AN EXTENSION OF A RESULT BY STEINBERG
TOWARDS A CHEVALLEY BASIS ALGORITHM

DAN ROOZEMOND

Abstract. Let L be the Lie algebra of a simple algebraic group defined over $\mathbb{F}$ and let H be a split Cartan subalgebra of L. Let $R = (X, \Phi, Y, \Phi^\vee)$ be the root datum of L, so that $H = Y \otimes \mathbb{F}$, and let $\langle \cdot, \cdot \rangle : \Phi \times \Phi^\vee \mapsto \mathbb{Z}$ be the corresponding bilinear form. This bilinear form induces a linear form on the roots of L by defining $\overline{\alpha} : h \mapsto \sum_i \langle \alpha, y_i \rangle t_i$, where $h = \sum_i y_i \otimes t_i$. Given a root α, we define the *multiplicity* of α in L to be the number of $\beta \in \Phi$ such that $\overline{\alpha} = \overline{\beta}$.

For R of adjoint type, Steinberg gave an overview of the cases where multiplicities greater than 1 occur. In this paper we give a complete overview of these cases, for R of any isogeny type.

1. Introduction

Throughout this paper we let $R = (X, \Phi, Y, \Phi^\vee)$ be a *root datum* of rank n, so X and Y are dual free $\mathbb{Z}$-modules of dimension n with a bilinear pairing $\langle \cdot, \cdot, \rangle : X \times Y \to \mathbb{Z}$. We fix dual bases $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$ of X and Y, respectively. Furthermore, Φ is a finite subset of X and $\Phi^\vee$ a finite subset of Y, called the *roots* and *coroots*, respectively. There is a one-to-one correspondence $^\vee : \Phi \to \Phi^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$ for all $\alpha \in \Phi$. See [4] for more details.

Given a root datum R we consider the free $\mathbb{Z}$-module

$$L_{\mathbb{Z}} = Y \oplus \bigoplus_{\alpha \in \Phi} \mathbb{Z} X_\alpha,$$

where the X_α are formal basis elements. Thus $L_{\mathbb{Z}}$ has rank $n + |\Phi|$.

We define a bilinear map $[\cdot, \cdot] : L_{\mathbb{Z}} \times L_{\mathbb{Z}} \to L_{\mathbb{Z}}$ determined by the following rules, where $N_{\alpha,\beta}$ are integral structure constants:

$$\begin{array}{lrcll}
\text{For } y, z \in Y: & [y, z] & = & 0, & \text{(CB1)} \\
\text{For } y \in Y, \beta \in \Phi: & [y, X_\beta] & = & \langle \beta, y \rangle X_\beta, & \text{(CB2)} \\
\text{For } \alpha, \beta \in \Phi: & [X_\alpha, X_\beta] & = & \begin{cases} N_{\alpha,\beta} X_{\alpha+\beta} & \text{if } \alpha + \beta \in \Phi, \\ \alpha^\vee & \text{if } \beta = -\alpha, \\ 0 & \text{otherwise.} \end{cases} & \text{(CB3)}
\end{array}$$

If the $N_{\alpha,\beta}$ are such that $[\cdot, \cdot]$ satisfies the Jacobi identity, then $L_{\mathbb{Z}}$ is called a *Chevalley Lie algebra*. A basis of $L_{\mathbb{Z}}$ consisting of a basis of Y and the formal elements X_α is called a *Chevalley basis* of $L_{\mathbb{Z}}$.

It is a well known result (see for example [2]) that the $N_{\alpha,\beta}$ may be chosen to be $\pm(p+1)$, where p is the biggest number such that $\alpha - p\beta$ is a root.

If $\mathbb{F}$ is a field, tensoring $L_{\mathbb{Z}}$ with $\mathbb{F}$ yields a Lie algebra $L_{\mathbb{F}}$ over $\mathbb{F}$. Suppose for the remainder of this section that $\mathbb{F}$ is a field of characteristic p.

Let $H = Y \otimes F$, fix a basis $\{y_1, \ldots, y_n\}$ of Y, and set $h_i = y_i \otimes 1$, $i = 1, \ldots, n$. For $\alpha \in \Phi$, the *root of H on $L_{\mathbb{F}}$* is the function

$$\overline{\alpha} : h \mapsto \sum_{i=1}^{l} \langle \alpha, y_i \rangle t_i, \quad \text{where } h = \sum_{i=1}^{l} y_i \otimes t_i,$$

and $\langle \alpha, y_i \rangle$ is interpreted in $\mathbb{Z}$ (if $p = 0$) or $\mathbb{Z}/p\mathbb{Z}$ (if $p \neq 0$). Note that this implies that $\langle \alpha, h \rangle := \overline{\alpha}(h)$ for $h \in H$ is completely determined by the values $\langle \alpha, y_i \rangle$, $i = 1, \ldots, n$.

Given a root α, we define the *multiplicity* of α in $L_{\mathbb{F}}$ to be the number of $\beta \in \Phi$ such that $\overline{\alpha} = \overline{\beta}$. If each root has multiplicity 1 it is easy to identify the root spaces, given $L_{\mathbb{F}}$ and H.

