WARWICK
THE UNIVERSITY OF WARWICK

A Thesis Submitted for the Degree of PhD at the University of Warwick

Permanent WRAP URL:
http://wrap.warwick.ac.uk/109521/

Copyright and reuse:
This thesis is made available online and is protected by original copyright.
Please scroll down to view the document itself.
Please refer to the repository record for this item for information to help you to cite it.
Our policy information is available from the repository home page.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

warwick.ac.uk/lib-publications

Affine Kac-Moody Groups:
Bounded Presentations and Subgroup Growth

by

Karina Kirkina

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Mathematics Institute

July 2018

THE UNIVERSITY OF WARWICK

Contents

Acknowledgments

First and foremost I would like to thank my supervisors, Dmitriy Rumynin and Inna Capdeboscq, for their endless patience and guidance.

I would like to thank my parents for all their support and encouragement. My friends outside Warwick, in London and beyond, have been a great source of warmth and diversion, and I wish to thank them all.

Warwick has been a wonderful place to study, and I would like to thank all the friends I met here, and members of faculty, for making the atmosphere so exciting.

Finally I would like to thank the examiners for their time and insightful suggestions.

Declarations

The introductory material and background results in this thesis are taken from various books and papers. These are referenced in the text. The remainder of the content is, to the best of my knowledge, original.

The original material in this thesis is based on two papers co-authored with my supervisors Inna Capdeboscq and Dmitriy Rumynin:

- *Subgroup growth in some profinite Chevalley groups*, Proc. Amer. Math. Soc., **145** (2017), no. 10, 4187 – 4200 ([CKR17])
- *Presentations of affine Kac-Moody groups*, preprint (2016), arXiv:1609.02464 ([CKR17a]).

Abstract

This thesis studies affine Kac-Moody groups $\widetilde{\mathbf{G}}(q)$ defined over a finite field $\mathbb{F}_q$, where q is a power of a prime p, and the related Chevalley groups $\mathbf{G}(\mathbb{F}_p([[t]])$. The groups $\widetilde{\mathbf{G}}(q)$ are finitely presented but their standard presentation is infinite. In the first half of the thesis we construct bounded presentations for these groups. The second half of the thesis studies the subgroup growth of the congruence subgroups of $\mathbf{G}(\mathbb{F}_p([[t]])$, which are examples of pro-p groups.

Chapter 1

Introduction

The objects studied in this thesis originated with the study of Lie groups and Lie algebras at the end of the 19th century. This was done by, among others, Lie, Killing and Cartan, and followed in the 20th century by the work of Dynkin. Lie theory and the study of finite simple groups naturally led to the study of the simple groups of Lie type. In the 50s Chevalley groups over fields were introduced in [Che55] as a way to systematically construct these groups, and the more general theory of linear algebraic groups was developed by, among others, Kolchin and Borel. In the 60s, Steinberg extended the notion of Chevalley groups and defined them using an explicit presentation (cf. [St62],[St68]), Demazure used the newly developed theory of group schemes to define Chevalley groups over rings (cf. [D65]), and infinite dimensional analogues of simple complex Lie algebras were defined by Serre, Kac and Moody (see [Kac83]). In analogy with simple algebraic groups associated with simple Lie algebras, in [Ti87] Tits defined groups over arbitrary fields associated with Kac-Moody algebras, called Kac-Moody groups. These groups are in general infinite and infinite dimensional.

The first half of this thesis is concerned with presentations of Kac-Moody groups. Let G be a group given by a presentation $\sigma = \langle D_\sigma \mid R_\sigma \rangle$ where D_σ is a set of generators for G and R_σ is a set of relations among these generators. Recall that G is said to be **finitely generated** if D_σ is finite for some presentation σ of G. If both D_σ and R_σ are finite we say that σ is a **finite presentation**, and we denote its **length** by

$$l(\sigma) := |D_\sigma| + |R_\sigma|.$$

We say that G is **finitely presented** if $l(\sigma)$ is finite for some presentation σ of G.

