A simple way to compute structure constants of semi-simple Lie algebras

Bill Casselman
University of British Columbia
cass@math.ubc.ca

A standard technique for computing the structure constants of semi-simple Lie algebras, which has been used in the computer program MAGMA and described well by [Cohen-Murray-Taylor:2005], relies on the additive structure of roots. In [Casselman:2015b] I explained another way to compute these structure constants by implementing an idea originally found in [Tits:1966a]. Titś’ idea was to replace the additive structure by features of the normalizer of a maximal torus. This provided some mathematical structure to the problem of computing structure constants that was missing in the standard approach. In practice, computation based on this method went fairly rapidly and seemed at least roughly comparable in efficiency to reported runs of the standard computation. There were, however, a number of rather ugly and presumably inefficient formulas involved in this new algorithm. Recently, it was suggested by Robert Kottwitz (in May of 2014 and expanded by him later that year), that an observation of his about choosing bases of semi-simple Lie algebras might make it possible to bypass the nastiest parts in a more elegant manner. In this paper, with Kottwitz’ permission, I’ll explain how this goes.

Kottwitz’ observations can be briefly summarized. Suppose

\[ G = \text{a simple, connected, simply connected, complex group} \]
\[ g = \text{Lie algebra of } G \]
\[ B = \text{Borel subgroup} \]
\[ T = \text{maximal torus in } B \]
\[ \Sigma = \text{associated root system} \]
\[ \Delta = \text{associated simple roots} \]
\[ W = \text{Weyl group}. \]

Because \( G \) is simply connected, the coroot lattice \( X_*(T) \) may be identified with the lattice spanned by the simple coroots \( \alpha^\vee \).

The root spaces \( g_\alpha \), all have dimension one. Fix for each \( \alpha \) in \( \Delta \) a spanning element \( e_\alpha \) in \( g_\alpha \). The triple \((B,T,\{e_\alpha\})\) make up a frame for \( G \). The set of all frames is a principal homogeneous space for the adjoint quotient of \( G \). (This notion originated in work by French mathematicians. In French the term is ‘épinglage’, which some translate literally into the noun ‘pinning’. But ‘frame’ is the term adopted in the English translation of Bourbaki’s treatise on Lie algebras.)

Chevalley has defined integral structures on \( g \) and \( G \). If \( \mathcal{N}(\mathbb{Z}) \) is the group of integral points in the normalizer \( \mathcal{N} = N_G(T) \), it fits into a well understood extension

\[ 1 \rightarrow T(\mathbb{Z}) = \{\pm 1\}^\Delta \rightarrow \mathcal{N}(\mathbb{Z}) \rightarrow W \rightarrow 1. \]

[Tits:1966b] defined a certain convenient section \( w \mapsto \hat{w} \) of the last quotient map, and described this extension precisely enough to enable computations in it, and [Langlands-Shelstad:1987] gave an explicit formula for a defining 2-cocycle. This extension certainly does not split. But now let \( V_\Sigma \) be the direct sum of non-trivial root spaces in \( g_\Sigma \). Let \( S(\mathbb{Z}) \) be the subgroup of transformations in \( GL(V_\Sigma) \) that act as \( \pm 1 \) on each root space. It may be identified with \( \text{Hom}(\Sigma, \mathbb{Z}) = (\mathbb{Z})^\Sigma \). There is a homomorphism from the group \( T(\mathbb{Z}) \) to \( S(\mathbb{Z}) \): \( \alpha^\vee(x) \) goes to \( (x^{\langle \gamma, \alpha^\vee \rangle})_{\gamma \in \Sigma} \). The kernel is \( Z_G \). The homomorphism from \( T \) to \( S \) gives rise to an extension

\[ 1 \rightarrow S(\mathbb{Z}) = \{\pm 1\}^\Sigma \rightarrow \mathcal{N}(\mathbb{Z}) \rightarrow W \rightarrow 1. \]
Although it does not act as automorphisms of $g$, the extension does act on $V_Z$, compatibly with the adjoint action of $T(Z)$. Kottwitz’ remarkable observation is that this new extension splits, and he gives an explicit splitting $w \mapsto \tilde{w}$. It has the property that if $w\lambda = \lambda$ then $\tilde{w}$ acts as the identity on $g\lambda$. This allows one to specify a natural choice of Chevalley basis, once one fixes one $e_\gamma$ for each $W$-orbit in $\Sigma$. One consequence of the new method is a very simple description of the action of $N(Z)$ on $g$. This is especially important in applications to computation in the group $G$ rather than just its Lie algebra.

The previous methods known have the virtue that they may be extended to all Kac-Moody root systems (see [Casselman:2015b]). Some variant of the method I describe here will work for a large class of these. I do not see how it can be extended to all of them, but one might hope that some variation of Kottwitz’ idea will work, taking into account some explicit obstruction. One promising prerequisite for extending the method to Kac-Moody algebras can be found in [Carbone et al.:2015], which classifies conjugacy classes of simple roots.

### Contents

1. Chevalley bases
2. Tits’ idea
3. Computation I
4. Kottwitz’ splittings
5. Computation II
6. References

For $g$ in $G$, $x$ in $g$, I’ll write

$$g \cdot x = \text{Ad}(g)x.$$

Even though $N(Z)$ does not act by automorphisms of $g$, I’ll use this notation for its action on $V_Z$ as well. I’ll usually refer to [Tits:1966a] as [T].