In the remainder of this paper we prove the following proposition, a generalization of a well known result by Steinberg [8].

Proposition 1. *Let $L_{\mathbb{F}}$ be a Lie algebra of a simple algebraic group over a field $\mathbb{F}$ of characteristic p and let H be a split Cartan subalgebra of $L_{\mathbb{F}}$. Then the multiplicities of the roots of H on $L_{\mathbb{F}}$ are either all 1 or indicated in Table 3.*

In Section 2 we clarify the concept of root data by means of the easiest non-trivial example: The root datum of type A_1. In Section 3 we give an overview of the motivation for this work: developing an algorithm to find a Chevalley bases for a given Lie algebra, and we indicate the difficulties that arise over fields of small characteristic. In Section 4 we study one of these difficulties, roots with a multiplicity greater than 1, in detail, giving a proof of Proposition 1. Finally, in Section 5 we briefly comment on the other difficulties and give an overview of the current and future research with regard to this topic.

2. Root data of type A_1

As an introductory example, we consider root data of type A_1. The Cartan matrix C of these root data is the 1×1 matrix (2). There exist integral 1×1 matrices A, B such that $C = A^T B$. Note that, for a given root datum R with Cartan matrix C, the vectors $(\langle \alpha, y_1 \rangle, \ldots, \langle \alpha, y_n \rangle)$ are precisely the rows of the matrix of roots A satisfying $C = A^T B$ (B is the matrix of coroots). Two canonical choices for A and B are $A = (1)$, $B = (2)$ (called *adjoint* type) and $A = (2)$, $B = (1)$ (called *simply connected* type).

First, consider the root datum R^{ad} of type A1 of adjoint type. In this case, $X = Y = \mathbb{Z}$, $\Phi = \{\alpha = 1, -\alpha = -1\}$, $\Phi^\vee = \{\alpha^\vee = 2, -\alpha^\vee = -2\}$. This implies that the pairing $\langle \cdot, \cdot \rangle$ between X and Y takes values $\langle e_1, \alpha^\vee \rangle = 2$, $\langle \alpha, f_1 \rangle = 1$, and $\langle \alpha, \alpha^\vee \rangle = 2$. As the rank of R^{ad} is 1 and the number of roots is 2, its Lie algebra ${L_{\mathbb{Z}}}^{\mathrm{ad}}$ has dimension 3. Fixing a basis $\{h\}$ of Y gives the multiplication table of ${L_{\mathbb{Z}}}^{\mathrm{ad}}$ shown in Table 1.

Next, consider the root datum R^{sc} of type A1 of simply connected type. X and Y are the same as in the previous case, but now $\Phi = \{\alpha = 2, -\alpha = -2\}$ and $\Phi^\vee = \{\alpha^\vee = 1, -\alpha^\vee = -1\}$. The pairing $\langle \cdot, \cdot \rangle$ between X and Y also takes different values: $\langle e_1, \alpha^\vee \rangle = 1$, $\langle \alpha, f_1 \rangle = 2$, and $\langle \alpha, \alpha^\vee \rangle = 2$. Fixing a basis $\{h\}$ of Y now gives the multiplication table of ${L_{\mathbb{Z}}}^{\mathrm{sc}}$ in Table 2.

Now let $\mathbb{F}$ be any field. Tensoring ${L_{\mathbb{Z}}}^{\mathrm{ad}}$ and ${L_{\mathbb{Z}}}^{\mathrm{sc}}$ with $\mathbb{F}$ gives Lie algebras ${L_{\mathbb{F}}}^{\mathrm{ad}}$ and ${L_{\mathbb{F}}}^{\mathrm{sc}}$ over $\mathbb{F}$, respectively.

	X_α	$X_{-\alpha}$	h
X_α	0	$-2h$	X_α
$X_{-\alpha}$	$2h$	0	$-X_{-\alpha}$
h	$-X_\alpha$	$X_{-\alpha}$	0

Table 1. $A_1{}^{\mathrm{ad}}$

	X_α	$X_{-\alpha}$	h
X_α	0	$-h$	$2X_\alpha$
$X_{-\alpha}$	h	0	$-2X_{-\alpha}$
h	$-2X_\alpha$	$2X_{-\alpha}$	0

Table 2. $A_1{}^{\mathrm{sc}}$

If the characteristic of $\mathbb{F}$ is not 2, we may define $\phi : L_{\mathbb{F}}{}^{\mathrm{ad}} \to L_{\mathbb{F}}{}^{\mathrm{sc}}$ by $X_\alpha \mapsto X_\alpha$, $X_{-\alpha} \mapsto X_{-\alpha}$, and $h \mapsto \frac{1}{2}h$. It is easy to verify that ϕ is an automorphism of Lie algebras, and therefore $L_{\mathbb{F}}{}^{\mathrm{ad}}$ and $L_{\mathbb{F}}{}^{\mathrm{sc}}$ are isomorphic.

