| = |\mathcal{B}| = e$, if there exist sequences $\{A_i\}_{i=1}^e$ and $\{B_i\}_{i=1}^e$ with $A_i \leq B_i$ for each i and $\mathcal{A} = \bigcup_{i=1}^e A_i$ and $\mathcal{B} = \bigcup_{i=1}^e B_i$, then $\mathcal{A} \leq \mathcal{B}$.

Let $U \leq A_d(p)$ be a maximal unipotent subgroup. For fixed $r \in \Phi^+$, let α_n be the smallest subgroup of the adjoint series of U such that $X_r \leq \alpha_n$. Let $\mathcal{M}_r$ be the collection of the multisets $\mathcal{A}$ of entries from $[\pi_{\mathbf{t}}]$, where $X_r \leq [\pi_{\mathbf{t}}]$ and $|\mathcal{A}| = n_1$.

Then $\mathcal{M}_r$ has a minimal element. Indeed, if $r = p_i + \cdots + p_j$, using symmetry, we may assume $i \leq m$, then the minimal element is

$$\mathcal{B} = \begin{cases} \{H_i, ..., H_{m-1}, U, U, H_{m-1}, ..., H_{d-j+1}\} & \text{if } d \text{ is even and } i \leq m < j, \\ \{H_i, ..., H_{m-1}, U, H_{m-1}, ..., H_{d-j+1}\} & \text{if } d \text{ is odd and } i \leq m < j, \\ \{H_i, ..., H_j\} & \text{if } i < j < m. \end{cases}$$

If α_n is the smallest term of the adjoint series containing X_r and $\mathcal{B}$ is the smallest multiset of $\mathcal{M}_r$, then

$$\alpha_n = \prod_{\{b_1,...,b_{n_1}\}=\mathcal{B}} [b_1, ..., b_{n_1}].$$

This observation is critical to the proof of Theorem 1.1.

4.1. **Proof of Theorem 1.1.**

Proof of Theorem 1.1. Let $r \in \Phi^+$ and write $r = p_i + \cdots + p_j$. Using the notation above, the smallest multiset $\mathcal{B}$ of $\mathcal{M}_r$ is given by the equation above. Observe that if $r' = p_{d-j+1} + \cdots + p_{d-i+1}$ then $\mathcal{B}$ is the smallest multiset in $\mathcal{M}_{r'}$. Therefore, if α_n is the smallest term of the adjoint series containing X_r, then α_n is the smallest term in the adjoint series containing $X_{r'}$.

We show that if $s \in \Phi^+$, where $s \neq r$ and $s \neq r'$, and if $\alpha_{n'}$ is the smallest term in the adjoint series containing X_s, then $\alpha_n \neq \alpha_{n'}$. If $\mathcal{B}_r$ and $\mathcal{B}_s$ are the smallest multisets contained in $\mathcal{M}_r$ and $\mathcal{M}_s$ respectively, then by the above equation for $\mathcal{B}$, we have that $\mathcal{B}_r \neq \mathcal{B}_s$. Therefore, $\alpha_n \neq \alpha_{n'}$. Hence, the orders of the factors of the adjoint series of U are either p (if $r = r'$) or p^2. □

Corollary 4.15. *The adjoint series of $U \leq A_d(p)$ has $\Theta(d^2)$ factors.*

Proof. Each factor has order p or p^2 and $\log_p |U| = \binom{d+1}{2}$. □

Remark 4.16. There are similar statements like that of Theorem 1.1 for the other classical types. In fact, for types B and C, the factor orders are either p or p^2, with an exception in the middle of the series, where one term has order roughly $p^{d/2}$. Furthermore, for type D, the factor orders are either p, p^2, or p^3; again with an exception in the middle of the series where one term has order roughly $p^{d/2}$.

4.2. **Proof of Theorem 1.2.**

Proof of Theorem 1.2. The proof of Theorem 1.1 applies to all roots r with $h(r) \leq d$ and whose summands are unique. Every root system Φ with $|\Pi| = d$, contains roots of the form $r = p_i + \cdots + p_{i+h-1}$ where $1 \leq i$ and $i + h - 1 \leq d$. Thus, the length of the adjoint series for $\mathfrak{g}(p)$ is at least as long as the length of the adjoint series for $A_d(p)$. □

Remark 4.17. When $p = 2$, some modest changes can be made to the previous lemmas and theorems, aside from the change from alternating to symmetric bilinear maps. While the structure constants of the bilinear map, $\circ : U/U' \times U/U' \to U'/\gamma_3(U)$, are different in characteristic two for types B and C [4, p. 848], the Jacobson radical of Adj $(\circ)$ is similar to that of type D. Thus, we obtain factors of order p^3 in this case.