1. **Chevalley bases**

I fix once and for all a frame $(B, T, \{e_\alpha\})$. The frame determines embeddings of $\text{SL}_2$ into $G$, one for each simple root. Let $\iota_\alpha$ be the one parametrized by $\alpha$. Each of these takes the diagonal matrices into $T$ and the differential of $\iota_\alpha$ takes

$$\begin{bmatrix} 1 \\ \beta \gamma \end{bmatrix}$$

to $e_\alpha$. The associated embedding of $\mathbb{C}^\times$ is the coroot $\alpha^\vee$, and is independent of the choice of $e_\alpha$. Let $h_\alpha$ be the image under $dt_\alpha$ of

$$\begin{bmatrix} 1 \\ \alpha \beta \end{bmatrix}.$$

The image $e_{-\alpha}$ of

$$\begin{bmatrix} \gamma \\ \alpha \beta \\ -1 \end{bmatrix}$$

is the unique element of $g_{-\alpha}$ such that

$$[e_{-\alpha}, e_\alpha] = h_\alpha.$$

This choice of sign is Tits’. It is not the common one, but it is exactly what is needed to make his analysis of structure constants work. The point is that there exists a unique automorphism $\theta$ of $g$ acting as $-I$ on $t$ and taking each $e_\alpha$ ($\alpha \in \Delta$) to $e_{-\alpha}$. Invariance under $\theta$ is extremely valuable.

**TITS’ SECTION.** The group $N(Z)$ fits into a short exact sequence

$$1 \longrightarrow T(Z) = (\pm 1)^\Delta \longrightarrow N(Z) \longrightarrow W \longrightarrow 1,$$
and [Tits:1966b] shows how to define a particularly convenient section. Define $s_\alpha$ to be the image under $\iota_\alpha$ of
\[
\begin{bmatrix}
0 & 1 \\
-1 & 0
\end{bmatrix}.
\]
It lies in the normalizer of $T$. Suppose $w$ in $W$ to have the reduced expression $w = s_1 \ldots s_n$. Then the product
\[
\dot{w} = \dot{s}_1 \ldots \dot{s}_n
\]
depends only on $w$, not the particular expression. The defining relations for this group, given those for $W$, are
\[
(xy)' = x'y' \quad (\ell(xy) = \ell(x) + \ell(y))
\]
\[
s_\alpha^2 = \alpha^\vee(-1) \quad (\alpha \in \Delta).
\]

**CHEVALLERY’S FORMULA.** Suppose $\gamma$ to be a root, $e_{\pm \gamma} \neq 0$ in $g_{\pm \gamma}$, and $h_\gamma = [e_{-\gamma}, e_\gamma]$. I’ll call $(e_\gamma, h_\gamma, e_{-\gamma})$ a Morozov triple if $\langle \gamma, h_\gamma \rangle = 2$. Any $e_\gamma$ may be extended to a unique Morozov triple.

Suppose given such a triple, and suppose that $e_\theta^\gamma = ce_{-\gamma}$. If $e_\gamma = e_\gamma/\sqrt{c}$ and $e_{-\gamma} = \sqrt{c}e_\gamma$, then $(e_\gamma, h_\gamma, e_{-\gamma})$ are also a Morozov triple, and $e_\theta^\gamma = e_{-\gamma}$. Up to sign—but only up to sign—$e_\gamma$ is unique with this invariance condition.

Any complete set $\{e_\gamma\}$ invariant under $\theta$ up to sign is often called a Chevalley basis (with respect to the given frame). It determines an integral structure on the Lie algebra $g$, and I’ll call such a basis an integral basis. If it is actually invariant under $\theta$, as it is here, I’ll call it an invariant integral basis.

Given any integral basis, Chevalley proved that if $\lambda, \mu, \nu$ are roots with $\lambda + \mu + \nu = 0$ then
\[
[e_\lambda, e_\mu] = \pm (p_{\lambda,\mu} + 1)e_{-\nu}.
\]
Here $p_{\lambda,\mu}$ is the least $p$ such that $\mu - p\lambda$ is a root. This was the crucial result used to construct the Chevalley groups over arbitrary fields.

The possible values for the string constants $p_{\lambda,\mu}$ (associated to finite root systems) are shown in the following figures.

The fourth figure occurs only in type $G_2$. In practice, we shall be interested in computing $p_{\lambda,\mu}$ only when $\langle \mu, \lambda^\vee \rangle \leq 0$. Under this assumption, as the figures illustrate:
\[
p_{\lambda,\mu} = \begin{cases} 
0 & \text{if } \mu - \lambda \text{ is not a root} \\
1 & \text{otherwise}.
\end{cases}
\]

I refer to [Chevalley:1955] or [Carter:1972] for the original proof of (1.1) and to [Casselman:2015a] for a proof extracted from [T], which works uniformly for all Kac-Moody groups. Tits’ choice of the $e_{-\alpha}$ (as opposed to the more common choice with the opposite sign) introduces an elegant symmetry that greatly simplifies both proofs and formulas.
Ultimately, Chevalley’s formula depends on the simple fact that for strings of length 2, as in the second figure above, one always has \( \|\lambda\| \geq \|\mu\| \). That is to say, the following configuration never occurs.

\[ \begin{array}{c}
\end{array} \]

Determining the sign in (1.1) has always seemed rather mysterious. Of course there is no one formula, since the choice of an integral basis is not canonical. But I don’t think it has ever been very clear what is going on. Changing even one \( e_\gamma \) to \( -e_\gamma \) forces a lot of other sign changes without apparent pattern. The situation has now been cleared up somewhat by Kottwitz, who has explained to me how to choose an almost canonical integral basis. I’ll discuss that in §3.

In §4 I’ll show how Kottwitz’ basis simplifies the computation of the signs in Chevalley’s formula. The starting point, at least, is the same as it was in [Casselman: 2015], in which I have already outlined the principal ingredients of a recipe for the constants. One of the troublesome points in the earlier approach was a somewhat arbitrary choice of integral basis. Kottwitz’ basis eliminates this inconvenience.