If, on the other hand, the characteristic of $\mathbb{F}$ is 2, we see that $L_{\mathbb{F}}{}^{\mathrm{sc}}$ has a one-dimensional centre, namely h, whereas $L_{\mathbb{F}}{}^{\mathrm{ad}}$ does not. So in this case $L_{\mathbb{F}}{}^{\mathrm{ad}}$ and $L_{\mathbb{F}}{}^{\mathrm{sc}}$ are not isomorphic.

This is just one type of problem that may occur when working with Lie algebras over these small characteristics.

3. Finding Chevalley Bases

The motivation for this work is the wish to construct a Chevalley basis for a Lie algebra $L_{\mathbb{F}}$, given only a splitting Cartan subalgebra H. Las Vegas algorithms to find such an H have been constructed by Cohen and Murray [3] and Ryba [6]. The first has been implemented in the Magma computer algebra system [1]. For now, we assume that we are also given the appropriate root datum R, although in the future we expect to be able to reconstruct this given only $L_{\mathbb{F}}$ and H. The output of such an algorithm is a basis $\{X_\alpha, h_i \mid \alpha \in \Phi, i \in \{1, \ldots, n\}\}$ of $L_{\mathbb{F}}$ satisfying (CB1)–(CB3).

For sufficiently large fields, in particular those of characteristic not $2, 3$, such an algorithm has been implemented in several computer algebra systems, for example Magma and GAP [7]. For details, see for example [5].

If, however, we consider Lie algebras of simple algebraic groups over a field $\mathbb{F}$ of characteristic 2 or 3, the current algorithms presented break down in several places.

Firstly, the eigenspaces of the Cartan subalgebra H acting on $L_{\mathbb{F}}$ are no longer necessarily one dimensional. This means that we will have to take extra measures in order to identify which vectors in these eigenspaces are root elements. Secondly, we can no longer always use root chains to compute Cartan integers, which are the most important piece of information for the root identification algorithm in the general case. Thirdly, when computing the Chevalley basis elements for non-simple roots, we cannot always simply obtain $X_{\alpha+\beta}$ by $X_{\alpha+\beta} = \frac{1}{N_{\alpha,\beta}}[X_\alpha, X_\beta]$ as $N_{\alpha,\beta}$ may be a multiple of $\mathrm{char}(\mathbb{F})$.

The first of these problems is the subject of the remainder of this paper.

4. Multidimensional eigenspaces

We investigated various root data with respect to the root multiplicities. This led to a generalization of [8], summarized in Table 3.

The meaning of the isogeny types marked * is as follows. A root datum of type A_3 has three possible isogeny types: adjoint, simply connected, and one intermediate one. The latter is induced by a (any) generator a of its fundamental group $\mathbb{Z}/4$, and

Char.	Root datum	Eigenspace dims
3	$\mathrm{A}_2{}^{\mathrm{sc}}$	3^2
3	G_2	$1^6, 3^2$
2	$\mathrm{A}_3{}^{\mathrm{sc}}, A_3^{(a)^\star}$	4^3
2	$\mathrm{B}_n{}^{\mathrm{ad}}$ $(n \geq 2)$	$2^n, 4^{(n^2-n)/2}$
2	$\mathrm{B}_2{}^{\mathrm{sc}}$	4^2
2	$\mathrm{B}_3{}^{\mathrm{sc}}$	6^3
2	$\mathrm{B}_4{}^{\mathrm{sc}}$	$2^4, 8^3$
2	$\mathrm{B}_n{}^{\mathrm{sc}}$ $(n \geq 5)$	$2^n, 4^{(n^2-n)/2}$
2	$\mathrm{C}_n{}^{\mathrm{ad}}$ $(n \geq 3)$	$2n^1, 2^{n^2-n}$
2	$\mathrm{C}_n{}^{\mathrm{sc}}$ $(n \geq 3)$	$2n^1, 4^{(n^2-n)/2}$
2	$\mathrm{D}_4^{(a),(b),(a+b)^\star}$	4^6
2	$\mathrm{D}_4{}^{\mathrm{sc}}$	8^3
2	$\mathrm{D}_n^{(a)^\star}, \mathrm{D}_n{}^{\mathrm{sc}}$ $(n \geq 5)$	$4^{\binom{n}{2}}$
2	F_4	$2^{12}, 8^3$
2	G_2	4^3
2	all remaining cases	$2^N (N = \lvert\Phi^+\rvert)$

TABLE 3. Multidimensional eigenspaces

therefore referred to by $\mathrm{A}_3^{(a)}$. A root datum of type D_n has fundamental group of type $(\mathbb{Z}/4\mathbb{Z})$ if n is odd, and of type $(\mathbb{Z}/2\mathbb{Z})^2$ if n is even. The unique intermediate type in the odd case is denoted by $\mathrm{D}_n^{(a)}$, and the three possible intermediate types in the even case by $\mathrm{D}_n^{(a)}$, $\mathrm{D}_n^{(b)}$, and $\mathrm{D}_n^{(a+b)}$.