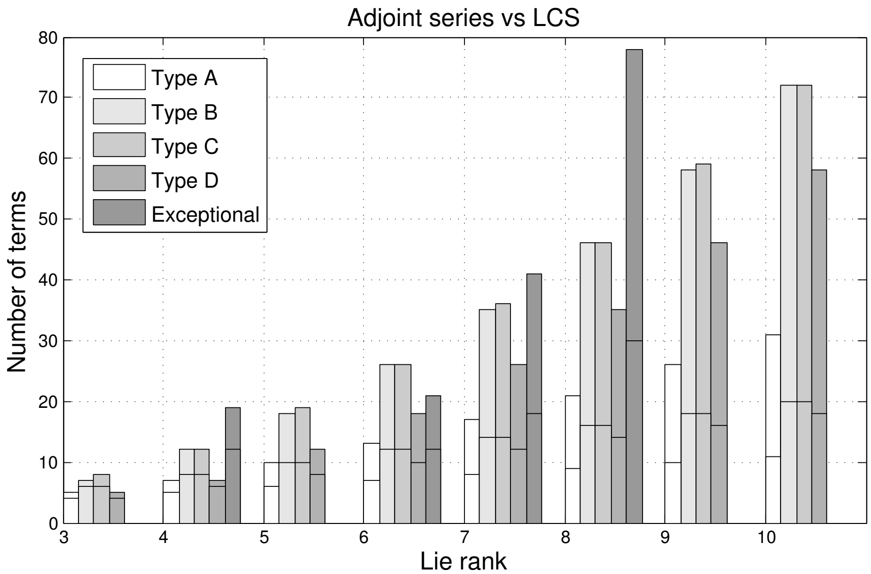

Figure 3. A comparison between the lower central series (lower bar) and the adjoint series (upper bar) for small Lie rank.

Remark 4.18. To generalize these results to field extensions of $\mathbb{Z}_p$, we use centroids to find the appropriate field extension without requiring it as input. As introduced by Wilson in [8], the *centroid* of a bilinear map $\circ : V \times V \to W$ is defined to be

$$\mathrm{Cent}(\circ) = \{(f, h) \in \mathrm{End}\,(V) \times \mathrm{End}\,(W) : \forall u, v \in V, uf \circ v = u \circ fv = (u \circ v)h\}.$$

If $U \leq \mathfrak{g}(K)$, then structure constants of $M_{\mathfrak{g}}$ are similar to that of Lemma 4.7. Instead of 1×1 blocks along the upper and lower diagonal, we get $e \times e$ blocks where the field has size p^e, and a calculation shows that $\mathrm{Cent}(M_{\mathfrak{g}}) \cong K$. In this case, the sizes of nearly every factor of the adjoint series is $|K|$-bounded.

The statement of the main theorem is not explicit about the length of the adjoint series. In particular, it is unknown if the adjoint series is significantly longer than the lower central series for small rank. However, we see in Figure 3 that the length of the lower central series is much smaller than the adjoint series, even for small ranks. Included in that figure are the lengths of the adjoint series for the exceptional types (F and E) for $p \geq 3$. The adjoint ring of the bilinear map for $G_2(p)$ has a trivial Jacobson radical for all $p \geq 5$, and hence, has no nontrivial adjoint refinement. These computations were run in Magma [1].

Acknowledgments

The author is indebted to J. B. Wilson for suggesting and advising this project, A. Hulpke for helpful discussions and coding advice, and the referee for insightful comments which improved the clarity of the paper.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

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

[3] Bettina Eick, C. R. Leedham-Green, and E. A. O'Brien. Constructing automorphism groups of p-groups. *Comm. Algebra*, 30(5):2271–2295, 2002.

[4] M. A. Gazdanova and Ya. N. Nuzhin. On the strong reality of unipotent subgroups of Lie-type groups over a field of characteristic 2. *Sibirsk. Mat. Zh.*, 47(5):1031–1051, 2006.

[5] Michel Lazard. Sur les groupes nilpotents et les anneaux de Lie. *Ann. Sci. Ecole Norm. Sup. (3)*, 71:101–190, 1954.

[6] Edward L. Spitznagel, Jr. Terminality of the maximal unipotent subgroups of Chevalley groups. *Math. Z.*, 103:112–116, 1968.

[7] James B. Wilson. Decomposing p-groups via Jordan algebras. *J. Algebra*, 322(8):2642–2679, 2009.

[8] James B. Wilson. Existence, algorithms, and asymptotics of direct product decompositions, I. *Groups Complex. Cryptol.*, 4(1):33–72, 2012.

[9] James B. Wilson. Division, adjoints, and dualities of bilinear maps. *Comm. Algebra*, 41:3989–4008, 2013.

[10] James B. Wilson. More characteristic subgroups, lie rings, and isomorphism tests for p-groups. *J. Group Theory*, 16:875–897, 2013.

Department Of Mathematics, Colorado State University, Fort Collins, CO 80523
E-mail address: maglione@math.colostate.edu