An explicit presentation of Kac-Moody groups using generators and relations was given by Carter and Chen (cf. [Car92], [CarCh93]). This presentation was modelled on the Steinberg presentation of Chevalley groups and is in general infinite:

both the number of generators and the number of relations are infinite. In this thesis we will be considering affine Kac-Moody groups $\widetilde{\mathbf{G}}(q)$ defined over finite fields $\mathbb{F}_q$, where q is a power of a prime. From the definition of these groups (see Chapter 2) it follows that they are finitely generated. Abramenko and Mühlherr [AbrM97] proved that a large class of Kac-Moody groups are in fact also finitely presented. This includes most of the affine Kac-Moody groups $\widetilde{\mathbf{G}}(q)$. Their proof is based on showing that under certain conditions a Kac-Moody group is the universal completion of an amalgam of rank two (Levi) subgroups (as they are arranged inside the group itself). Recall that for simply connected Kac-Moody groups these are just certain subgroups isomorphic to the finite groups $\mathrm{SL}\,(3,q)$, $\mathrm{Sp}\,(4,q)$ or $\mathrm{G}_2(q)$. So the presentation of the whole group can be pieced together from the finite presentations of these subgroups. In particular their paper concludes the following.

Theorem 1.1 (Abramenko, Mühlherr)**.** *Let G denote a Kac-Moody group over a finite field $\mathbb{F}_q$. Let $M = (m_{ij})_{i,j \in I}$ be the associated Coxeter matrix and let $m = \max\{m_{ij} \mid i, j \in I\}$. Suppose that $m < \infty$, $q \geq 3$ if $m = 4$ and that $q \geq 4$ if $m = 6$. Then G has a finite presentation.*

We will define Coxeter matrices associated to Kac-Moody groups in Charter 2. The definition implies that the only groups $\widetilde{\mathbf{G}}(q)$ excluded from the above theorem are those of types $\widetilde{A}_1$ and $\widetilde{A}'_1$, since these types both have $m = \infty$.

Recently there have been several papers showing that various infinite families of finitely presented groups have **bounded presentations**, that is presentations with a bounded number of generators and relations, with this bound being universal for the whole family. These papers prove the following type of result.

Let $\mathcal{A}$ be a certain family of groups. There exists $C > 0$ such that for any group $G \in \mathcal{A}$, G admits a presentation $\sigma(G) = \langle D_{\sigma(G)} \mid R_{\sigma(G)} \rangle$ such that

$$l(\sigma(G)) = |D_{\sigma(G)}| + |R_{\sigma(G)}| < C.$$

This result is known if the family $\mathcal{A}$ is a family of finite simple groups [GKaKasL07, GKaKasL08, GKaKasL11], a family of Chevalley groups over various rings [CLRe16], and a family of affine Kac-Moody groups defined over finite fields [C13]. The latter paper proves the following result.

Theorem 1.2 (Capdeboscq, [C13] Theorem 2.1)**.** *There exists $C > 0$ such that if $G = \widetilde{\mathbf{G}}(q)$ is an affine Kac-Moody group corresponding to an indecomposable generalized Cartan matrix A and defined over a finite field $\mathbb{F}_q$, $q \geq 4$, and if G has rank $l \geq 3$, then G has a presentation σ with $l(\sigma) \leq C$.*

In Chapter 2 we will see that the rank $l \geq 3$ requirement again only excludes the groups $\widetilde{A}_1(q)$ and $\widetilde{A}'_1(q)$.

After proving the existence of bounded presentations for a certain family of groups, the next natural step is to find a numerical bound on C for these groups. Guralnick, Kantor, Kassabov and Lubotzky [GKaKasL07, GKaKasL11] do this in the case when $\mathcal{A}$ is a family of finite simple groups (with the possible exception of ${}^2G_2(q)$. They prove the following result.

Theorem 1.3 ([GKaKasL11], Theorem A)**.** *All finite quasisimple groups, with the possible exception of the Ree groups ${}^2G_2(3^{2e+1})$, have presentations with at most 2 generators and 51 relations.*

The third chapter of this thesis finds a numerical bound on C for the Kac-Moody groups $\widetilde{\mathbf{G}}(q)$, establishing a value of 75. Namely, we obtain the following result.

Theorem A. *Let G be a simply connected affine Kac-Moody group of rank $l \geq 3$ defined over a finite field $\mathbb{F}_q$. If $q \geq 4$, then G has a presentation with 2 generators and at most 73 relations.*

The result also holds if $q \in \{2, 3\}$ provided that the Dynkin diagram of G is not of type $\tilde{A}_2$ and does not contain a subdiagram of type B_2 or G_2 for $q = 2$, and of type G_2 for $q = 3$. If $G = \widetilde{A}_2(2)$ or $\widetilde{A}_2(3)$, G has a presentation with at most 3 generators and 29 relations.