Proof of Proposition 1. We will write $\equiv$ for equality mod p. We write $(X, \Phi, Y, \Phi^\vee)$ for the root datum underlying $(L_{\mathbb{F}}, H)$. This means that $L_{\mathbb{F}}$ has a basis as in (CB1)–(CB3), with $H = Y \otimes_{\mathbb{Z}} \mathbb{F}$.

We prove the proposition for each of the four classical series and the five exceptional cases separately. Furthermore, we distinguish the different isogeny types. Notice that, for a fixed type and two root data R_1, R_2 of that type, when $\mathbb{Z}\Phi_1 \subseteq \mathbb{Z}\Phi_2$, the multiplicities for $L_{\mathbb{F}}(R_1)$ will be at least those of $L_{\mathbb{F}}(R_2)$. This implies that considering root data of the adjoint and simply connected isogeny types often suffices to understand the intermediate cases.

Our strategy will be to write $\overline{\alpha}$ as an integral linear combination of $\overline{\alpha_i}$. This can be read off from $C = AB^T$, since C is the Cartan matrix, the rows of A are the fundamental roots, and the rows of B are the fundamental coroots. Moreover, if we use the standard basis for X and Y, the pairing $\langle \cdot, \cdot \rangle$ is the standard scalar product.

In each of the cases, we try to find roots $\alpha \neq \beta$ such that $\overline{\alpha} = \overline{\beta}$. By transitivity of the Weyl group on Φ, it suffices to consider only $\alpha = \alpha_1$ in the cases where all roots have the same length $(\mathrm{A}_n, \mathrm{D}_n, \mathrm{E}_{6,7,8})$ and $\alpha = \alpha_1$ or α_n if there are multiple root lengths $(\mathrm{B}_n, \mathrm{C}_n, \mathrm{F}_4, \mathrm{G}_2)$.

In the adjoint cases, the fundamental roots $\alpha_1, \ldots, \alpha_n$ may be taken to be the standard basis vectors $e_1, \ldots, e_n$, since then the root and coroot matrix may be taken to be I and C^T, respectively. In the simply connected cases, the fundamental roots $\alpha_1, \ldots, \alpha_n$ may be taken to be the rows of the Cartan matrix C, since then the root and coroot matrix may be taken to be C and I, respectively. Suppose furthermore that β is expressed in the fundamental roots, i.e. $\beta = \sum_{i=1}^n c_i \alpha_i$ with either all $c_i \in \mathbb{N}$ or all $c_i \in -\mathbb{N}$.

In the current paper, we give the proofs of the cases where R is of type A_n, B_n or G_2. The other cases are proved in a very similar way.

$\mathbf{A_n(n \geq 1)}$. The root datum of type A_n has Cartan matrix

$$C = \begin{pmatrix} 2 & -1 & 0 & \dots & 0 \\ -1 & 2 & -1 & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & \dots & -1 & 2 & -1 \\ 0 & \dots & 0 & -1 & 2 \end{pmatrix},$$

and the roots are

$$\pm(\alpha_j + \cdots + \alpha_l), \quad j \in \{1, \dots, n\}, l \in \{j, \dots, n\},$$

where $\{\alpha_1, \dots, \alpha_n\}$ are the simple roots, thus giving a total of $2 \cdot \frac{1}{2}n(n+1)$ roots.

For the adjoint case, suppose $\overline{\alpha_1} = \overline{\beta}$. Since $A = I$, we must have $c_1 \equiv 1$ and $c_j \equiv 0$ $(j = 2, \dots, n)$, which implies either $p \neq 2$, $c_1 = 1$, and $c_2 = \cdots = c_n = 0$, or $p = 2$, $c_1 = \pm 1$, and $c_2 = \cdots = c_n = 0$. This gives $\beta = -\alpha_1$, so $\frac{n^2+n}{2}$ eigenspaces of dimension 2.

In the simply connected case the fundamental roots are equal to the rows of C, so that $\overline{\alpha_1} = \overline{\beta}$ implies $2c_1 - c_2 \equiv 2$, $-c_1 + 2c_2 - c_3 \equiv -1$, $-c_{j-2} + 2c_{j-1} - c_j \equiv 0$ for $j = 4, \dots, n$, and $-c_{n-1} - c_n \equiv 0$.

If $c_1 = 1$, then $c_2 \equiv 0$, so $c_2 = 0$. Because $c_1\alpha_1 + \cdots + c_n\alpha_n$ must be a root, this implies $c_3 = \cdots = c_n = 0$, so this only gives $\overline{\beta} = \overline{\alpha_1}$.