2. Tits’ idea

In order to see how Kottwitz’ basis gives rise to practical algorithms, it is necessary first to recall Tits’ results. Suppose given some \( f_\gamma \) generating \( g_\gamma \cap g_\mathbb{Z} \). It is unique up to sign. I have indicated above how it determines an embedding of \( \text{SL}_2(\mathbb{Z}) \) into \( G(\mathbb{Z}) \) and elements \( h_\gamma, f_{-\gamma} \) making up a copy of \( \mathfrak{sl}_2 \). We also get then an element \( \sigma_\gamma \) in \( N(\mathbb{Z}) \), the image of

\[ \begin{bmatrix}
\gamma & 1 \\
-1 & \gamma
\end{bmatrix}. \]

Thus \( \sigma_\gamma \) depends on the choice of \( f_\gamma \) (and \( T \), which we have fixed), but on nothing else. If \( \gamma = \alpha \) and \( f_\alpha = e_\alpha \), then \( \sigma_\alpha = \delta_\alpha \). In any case its image in \( W \) will be \( s_\gamma \), the reflection corresponding to \( \gamma \). The basic observation of Tits ([T], Proposition 1) is that each of the objects \( f_\pm \lambda, \sigma_\lambda \) determine the other two. The choice of sign for any one of these determines a change of sign in the others. This relationship is summarized in the equation

\[ \exp(f_\gamma) \exp(f_{-\gamma}) \exp(f_\gamma) = \sigma_\gamma, \]

mirroring this equation in \( \text{SL}_2 \):

\[ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \]

In other words, the choice of a Chevalley basis is equivalent to a certain choice of elements \( \sigma_\gamma \) in the normalizer \( N(\mathbb{Z}) = N_G(T) \cap G(\mathbb{Z}) \). There are two basic equations satisfied by \( \sigma_\gamma \):

\[ \sigma_\gamma^{-1} = \gamma (-1) \sigma_\gamma, \]

\[ \sigma_\gamma = \sigma_{-\gamma}. \]

I repeat: there are two integral elements \( \pm f_\gamma \) in \( g_\gamma \), and likewise two \( \gamma (-1) \sigma_\gamma \) in \( N(\mathbb{Z}) \). Let \( W_\gamma(\mathbb{Z}) \) be the subgroup of \( N_G(\mathbb{Z}) \) generated by the \( \gamma (-1) \sigma_\gamma \).

One practical consequence of Tits’ observation is this:

2.1. Lemma. Suppose \( \omega \) to be in \( N(\mathbb{Z}) \) with image \( w \) in \( W \), with \( w\lambda = \mu \). Then

\[ \omega \circ f_\lambda = e f_\mu \]
Computing structure constants

if and only if

\[ \omega \sigma \omega^{-1} = \mu^\vee (\varepsilon) \sigma_\mu . \]

Proof. Since

\[ \exp(\varepsilon f_\mu) \exp(\varepsilon f_{-\mu}) \exp(\varepsilon f_\mu) = \mu^\vee (\varepsilon)\sigma_\mu . \]

Given an integral basis \((f_\gamma)\), we want to figure out how to calculate the sign in

\[ [f_\lambda, f_\mu] = \pm (p_{\lambda,\mu} + 1) f_{\lambda + \mu} . \]

Tits has introduced a convenient symmetry into this problem by his choice of \(\epsilon_{-\gamma}\). For example, since this basis is invariant under \(\theta\), the constants are now the same for \(-\lambda, -\mu\) and \(\lambda, \mu\). Tits has introduced a second symmetry by another simple notion. I define a Tits triple to be a set of roots \(\lambda, \mu, \nu\) whose sum is \(0\). He makes this choice instead of writing \(\lambda + \mu = \nu\), which is more conventional.

In any irreducible root system there are at most two lengths. If \(\lambda + \mu + \nu = 0\), two of them must be of the same length. As I have already mentioned, the common length cannot be greater than the third. Therefore any Tits triple can be cyclically permuted to satisfy the condition

\[ \|\lambda\| \geq \|\mu\| = \|\nu\| . \]

In this case, I shall call it an ordered Tits triple.

### 2.2. Proposition. (Lemma 1 of §2.5)

Suppose \((\lambda, \mu, \nu)\) to be a Tits triple. The following are equivalent:

(a) it is an ordered triple;
(b) \(s_\lambda \mu = -\nu\);
(c) \(\langle \mu, \lambda^\vee \rangle = -1\).

In some sense the notion of an ordered Tits triple remains valid for Kac-Moody root systems.

For an ordered triple, because of (b):

\[ \sigma_\lambda \sigma_\mu \sigma_\lambda^{-1} = \nu^\vee (\pm 1) \sigma_\nu . \]

The upshot of the discussion so far is that there exists a function \(\varepsilon(\sigma_\lambda, \sigma_\mu, \sigma_\nu)\), defined on all products \(W_\lambda(Z) \times W_\mu(Z) \times W_\nu(Z)\) whenever \((\lambda, \mu, \nu)\) is a Tits triple, such that

\[ [f_\lambda, f_\mu] = \varepsilon(\sigma_\lambda, \sigma_\mu, \sigma_\nu) (p_{\lambda,\mu} + 1) f_{-\nu} . \]

The following is the basis of computation of structure constants by Tits’ method. (See [T], §2.9.)