The upper bound of 73 in this theorem comes from the groups of type $\widetilde{C}^t_n(q)$. We obtain better bounds for the other types, as stated in the next theorem.

Theorem B. *Let G be a simply connected affine Kac-Moody group of rank $l \geq 3$ defined over a finite field $\mathbb{F}_q$. If $q \geq 4$, G has a presentation $\sigma_G = \langle D_\sigma \mid R_\sigma \rangle$ where $|D_\sigma|$ and $|R_\sigma|$ are given in Table A.2.*

The result also holds if $q \in \{2, 3\}$ provided that the Dynkin diagram of G does not contain a subdiagram of type B_2 or G_2 for $q = 2$, and of type G_2 for $q = 3$.

This theorem is proved by using the results of Abramenko and Mühlherr from [AbrM97] to construct a presentation of $\widetilde{\mathbf{G}}(q)$ using presentations of its rank one and two subgroups, piecing together the results of Guralnick, Kantor, Kassabov and Lubotzky from [GKaKasL07], [GKaKasL08] and [GKaKasL11] giving explicit presentations and bounds on presentation lengths for finite simple and quasisimple groups, as well as using results about reducing the final presentation length. These results will be summarised in Chapter 3.

The second half of this thesis deals with the topic of subgroup growth in Chevalley groups over the ring $\mathbb{F}_p[[t]]$, where p is a prime. For a finitely generated group G, let $a_n(G)$ be the number of subgroups of G of index n and $s_n(G)$ the number of subgroups of G of index at most n. If G is a topological group, $a_n(G)$ is the number of *open* subgroups of index n, and similarly for $s_n(G)$. The topic of **subgroup growth** is concerned with the asymptotic behaviour of the sequences $(a_n(G))_{n\in\mathbb{N}}$ and $(s_n(G))_{n\in\mathbb{N}}$. In some cases we can derive information about the structure of G from knowledge of its subgroup growth.

For example, Lubotzky and Mann [LMa91] showed that a group G is so-called p-adic analytic if and only if there exists a constant $c > 0$ such that $a_n(G) < n^c$. Later Shalev proved that if G is a pro-p group for which $a_n(G) \leq n^{c \log_p n}$ for some constant $c < \frac{1}{8}$, then G is p-adic analytic. Mann then asked how big c could be so that all pro-p groups G for which $a_n(G) \leq n^{c \log_p n}$ were p-adic analytic. Barnea and Guralnick investigated this in [BG01] by looking at the subgroup growth of $SL_2^1(\mathbb{F}_p[[t]])$, the first congruence subgroup of $SL_2(\mathbb{F}_p[[t]])$, for $p > 2$, and showed that c could be no bigger than $\frac{1}{2}$. Thus it is not only the growth type, but also the precise values of the constants involved that matter when studying the connection between subgroup growth and the structure of a group.

Later Lubotzky and Shalev pioneered a study of the so-called Λ-standard groups [LSh94], where Λ is a local ring. A particular subclass of these groups are Λ-perfect groups for which they showed the existence of a constant $c > 0$ such that

$$a_n(G) < n^{c \log_p n}.$$

An important subclass of these groups consists of the congruence subgroups of Chevalley groups over $\mathbb{F}_p[[t]]$, which are $\mathbb{F}_p[[t]]$-perfect. Let $\mathbf{G}$ be a simple simply connected Chevalley group scheme and G_1 the first congruence subgroup of $\mathbf{G}(\mathbb{F}_p[[t]])$. Abért, Nikolov and Szegedy established a precise value for the constant c for these groups in the following result.

Theorem 1.4 ([AbNS03], Theorem 2)**.** *Let m be the dimension of $\mathbf{G}$. Then*

$$s_{p^k}(G_1) \leq p^{\frac{7}{2}k^2 + mk}.$$

Another way of stating this is $s_n(G_1) \leq n^{\frac{7}{2}\log_p n + m}$.

The second half of this thesis is concerned with improving this estimate. We do this by defining a new parameter of the Lie algebra $\mathfrak{g}$ of $\mathbf{G}$ called the ridgeline number $v(\mathfrak{g})$. Using this we prove the following result, which is valid for certain characteristics that we call very good or tolerable.