If $c_1 = 0$, then $-c_2 \equiv 2$, so that either $p = 2$ and $c_2 = 0$, or $p = 3$ and $c_2 = 1$. In the first case, we find $c_3 \equiv 1$, giving a contradiction if $n \geq 5$ (because then $c_4 \equiv 0$ and $c_5 \equiv 1$), a contradiction if $n = 4$ (because then the last relation becomes $0 = -c_3 + 2c_4$, which is not satisfied), and the special case $n = 3, p = 2$ discussed below. In the second case, where $p = 3$ and $c_2 = 1$, we get $-1 \equiv 2 - c_3$, so that $c_3 \equiv 0$, giving a contradiction if $n \geq 4$ (because then $c_4 \equiv 1$), a contradiction if $n = 3$ (because then the last relation becomes $0 = -c_2 + 2c_3$, which is not satisfied), and the special case $n = 2, p = 3$ discussed below.

If $c_1 = -1$, then $-c_2 \equiv 4$, so that either $p = 2$ and $c_2 = 0$, or $p = 3$ and $c_2 = -1$. In the first case, we find $c_3 = \cdots = c_n = 0$, so this gives $\beta = -\alpha_1$. In the second case, we find that either $n = 2$ (the special case below), or $c_3 = 0$, which leads to a contradiction if $n \geq 4$ (because then $c_3 = 0$ but $c_4 \neq 0$), and also if $n = 3$ (because then the last equation becomes $0 = -c_2 + 2c_3$).

For $n = 3$ and $p = 2$ we have

$$A = C = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

thus giving $\overline{\alpha_1} = \overline{\alpha_3}$, and also $\overline{\alpha_1 + \alpha_2} = \overline{\alpha_2 + \alpha_3}$ and $\overline{\alpha_2} = \overline{\alpha_1 + \alpha_2 + \alpha_3}$, accounting for not 6 eigenspaces of dimension 2 (as expected for $p = 2$) but rather 3 eigenspaces of dimension 4.

For $n = 2$ and $p = 3$ we have

$$A = C = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$$

which means $\overline{\alpha_1} = \overline{\alpha_2}$, implying also $\overline{\alpha_1} = \overline{-(\alpha_1 + \alpha_2)}$. Similarly, $\overline{-\alpha_1} = \overline{-\alpha_2} = \overline{\alpha_1 + \alpha_2}$ thus giving 2 eigenspaces of dimension 3.

$\mathbf{B_n(n \geq 2)}$. The root datum of type B_n has Cartan matrix

$$C = \begin{pmatrix} 2 & -1 & 0 & \dots & 0 \\ -1 & 2 & -1 & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & \dots & -1 & 2 & -2 \\ 0 & \dots & 0 & -1 & 2 \end{pmatrix},$$

and the roots are

(a) $\pm(\alpha_j + \cdots + \alpha_l)$, $j \in \{1, \dots, n\}, l \in \{j, \dots, n\}$,
(b) $\pm(\alpha_j + \cdots + \alpha_{l-1} + 2\alpha_l + \cdots + 2\alpha_n)$, $j \in \{1, \dots, n-1\}, l \in \{j+1, \dots, n\}$,

giving a total of $2 \cdot \frac{1}{2}n(n+1) + 2 \cdot \frac{1}{2}n(n-1) = 2n^2$ roots.

In the adjoint case, for the long roots, suppose $\overline{\alpha_1} = \overline{\beta}$, so $c_1 \equiv 1$ and $c_2 \equiv \cdots \equiv c_n \equiv 0$. If $c_1 = 1$, then either $c_2 = 0$, which gives $\beta = \alpha_1$, or $c_2 \neq 0$, which implies $p = 2$ and $\beta = \alpha_1 + 2\alpha_2 + \cdots 2\alpha_n$. If $c_1 = -1$, then $p = 2$, and either $c_2 = 0$, which gives $\beta = -\alpha_1$, or $c_2 \neq 0$, which implies $\beta = -\alpha_1 - 2\alpha_2 - \cdots - 2\alpha_n$. This shows that the long roots are all in 4-dimensional eigenspaces.

In the adjoint case, for the short roots, suppose $\overline{\alpha_n} = \overline{\beta}$, so $c_n \equiv 1$ and $c_1 \equiv \cdots \equiv c_{n-1} \equiv 0$. This yields three possibilities for c_n: If $c_n = -2$, then $p = 3$, implying c_{n-1} is either 0 or -3, neither of which give rise to roots. If $c_n = -1$, then $p = 2$. Either $c_{n-1} = 0$ (yielding $\beta = -\alpha_n$), or $c_{n-1} = -2$ (not giving any roots). If $c_n = 1$ we must have $c_{n-1} = \cdots = c_1 = 0$, giving $\beta = \alpha_n$. This shows that the short roots are all in 2-dimensional eigenspaces.

In the simply connected case we have $A = C$. We consider the cases $n = 2, 3, 4$ separately below.

For the long roots, suppose $n \geq 5$ and $\alpha_1 = \beta$, so $2c_1 - c_2 \equiv 2$, $-c_1 + 2c_2 - c_3 \equiv -1$, $-c_{j-2} + 2c_{j-1} - c_j \equiv 0$ $(j = 4, \dots, n)$, and $-2c_{n-1} + 2c_n \equiv 0$.