### 2.3. Proposition. The function \(\varepsilon(\sigma_\lambda, \sigma_\mu, \sigma_\nu)\) satisfies these basic properties

(a) replacing \(\sigma_\lambda\) by \(\sigma_\lambda^{-1}\) changes the sign;
(b) it is skew-symmetric in any pair;
(c) it is invariant under cyclic rotation of the arguments;
(d) if \(\lambda, \mu, \nu\) are an ordered triple with \(\sigma_\lambda \sigma_\mu \sigma_\lambda^{-1} = \sigma_\nu\) then

\[ \varepsilon(\sigma_\lambda, \sigma_\mu, \sigma_\nu) = (-1)^{p_{\lambda,\mu}} . \]

The first two are immediate, but the third is not quite so. Together, these mean that we can apply a permutation to any triple to reduce to a special case, but what is now needed is one explicit formula in that special case—i.e. to pin down signs. That is what the last does. It follows from an analysis (in [T], §1.3) of the action of copies of \(\text{SL}_2(Z)\) on the root spaces determined by root strings in \(\mathfrak{g}\).

### 2.4. Lemma. Suppose \((\lambda, \mu, \nu)\) to be an ordered Tits triple. The following are equivalent:
(a) $\sigma_\lambda \sigma_\mu \sigma_\lambda^{-1} = \nu^\vee (\varepsilon) \sigma_\nu$;
(b) $\sigma_\lambda \circ f_\mu = \varepsilon f_{-\mu}$;
(c) $[f_\lambda, f_\mu] = \varepsilon (-1)^{p_{\lambda,\mu}} (p_{\lambda,\mu} + 1) f_{-\mu}$.

One more thing I need is due to Tits, but formulated more explicitly in Chapter 4 (Theorem 4.1.2 (ii)) of [Carter:1972] and as Lemma 2.5 in [Casselman:2015]:

2.5. Proposition. If $(\lambda, \mu, \nu)$ is a Tits triple then

$$\frac{p_{\lambda,\mu} + 1}{\|\nu\|^2} = \frac{p_{\mu,\nu} + 1}{\|\lambda\|^2} = \frac{p_{\nu,\lambda} + 1}{\|\mu\|^2}$$

In other words, $p_{\lambda,\mu}$ satisfies a twisted cyclic symmetry.

I repeat: this whole treatment is valid only for a choice of integral basis invariant under $\theta$.

3. Computation

How do results in the previous section apply to practical computation of structure constants?

The ultimate goal is to come up with a procedure to determine $[f_\lambda, f_\mu]$ easily, given an invariant integral basis $(f_\lambda)$. There are three possibilities. (1) If $\lambda = -\mu$, the bracket is $h_\mu$. We can express it as a linear combination of basis elements $h_\alpha$. (2) The sum $\lambda + \mu$ is not a root, and the bracket is 0. We shall have available a look-up table to decide this. (3) We have an equation

$$[f_\lambda, f_\mu] = N_{\lambda,\mu} f_{\lambda+\mu}$$

for some constant $N_{\lambda,\mu}$ of the form $\pm (p_{\lambda,\mu} + 1)$. So we would be given a Tits triple $(\lambda, \mu, \nu)$. We can rotate it to make it an ordered triple. According to Proposition 2.3 and Proposition 2.5, our problem is thus reduced to finding just the values $N_{\lambda,\mu}$ when $(\lambda, \mu, \nu)$ is an ordered triple. Since $N_{-\lambda, -\mu} = N_{\lambda,\mu}$, we may restrict to the case $\lambda > 0$.

We shall in fact calculate and then store all such values. The amount of storage required is roughly proportional to the number of Tits triples. As reported in [Cohen-Murray-Taylor:2005], this is of order $r^3$, where $r$ is the rank of the system, so this procedure is entirely feasible, and noticeably better in storage use than storing all the $N_{\lambda,\mu}$, since there are roughly $r^4$ such pairs. (Of course using the smaller table involves more computation. The trade-off of time versus memory that we see here is a basic problem in all programming.)

There are three steps to this computation.

Step 1. In the first, we construct the root system, without reference to a Lie algebra. This includes (i) root lengths $\|\lambda\|$, (ii) values of $\langle \lambda, \alpha^\vee \rangle$, (iii) root reflection tables $s_\alpha \lambda$, (iv) an expression for each root as a linear combination of the $\alpha$ in $\Delta$, and (v) a corresponding expression for each $\lambda^\vee$ as a sum of $\alpha^\vee$. We can also construct a table recording whether or not a given array of coordinates is that of a root or not.

Step 2. In some way specified in the next sections, we then find an invariant basis $(f_\lambda)$. It is here where Kottwitz’ contribution appears. This gives us also the associated Tits section $\tilde{w}$ from $W$ to $N_G(T)$, in which $\tilde{s}_\alpha$ for $\alpha$ in $\Delta$ is the same as the reflection $\sigma_\alpha$ determined by $f_\alpha$. Miraculously:

The construction of the basis $(f_\lambda)$ will give us at the same time all the constants $c(s_\alpha, \lambda)$ (with $\alpha$ simple) such that

$$\tilde{s}_\alpha \circ f_\mu = c(s_\alpha, \lambda) f_{s_\alpha \lambda}.$$
then
\[ c(xy, \lambda) = c(x, y\lambda)c(y, \lambda) . \]

**Remark.** This can be somewhat inefficient, since the element \( w \) can have length up to the number of positive roots. There is a possible improvement, however, offering a trade of memory for time. Choose an ordering of \( \Delta \), and let \( W_i \) be the subgroup of \( W \) generated by the \( s_{\alpha_j} \) for \( j \leq i \). As Fokko du Cloux pointed out, every \( w \) in \( W \) can be expressed as a unique product

\[ w = w_1 w_2 \ldots w_r \]

with each \( w_i \) a distinguished representative of \( W_{i-1} \setminus W_i \). The sizes of these cosets are relatively small, and it is perhaps not infeasible to store values of the \( w\lambda \) and the \( c(w, \lambda) \) for \( w \) a distinguished element in one of them.