If $c_1 = 0$, then $-c_2 \equiv 2$, so that $p = 3$ and $c_2 = 1$, or $p = 2$ and $c_2 = 0$. In the first case, we find $2 - c_3 \equiv -1$, which means $c_3 = 0$. But then $c_4 = 0$ by the fact that we are working in a root system, contradicting $0 = -c_2 + 2c_3 - c_4$. In the second case, the subsequent equations give $c_3 = c_4 = \cdots = c_n = 0$, which does not give a root.

If $c_1 = 1$, then $c_2 \equiv 0$. If $c_2 = 0$, we find $\beta = -\alpha_1$. If $c_2 \neq 0$ then $p = 2$ and $c_2 = 2$, which gives $\beta = \alpha_1 + 2\alpha_2 + \cdots + 2\alpha_n$. If $c_1 = -1$, then $4 \equiv -c_2$ so $p = 2$ and $c_2 \equiv 0$. If $c_2 = 0$, we find $\beta = -\alpha_1$, if $c_2 = -2$ then we find $\beta = -\alpha_1 - 2\alpha_2 - \cdots - 2\alpha_n$. This shows that, for $n \geq 5$, the long roots are all in 4-dimensional eigenspaces.

For the short roots, suppose $n \geq 5$ and $\overline{\alpha_n} = \overline{\beta}$, yielding $2c_1 - c_2 \equiv 0$, $-c_{j_2} + 2c_{j-1} - c_j \equiv 0$ $(j = 4, \dots, n-1)$, $-c_{n-2} + 2c_{n-1} - c_n \equiv -1$, and $-c_{n-2} + 2c_n \equiv 2$. First, suppose $p = 2$ and $c_n \equiv 0$. Then $c_{n-1} \equiv 0$, so that $c_{n-2} \equiv 1$ by $1 \equiv -c_{n-2} + 2c_{n-1} - c_n$, $c_{n-3} \equiv 0$ by $0 \equiv -c_{n-3} + 2c_{n-2} - c_{n-1}$, and $c_{n-4} \equiv 1$ by $0 = -c_{n-4} + 2c_{n-3} + c_{n-2}$. But this is never a root.

If $c_n = -2$ and $p \neq 2$, we have $c_{n-1} \equiv -6$, while $c_{n-1} \in \{-1, -2\}$. Since $p \neq 2$ we must have $c_{n-1} = -1$ and $p = 5$, giving $c_{n-2} = 1$, which cannot be. If $c_n = -1$ then $c_{n-1} \equiv -4$, so $p = 2$. Since $c_{n-2} = -2$ never yields a root, we must have $c_{n-2} = 0$, giving $\beta = -\alpha_n$. If $c_n = 0$ and $p \neq 2$ then $-c_{n-1} = 2$, so $c_{n-1} = 1$ and $p = 3$. This implies $c_{n-2} \equiv 0$, implying $c_{n-2} = c_{n-3} = 0$, which contradicts $-c_{n-3} + 2c_{n-2} - c_{n-1} \equiv 0$. If $c_n = 1$ then $c_{n-1} \equiv 0$, so $c_{n-1} = \cdots = c_1 = 0$, only

giving $\beta = \alpha_n$. If $c_n = 2$ and $p \neq 2$ we find $c_{n-1} \equiv 2$, so that $c_{n-1} = 2$. This implies $c_{n-2} \equiv 3$, which means $p = 3$ and $c_{n-2} = 0$ since $p \neq 2$. But this never gives a root. This accounts for n eigenspaces of dimension 2 containing the long roots, provided $n \geq 5$.

If $n = 2$

$$C = \begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}.$$

Now suppose $\overline{\alpha_1} = \overline{\beta}$, hence $2c_1 - c_2 \equiv 2$ and $-2c_1 + 2c_2 \equiv -2$. Adding the two equations yields $c_2 \equiv 0$. Since $c_2 \in \{-2, -1, 0, 1, 2\}$ we must have either $c_2 = 0$ (hence $\beta = \alpha_1$ or $p = 2$ and $\beta = -\alpha_1$), or $c_2 = \pm 2$, hence $p = 2$ and $c_1 = \pm 1$, giving $\beta = \pm\alpha_1$ or $\beta = \pm(\alpha_1 + 2\alpha_2)$.

Next, suppose $\overline{\alpha_2} = \overline{\beta}$, hence $2c_1 - c_2 \equiv -1$ and $-2c_1 + 2c_2 \equiv 2$. This implies $c_2 \equiv 1$, so either $c_2 = -2$ and $p = 3$ (which means $c_1 = -1$, contradicting the first equation), or $p = 2$ (which gives $\beta = \pm\alpha_2$ or $\beta = \pm(\alpha_1 + \alpha_2)$.

This shows that simply connected B_2 has 2 eigenspaces of dimension 4 if $p = 2$, and no multidimensional eigenspaces in other characteristics.

If $n = 3$

$$C = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -2 \\ 0 & -1 & 2 \end{pmatrix}.$$

If $p = 2$, we have $\overline{\alpha_1} = \overline{\alpha_3} = \overline{\alpha_1 + 2\alpha_2 + 2\alpha_3}$, and also $\overline{\alpha_2} = \overline{\alpha_1 + \alpha_2 + \alpha_3} = \overline{\alpha_2 + 2\alpha_3}$ and $\overline{\alpha_1 + \alpha_2} = \overline{\alpha_2 + \alpha_3} = \overline{\alpha_1 + \alpha_2 + 2\alpha_3}$. This gives the 3 eigenspaces of dimension 6 as in Table 3.

So suppose $p \neq 2$ and $\overline{\alpha_1} = \overline{\beta}$, hence $2c_1 - c_2 \equiv 2, -c_1 + 2c_2 - c_3 \equiv -1$, and $-2c_2 + 2c_3 \equiv 0$. If $c_1 = 1$, we have $c_2 \equiv 0$, implying $c_2 = 0$ since $p \neq 2$, which only gives $\beta = \alpha_1$. If $c_1 = 0$, we find $c_2 \equiv -2$, implying $c_2 = 1$ and $p = 3$. But then $c_3 \equiv 0$ by the second equation, contradicting the third. If $c_1 = -1$, we find $4 \equiv -c_2$. Since $p \neq 2$ we must have $c_2 = -1$ and $p = 3$, giving again $c_3 \equiv 0$ by the second equation, a contradictin with the third.

Next, suppose $p \neq 2$ and $\overline{\alpha_3} = \overline{\beta}$, hence $2c_1 - c_2 \equiv 0, -c_1 + 2c_2 - c_3 \equiv -1$, and $-2c_2 + 2c_3 \equiv 2$. If $c_3 = -2$, we have $c_2 \equiv -3$, implying $p = 3$ and $c_2 = 0$, but that can never be a root. If $c_3 = -1$, we have $c_2 \equiv -2$ and $c_1 \equiv -2$, implying $p = 3$ and $c_1 = 1$, but that is never a root. If $c_3 = 0$, we find $c_2 \equiv -1$ and $c_1 \equiv -1$, a contradiction with the first equation. If $c_3 = 1$, we find $c_2 \equiv 0$ and $c_1 \equiv 1$, but that can never be a root. If $c_3 = 2$, we find $c_2 \equiv 1$ and $c_1 \equiv 1$, but that is a contradiction with the first equation.

This shows that simply connected B_3 has 3 eigenspaces of dimension 6 if $p = 2$, and no multidimensional eigenspaces in other characteristics.

If $n = 4$

$$C = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -2 \\ 0 & 0 & -1 & 2 \end{pmatrix}.$$

If $p = 2$ we see $\overline{\alpha_1} = \overline{\alpha_3}$. This gives us $\overline{\alpha_1} = \overline{\alpha_3} = \overline{\alpha_3 + 2\alpha_4} = \overline{\alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4}$, as well as $\overline{\alpha_2} = \overline{\alpha_1 + \alpha_2 + \alpha_3} = \overline{\alpha_1 + \alpha_2 + \alpha_3 + 2\alpha_4} = \overline{\alpha_2 + 2\alpha_3 + 2\alpha_4}$ and $\overline{\alpha_1 + \alpha_2} = \overline{\alpha_2 + \alpha_3} = \overline{\alpha_2 + 2\alpha_3 + 2\alpha_4} = \overline{\alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4}$. The remaining $32 - 24 = 8$

roots $(\pm(\alpha_j + \cdots + \alpha_n), j = 1, \ldots, 4)$ are in 2-dimensional spaces, giving $2^4, 8^3$ as in Table 3.

So suppose $p \neq 2$ and $\overline{\alpha_1} = \overline{\beta}$, hence $2c_1 - c_2 \equiv 2$, $-c_1 + 2c_2 - c_3 \equiv -1$, $-c_2 + 2c_3 - c_4 \equiv 0$, and $-2c_3 + 2c_4 \equiv 0$. If $c_1 = -1$, we have $c_2 \equiv -4$, implying $p = 3$ and $c_2 = -1$, and no solution for c_3 and c_4 exists. If $c_1 = 0$, we have $c_2 \equiv -2$. Then either $c_2 = -2$, giving $c_3 \equiv -3$ which cannot be since $p \neq 2$, or $c_2 = 1$ and $p = 3$, which gives no solutions for c_3 and c_4. If $c_1 = 1$, we have $c_2 \equiv 0$, so $c_2 = c_3 = c_4 = 0$, giving only $\beta = \alpha_1$.

Next, suppose $p \neq 2$ and $\overline{\alpha_4} = \overline{\beta}$, hence $2c_1 - c_2 \equiv 0$, $-c_1 + 2c_2 - c_3 \equiv 0$, $-c_2 + 2c_3 - c_4 \equiv -1$, and $-2c_3 + 2c_4 \equiv 2$. If $c_4 = -2$, we find $c_3 \equiv -3$, hence $p = 3$ and $c_3 = 0$, but that can never be a root. If $c_4 = -1$, we get $c_3 \equiv -2$, which never gives a root. If $c_4 = 0$, we get $c_3 \equiv -1$, $c_2 \equiv -1$, but $c_1 \equiv 1$, which can never give a root. If $c_4 = 1$, we get $c_3 \equiv 0$, so $c_3 = c_2 = c_1 = 0$, but this only gives $\beta = \alpha_4$. If $c_4 = 2$, we get $c - 3 \equiv 1$, $c_2 \equiv 1$ and $2c_1 \equiv 1$. This implies $p = 3$ and $c_1 = -1$, but that is never a root.