**Step 3.** Given the results of the previous step, we want now to tell how to compute the constants \( N_{\lambda,\mu} \) when \( (\lambda, \mu, \nu) \) make up an ordered Tits triple with \( \lambda > 0 \).

We can do this by a kind of induction on \( \lambda \). Every positive root \( \lambda = w\alpha \) for \( w \) in \( W \) and \( \alpha \) simple. The **depth** \( n \) of \( \lambda \) is the minimal length of a chain

\[ \alpha = \lambda_0 - \lambda_1 - \cdots - \lambda_n = \lambda \]

in which each \( \lambda_{i+1} = s_{\alpha_i} \lambda_i \) for some simple \( \alpha_i \). Finding such chains for all positive roots is part of the natural process for constructing the set of roots in the first place. If

\[ [f_\lambda, f_\mu] = N_{\lambda,\mu} f_{-\nu} \]

then

\[ [s_\alpha \circ f_\lambda, s_\alpha \circ f_\mu] = N_{\lambda,\mu} (s_\alpha \circ f_{-\nu}) , \]

and hence

\[ N_{s_\alpha \lambda, s_\alpha \mu} = c(s_\alpha, \lambda)c(s_\alpha, \mu)c(s_\alpha, -\mu)N_{\lambda,\mu} . \]

Reflections transform ordered triples to ordered triples. Hence if we know how to deal with the case in which \( \lambda = \alpha \) is simple we can compute all the constants for ordered triples in which \( \lambda > 0 \) by following up the chain. Furthermore, according to Proposition 2.2 it is very easy to list ordered triples \( (\alpha, \mu, \nu) \).

Now according to Lemma 2.4 we have

\[ [f_\alpha, f_\mu] = c(s_\alpha, \mu)(-1)^{p_{\alpha,\mu}}(p_{\alpha,\mu} + 1)f_{-\nu} . \]

Since \( (\mu, \alpha^\vee) = -1 \) we know that \( p_{\alpha,\mu} \) is 0 if \( \mu - \alpha \) is not a root, and is 1 otherwise (in which case we are dealing with \( G_2 \)).

At the end we have the structure constants for all ordered Tits triples with \( \lambda \) positive.
4. Kottwitz’ splittings

Tits’ methods apply if we are given an invariant integral basis. How is one to be found?

The traditional method (found in [Cohen-Murray-Taylor:2005], specifying such a basis in terms of an ordered decomposition of a given root as a sum of simple ones, and the method I described in [Casselman:2015a] and [Casselman:2015b] does this in terms of paths in a spanning tree in what I call the root graph. There is a great deal of arbitrariness in both. Kottwitz’ contribution is to remove nearly all this annoying ambiguity. A basis chosen directly by his method will not be invariant under \( \theta \), but it will be easy to determine from it one that is.

Our choice of frame gives us a map \( w \mapsto \tilde{w} \) from \( W \) back to \( N(\mathbb{Z}) \), and then to \( \mathcal{N}_{\text{ext}}(\mathbb{Z}) \). How can it be modified to become a homomorphism?

We are looking for a splitting of the sequence

\[
1 \rightarrow S(\mathbb{Z}) \rightarrow \mathcal{N}_{\text{ext}}(\mathbb{Z}) \rightarrow W \rightarrow 1 .
\]

This will be of the form

\[
\tilde{w} = w \cdot \tau_w ,
\]

with each \( \tau_w \) in \( S(\mathbb{Z}) \). Thus for each root \( \beta \) we are looking for a factor \( \tau_w(\beta) = \pm 1 \). The map \( w \mapsto \tilde{w} \) will be a homomorphism if and only if (for \( \alpha \) in \( \Delta \))

(a) \( \tilde{1} = 1 \)
(b) \( \bar{s}_\alpha \bar{x} = (s_\alpha x)^\vee \) if \( s_\alpha x > x \)
(c) \( \bar{s}_\alpha \bar{s}_\alpha = 1 \).

These translate directly to properties of \( \tau_w \):

(a') \( \tau_1 = 1 \)
(b') \( \tau_{s_\alpha}(y\beta)\tau_y(\beta) = \tau_{s_\alpha y}(\beta) \) for all \( \beta \) if \( s_\alpha y > y \)
(c') \( (-1)^{\langle \beta, \alpha^\vee \rangle} = \tau_{s_\alpha}(s_\alpha \beta) \cdot \tau_{s_\alpha}(\beta) \).

We shall see a bit later a fourth condition on \( \tilde{w} \) and hence also on \( \tau_w \).

At any rate, here is Kottwitz’ solution of the problem. For \( w \) in \( W \) set

\[
R_w = \{ \lambda > 0 \mid w\lambda < 0 \} .
\]

Thus \( \ell(xy) = \ell(x) + \ell(y) \) if and only if

(4.1) \( R_{xy} = R_y \sqcup y^{-1}R_x \),

and in particular

\[
R_1 = 0 \quad \quad R_\alpha = \{ \alpha \} \quad \quad R_{s_\alpha w} = R_w \sqcup \{ w^{-1}\alpha \} \quad (w^{-1}\alpha > 0) .
\]

According to Kottwitz’ recipe, the factor \( \tau_w(\beta) \) is required to be of the form \((-1)^{F(w,\beta)}\) with \( F \) of the form

(4.2) \( F(w,\beta) = \sum_{\gamma \in R_w} \langle \beta, \gamma \rangle \).

The summands are yet to be specified, and everything in this formula is to be taken modulo 2.
• Since \( R_1 = \emptyset \) and an empty sum is 0, condition (a) above is immediate.