$\mathbf{G_2}$. The root datum of type G_2 has Cartan matrix

$$C = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix},$$

and the roots are

$$\pm\alpha_1, \pm\alpha_2, \pm(\alpha_1 + \alpha_2), \pm(2\alpha_1 + \alpha_2), \pm(3\alpha_1 + \alpha_2), \pm(3\alpha_1 + 2\alpha_2),$$

giving a total of 12 roots. As in the previous case, we take $A = I$, since also for G_2 the adjoint and simply connected case are identical. We first consider the cases $p = 2$ and $p = 3$, and then show that these are the only cases where multidimensional eigenspaces occur.

If $p = 3$ we see $\overline{3\alpha_1 + \alpha_2} = \overline{\alpha_2} = \overline{-(3\alpha_1 + 2\alpha_2)}$ and $\overline{-(3\alpha_1 + \alpha_2)} = \overline{-\alpha_2} = \overline{3\alpha_1 + 2\alpha_2}$, and the remaining 6 roots all have distinct eigenspaces.

If $p = 2$ we find $\overline{\alpha_1 + \alpha_2} = \overline{3\alpha_1 + \alpha_2}$, $\overline{\alpha_1} = \overline{3\alpha_1 + 2\alpha_2}$ and $\overline{\alpha_2} = \overline{2\alpha_1 + \alpha_2}$, giving 3 eigenspaces of dimension 4.

Now suppose $\overline{\alpha_1} = \overline{\beta}$, so $c_1 \equiv 1$ and $c_2 \equiv 0$. Observe that $c_1 \notin \{0, 2\}$. If $c_1 \in \{-3, -1, 3\}$, we must have $p = 2$. If $c_1 = -2$, we must have $p = 3$. Finally, if $c_1 = 1$, we either have $c_2 = 0$ (giving only $\beta = \alpha_1$) or $c_2 = 2$, whence $p = 2$.

Finally, suppose $\overline{\alpha_2} = \overline{\beta}$, so $c_1 \equiv 0$ and $c_2 \equiv 1$. Observe that $c_2 \notin \{0, 2\}$. If $c_2 = -2$ we must have $p = 3$, if $c_2 = -1$ we must have $p = 2$, and if $c_2 = 1$ then either $c_1 = 0$ (giving only $\beta = \alpha_1$) or $c_2 = 2$ or $c_2 = 3$, giving $p = 2$ or $p = 3$, respectively). □

5. Conclusion and Future Research

In this paper we have given an overview of some of the problems we may encounter when computing Chevalley bases of Lie algebras over fields of small characteristic. The roots of multiplicity greater than 1, that have been discussed in detail, form the major challange at this point. We have developed algorithms to solve these problems, and we are able to successfully resolve almost all of the cases. Some of these algorithms only require linear algebra, a few use small Gröbner basis computations, and yet others use the MeatAxe to find an ideal of the Lie algebra at hand. Developing new algorithms and optimizating the existing ones is subject to ongoing research.

Solving the other problems mentioned, for example identification of the roots of the underlying root system in the Lie algebra, is also part of ongoing research. We use specific algorithms that depend on the type of the root datum, thus exploiting known structural properties to circumvent the difficulties posed by the small characteristic of the field.

References

[1] W. Bosma and J. J. (Eds) Cannon. *Handbook of Magma Functions, Edition 2.13*. School of Mathematics and Statistics, University of Sydney, 2006. `http://magma.maths.usyd.edu.au/`.

[2] Roger W. Carter. *Simple groups of Lie type*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1972.

[3] Arjeh M. Cohen and Scott H. Murray. Algorithm for lang's theorem. *Journal of Algebra*, to appear, 2006.

[4] Arjeh M. Cohen, Scott H. Murray, and D.E. Taylor. Computing in groups of Lie type. *Mathematics of Computation*, 73(247):1477–1498, 2004.

[5] Willem A. de Graaf. *Lie Algebras: Theory and Algorithms*, volume 56 of *North Holland Mathematical Library*. Elsevier Science, 2000.

[6] Alexander J. E. Ryba. Computer construction of split Cartan subalgebras. *J. Algebra*, 309(2):455–483, 2007.

[7] Martin Schönert et al. *GAP – Groups, Algorithms, and Programming*. Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, fifth edition, 1995.

[8] Robert Steinberg. Automorphisms of classical Lie algebras. *Pacific J. Math.*, 11:1119–1129, 1961.

(Dan Roozemond) Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands

E-mail address: `d.a.roozemond@tue.nl`