• What about condition (b)? Suppose \( x = s_\alpha y > y \). It must be shown that the cocycle condition

\[
F(s_\alpha y, \beta) = F(s_\alpha, y\beta) + F(y, \beta)
\]

holds. First of all, note that

\[
F(s_\alpha, \beta) = \langle \langle \beta, \alpha \rangle \rangle
\]

since \( R_{s_\alpha} = \{ \alpha \} \). Also

\[
F(x, \beta) = \sum_{\gamma \in R_x} \langle \langle \gamma, \beta \rangle \rangle = \langle \langle \beta, y^{-1} \alpha \rangle \rangle + \sum_{\gamma \in R_y} \langle \langle \beta, \gamma \rangle \rangle
\]

whereas

\[
F(s_\alpha, y\beta) + F(x, \beta) = \langle \langle y\beta, \alpha \rangle \rangle + \sum_{\gamma \in R_y} \langle \langle \beta, \gamma \rangle \rangle.
\]

Therefore (b) will be satisfied if \( W \)-invariance holds:

\[
\langle \langle w\beta, w\gamma \rangle \rangle = \langle \langle \beta, \gamma \rangle \rangle \text{ for all } w \text{ in } W.
\]

• Condition (c)? We have

\[
\hat{s}_\alpha \circ e_\beta = (-1)^{\langle \langle \beta, \alpha \rangle \rangle} s_\alpha \circ e_\beta.
\]

Since \( \hat{s}_\alpha = \alpha(-1) \) we thus require that

\[
\langle \langle s_\alpha \beta, \alpha \rangle \rangle + \langle \langle \beta, \alpha \rangle \rangle = \langle \langle \beta, \alpha^\vee \rangle \rangle.
\]

This last condition suggests what comes now. If \( \langle \beta, \alpha^\vee \rangle = 0 \) and hence \( s_\alpha \beta = \beta \) this imposes no condition (since everything is modulo 2). Otherwise \( \langle \beta, \alpha^\vee \rangle \) and \( \langle s_\alpha \beta, \alpha^\vee \rangle \) will be of different signs. It is therefore natural to set

\[
\langle \langle \beta, \gamma \rangle \rangle = \begin{cases} 
\langle \beta, \gamma^\vee \rangle & \text{if } \langle \beta, \gamma^\vee \rangle > 0 \\
0 & \text{if } \langle \beta, \gamma^\vee \rangle < 0.
\end{cases}
\]

One good sign:

4.4. Lemma. The function \( \langle \langle \beta, \gamma \rangle \rangle \) is Weyl-invariant.

Proof. Since the pairing \( \langle \beta, \gamma^\vee \rangle \) is \( W \)-invariant.

The requirement that \( w \mapsto \hat{w} \) be a homomorphism imposes no extra condition in the case that \( \langle \beta, \gamma^\vee \rangle = 0 \), but one more requirement will do so. I ask now, for reasons that will become apparent in a moment, that

\[
\hat{w} \circ e_\beta = e_\beta
\]

if \( w\beta = \beta \). To guarantee that this occurs, it suffices to assume that \( \beta \) lies in the closed positive Weyl chamber. Then the \( w \) fixing \( \beta \) are generated by simple root reflections, so we need to require only that \( \tilde{s}_\alpha v_\beta = v_\beta \) (\( v_\beta \in \mathfrak{g}_\beta \)) for simple roots \( \alpha \) with \( \langle \beta, \alpha^\vee \rangle = 0 \). Consideration of the representation of \( \text{SL}_2 \) corresponding to the root string tells us that

\[
\tilde{s}_\alpha \circ e_\beta = (-1)^{p_\alpha,\beta} e_\beta.
\]

Therefore

\[
\hat{\tilde{s}}_\alpha \circ e_\beta = (-1)^{\langle \langle \beta, \alpha \rangle \rangle} (-1)^{p_\alpha,\beta} e_\beta
\]

and so we set

\[
\langle \langle \beta, \gamma \rangle \rangle = p_{\gamma,\beta} \quad \text{if } \langle \beta, \gamma^\vee \rangle = 0.
\]
Computing structure constants

Equations (4.3) and (4.5) define the terms $\langle \beta, \gamma \rangle$ completely. In summary:

**4.6. Theorem.** (Kottwitz) Let

$$
\langle \beta, \gamma \rangle = \begin{cases} 
(\beta, \gamma^\vee) & \text{if this is positive} \\
p_{\gamma, \beta} & \text{if } \langle \beta, \gamma^\vee \rangle = 0 \\
0 & \text{otherwise.}
\end{cases}
$$

$$
F(w, \beta) = \sum_{\gamma \in \mathcal{R}} \langle \beta, \gamma \rangle
$$

Then

$$
\tau_w = ((-1)^F(w, \beta))_{\beta \in \Sigma}.
$$

Let

$$
\tilde{w} = \cdot w \cdot \tau_w
$$

is a splitting homomorphism of $N_{\text{ext}}(\mathbb{Z})$. In addition, if $w \gamma = \gamma$ then $\text{Ad}(\tilde{w})$ is the identity on $\mathfrak{g}_\gamma$.

If the root system is simply laced or equal to $G_2$ then $s_{\lambda} \beta = \beta$ implies that $p_{\lambda, \beta} = 0$. Therefore the non-trivial case occurs only for systems $B_n$, $C_n$, or $F_4$.

**Remark.** Lemma 2.1A of [Langlands–Shelstad:1987] exhibits the 2-cocycle defining the extension $N(\mathbb{Z})$ determined by Tits’s splitting $w \mapsto w \cdot \tau_w$. Explicitly,

$$
\tilde{x} \tilde{y} = \kappa(x, y)(xy) \cdot \text{with } \kappa(x, y) = \prod_{\gamma > 0} (x^{-1}) \gamma < 0 \prod_{\gamma > 0} (y^{-1}) x^{-1} \gamma < 0.
$$

Does Kottwitz’ splitting allow arguments of Langlands and Shelstad to be simpler?

**4.7. Corollary.** There exists an integral basis $(e_\gamma)$ of $V_\mathbb{Z}$ such that $\tilde{w} \cdot e_\gamma = e_{w \gamma}$ for all roots $\gamma$ and $w$ in $W$.

I’ll call such a basis *semi-canonical*. There are several possibilities, two for each $W$-orbit in $\Sigma$.

**Proof.** The $W$-orbits are the sets of all roots of the same length. Pick one simple root $\alpha$ in each orbit, and let $e_\alpha = e_\alpha$ be the corresponding element in the frame chosen at the beginning. If $\lambda = w \alpha$ is root with $\alpha$ equal to one of these distinguished choices, define

$$
e_\lambda = \tilde{w} \cdot e_\alpha.
$$

The definition of $F(s_\alpha, \beta)$ in the case when $\langle \beta, \alpha^\vee \rangle = 0$ insures that this is a valid definition.

In practice, we shall want to compute $\tau_w$ explicitly only when $w = s_\alpha$ for $\alpha$ in $\Delta$. In this case, there is a simplification, since $R_{s_\alpha}$ is a singleton. If $c = \langle \lambda, \alpha^\vee \rangle$, then

$$
F(s_\alpha, \lambda) = \begin{cases} 
c & \text{if } c > 0 \\
p_{\alpha, \beta} & \text{if } c = 0 \\
0 & \text{otherwise.}
\end{cases}
$$

**Example.** For a simply laced root system, if $\langle \beta, \alpha^\vee \rangle = 0$ then $p_{\alpha, \beta} = 0$. Therefore

$$
\tau_{s_\alpha}(\lambda) = \begin{cases} 
(-1)^{\beta, \alpha^\vee} & \text{if } \langle \lambda, \alpha^\vee \rangle > 0 \\
1 & \text{otherwise.}
\end{cases}
$$

This applies in particular to $G = \text{SL}_3$. Take $\alpha, \beta$ as the standard simple roots, and let $\gamma = \alpha + \beta$. Recall that $e_{i, j}$ is the matrix with a single non-zero entry 1 at $(i, j)$. Choose $e_{1, 2}$ and $e_{2, 3}$ to define the frame, spanning the root spaces for $\alpha, \beta$. The corresponding elements of $N(\mathbb{Z})$ are

$$
\begin{bmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.
$$

And here is a table of the $\cdot$ actions:
Recall that \( \langle \alpha, \beta \rangle < 0 \) while \( \langle \gamma, \alpha \rangle > 0 \). If we start with \( e_\alpha = e_{1,2} \) we get

\[
\begin{align*}
\epsilon_\alpha &= \epsilon_{1,2} = e_\alpha \\
\epsilon_\gamma &= s_\beta \epsilon_\alpha \\
&= (-1)^0 s_\beta \epsilon_{1,2} \\
&= -\epsilon_{1,3} \\
\epsilon_\beta &= s_\alpha \epsilon_\gamma \\
&= (-1)^1 s_\alpha \epsilon_{1,3} \\
&= -\epsilon_{2,3} = -\epsilon_\beta.
\end{align*}
\]

Thus:

**4.8. Proposition.** If \( G = SL_3 \) and \( e_\alpha = e_\alpha \), then \( e_\beta = -e_\beta \).

This example has consequences for arbitrary root systems.

Something similar is true for \( SL_n \). Here, choose the base point of the Dynkin diagram to be the end corresponding to the simple root \( \epsilon_1 - \epsilon_2 \). Then

\[
\epsilon_{i,j} = (-1)^j \epsilon_{i,j}.
\]

A semi-canonical basis will not be invariant under \( \theta \), but it is easy to see how it fails, and then how to modify it to be so. Recall that the height of a root is defined by the formula

\[
ht \left( \sum_\Delta \lambda_\alpha \right) = \sum_\Delta \lambda_\alpha.
\]

**4.9. Theorem.** For any root \( \gamma \) and Kottwitz basis \( (e_\gamma) \)

\[
e_\gamma^\theta = (-1)^{ht(\gamma)} e_{-\gamma}.
\]

In particular, if \( \alpha \) is simple then

\[
e_\alpha^\theta = e_{-\alpha}.
\]

This particularly simple formulation is due to Kottwitz.

**Proof.** In a number of short steps.

**Step 1.** The following is straightforward:

- For all \( \beta, \gamma \)

\[
\langle \beta \rangle + \langle -\beta \rangle = \langle \beta, \gamma \rangle + \langle -\beta, \gamma \rangle = \langle \beta, \gamma \rangle.
\]
This is to be interpreted modulo 2, of course.

**Step 2.** Now let

\[ h(w, \beta) = \sum_{\gamma \in R_w} \langle \beta, \gamma \rangle. \]

- For \( v \in g_\beta \)

\[ (\tilde{w} \circ v)^\theta = (-1)^{h(w, \beta)} \tilde{w} \circ v^\theta. \]

This is because \( s_\alpha^\theta = s_\alpha \).

**Step 3.** Induction on the length of \( w \) together with (4.1) will prove:

- For \( w \) in \( W \) and root \( \lambda \)

\[ \text{ht}(w\lambda) - \text{ht}(\lambda) = h(w, \lambda). \]

This concludes the proof of the Theorem.

In order to specify the \( e_\alpha \), given a frame \((e_\alpha)\), we fix one simple root \( \alpha \) in each \( W \)-orbit, and set \( e_\alpha = e_\alpha \).

Fixing the \( e_\beta \) for other simple roots \( \beta \) is then very easy. The \( W \)-orbits are in bijection with possible root lengths. For finite-dimensional Lie algebras simple roots of the same length lie in connected segments in the Dynkin diagram. Furthermore, there will be exactly one simple root that is long, and a segment of short ones. One may therefore select the end points of the diagram—both, if necessary—as special ones. For every simple root \( \alpha \), let

\[ d(\alpha) = \text{the distance from } \alpha \text{ to the appropriate end of the diagram}. \]

Any two neighbours in the Dynkin diagram of the same length lie in the simple root system of a copy of \( SL_3 \).

The following is hence a consequence of Proposition 4.8:

**4.11. Corollary.** For \( \alpha \) in \( \Delta \) let \( e_\alpha = (-1)^{d(\alpha))}. \) Then

\[ e_\alpha = e_\alpha, \quad \sigma_\alpha = \alpha^\gamma (e_\alpha)^\theta s_\alpha. \]

Here, I recall, \( \sigma_\alpha \) is the element of \( N_E(T) \) associated by Tits' scheme to the choice of \( e_\alpha \) as basis of \( g_\alpha \) (or of \( e_{-\alpha} \) for \( g_{-\alpha} \)).

5. Computation II

As an immediate consequence of Theorem 4.9:

**5.1. Proposition.** Given the Kottwitz basis \((e_\gamma)\), and \( \gamma > 0 \), define

\[ f_{\gamma} = \begin{cases} e_\gamma & \text{if } \lambda > 0, \\ (-1)^{\text{ht}(\gamma) - 1} \cdot e_\gamma & \text{otherwise.} \end{cases} \]

Then \((f_\gamma)\) is an invariant integral basis.

**Remark.** Admittedly, there is something bizarre about this business. We start with a given frame, then find a new frame that is almost always not the same as the original. It is this new frame that we extend to an integral basis in a uniquely determined way.
Let \( w \) be the corresponding Tits section. It is convenient that \( w = \sigma \).

We must now figure out how to compute the constants \( c(s_\alpha, \lambda) \) for \( \lambda > 0 \) and \( \alpha \) in \( \Delta \) such that

\[
\sigma_\alpha \cdot \lambda = c(s_\alpha, \lambda) \cdot s_\alpha \lambda ,
\]

as promised in an earlier section. The following result encapsulates the basic reason why Kottwitz’ basis makes computation simple. Recall that

\[
c_\alpha = (-1)^d(\alpha),
\]

where \( d(\alpha) \) measures distance along the Dynkin diagram from selected endpoints.

5.2. Proposition. Suppose \( \alpha \) in \( \Delta \), \( s_\alpha \lambda = \mu \). If

\[
m_{\alpha, \lambda} = (-1)^{\langle \lambda, \alpha \rangle} c_{\alpha}^{\langle \lambda, \alpha^\vee \rangle}
\]

then

\[
c(s_\alpha, \lambda) = \begin{cases} m_{\alpha, \lambda} & \text{if } \lambda > 0 \\ m_{\alpha, -\lambda} & \text{otherwise.} \end{cases}
\]

Proof. Since \( \lambda(\alpha^\vee(x)) = x^{\langle \lambda, \alpha^\vee \rangle} \):

\[
s_\alpha \cdot e_\lambda = e_\mu = (-1)^{\langle \lambda, \alpha \rangle} s_\alpha \cdot e_\lambda \quad \text{(definition)}
\]

\[
s_\alpha \cdot e_\lambda = c_{\alpha}^{\langle \lambda, \alpha^\vee \rangle} \cdot e_\lambda
\]

\[
= m_{\alpha, \lambda} \cdot e_\mu. \quad \text{(Corollary 4.11)}
\]

This concludes when \( \lambda > 0 \)—even if \( \lambda = \alpha \) and \( \sigma_\alpha \cdot f_\alpha = f_{-\alpha} \). When not, apply the involution \( \theta \) to this equation, noting that \( \sigma_\alpha \) commutes with it.

Example. Look at \( \text{SL}_3 \) again. What is \( \left[ e_\alpha, e_\beta \right] \)?

\[
c_\alpha = 1
\]

\[
\langle \beta, \alpha^\vee \rangle = -1
\]

\[
\langle \alpha, \beta \rangle = 0
\]

\[
p_{\alpha, \beta} = 0
\]

\[
c(s_\alpha, \lambda) = 1
\]

Hence \( \left[ e_\alpha, e_\beta \right] = e_\gamma \).

Remark. It is not difficult to compute any \( p_{\lambda, \mu} \) by finding directly the maximum value of \( n \) such that \( \mu - n\lambda \) is a root. But this is more expensive in time than necessary. The circumstances in which we want to compute \( p_{\lambda, \mu} \) are in fact somewhat limited: (1) when \( \lambda = \alpha \) is simple and \( \langle \mu, \alpha^\vee \rangle = -1 \); (2) when \( \alpha \) is simple and \( \langle \mu, \alpha^\vee \rangle = 0 \); (3) \( \langle \lambda, \mu, \nu \rangle \) form a Tits triple. In case (1) or (2), we just have to check whether \( \mu - \alpha \) is a root. But if \( \alpha \) is simple, computing \( \mu - \alpha \) is trivial, a matter of decrementing one coordinate. In case (3), we can apply Proposition 2.5 in order to reduce to the case in which \( \langle \lambda, \mu, \nu \rangle \) is an ordered triple. These are dealt with in the process of ascending the root tree that is mentioned at the end of §3, since \( p_{s_\alpha \lambda, s_\alpha \mu} = p_{\lambda, \mu} \).
6. References