Theorem C. *Let $\mathbf{G}$ be a simple simply connected Chevalley group scheme of rank $l \geq 2$. Suppose p is a tolerable prime for $\mathbf{G}$. Let G_1 be the first congruence subgroup* *of* $\mathbf{G}(\mathbb{F}_p[[t]])$*, that is* $G_1 = \ker(\mathbf{G}(\mathbb{F}_p[[t]]) \twoheadrightarrow \mathbf{G}(\mathbb{F}_p))$*. If* $m := \dim \mathbf{G}$*, then*

$$a_{p^k}(G_1) \leq p^{\frac{(3+4v(\mathfrak{g}))}{2}k^2+(m-\frac{3}{2}-2v(\mathfrak{g}))k}.$$

If $l = 2$ *and* p *is very good, then a stronger estimate holds:*

$$a_{p^k}(G_1) \leq p^{\frac{3}{2}k^2+(m-\frac{3}{2})k}.$$

The biggest possible value of $v(\mathfrak{g})$ is $\frac{2}{3}$ (cf. Appendix A.6) so this makes $\frac{3+4v(\mathfrak{g})}{2} \leq \frac{17}{6} < \frac{7}{2}$.
Our proof of Theorem C follows the ones of Barnea and Guralnick and of Abért, Nikolov and Szegedy. The improvement in the result is due to the following new estimates.

Theorem D. *Let* $\mathfrak{a}$ *be a Lie algebra over a field* $\mathbb{K}$*. Suppose that the Lie algebra* $\mathfrak{g} = \mathfrak{a} \otimes_{\mathbb{K}} \overline{\mathbb{K}}$ *is a Chevalley Lie algebra of rank* $l \geq 2$ *and that the characteristic of* $\mathbb{K}$ *is zero or tolerable. Then for any two subspaces* U *and* V *of* $\mathfrak{a}$*, we have*

$$\operatorname{codim}([U,V]) \leq (1 + v(\mathfrak{g}))(\operatorname{codim}(U) + \operatorname{codim}(V)).$$

If $l = 2$ *and the characteristic of* $\mathbb{K}$ *is zero or very good, a stronger result holds:*

$$\operatorname{codim}([U,V]) \leq \operatorname{codim}(U) + \operatorname{codim}(V).$$

The thesis is structured as follows.
Chapter 2 covers the basics of the groups involved. Each subsequent chapter starts with a section of preliminaries, which summarises the background results we will need to use.
Chapter 3 studies the bounded presentations of the affine Kac-Moody groups $\widetilde{\mathbf{G}}(q)$.
Chapter 4 deals with the subgroup growth of the first congruence subgroup of the Chevalley groups $\mathbf{G}(\mathbb{F}_p[[t]])$.
Chapter 5 includes a partial solution to the problem of determining the subgroup growth of the twisted analogues of the groups from Chapter 4.
Appendix A contains various tables that we construct or use in the thesis. Appendix B provides a short example of a MAGMA calculation necessary for one of the proofs in Chapter 4. Finally Appendix C contains a list of affine Dynkin diagrams and generalised Cartan matrices.

Chapter 2

Preliminaries

In this chapter we introduce the basics of the groups we are working with - affine Kac-Moody groups over finite fields and Chevalley groups over $\mathbb{F}_p([[t]])$, and explain how these are related to each other. Each later chapter will have a section of preliminaries to define the basic notions needed there.
References to results will be directly indicated. The material here is largely taken from the books by Kac [Kac83] and Carter [Car05], and Rammage's thesis [Ra92].

2.1 Chevalley groups

We begin by briefly reminding the reader of the construction of Chevalley groups. See for example [Car72] for details of the construction over fields, and [PVa96] or [A69] for details over commutative rings. There are different versions of Chevalley groups, according to different so-called isogeny types. Two examples of these are the adjoint Chevalley groups and the simply connected Chevalley groups.
In what follows we will mainly be looking at the first congruence subgroup of Chevalley groups over $\mathbb{F}_p([[t]])$. Note that the congruence subgroups are kernels of certain homomorphisms, and that the differences between the isogeny types are preserved in the images of these homomorphisms. In other words, the kernels for the different types of Chevalley groups coincide, so the distinction makes no difference for our purposes. Hence we can afford to be somewhat vague here. We start by defining the adjoint Chevalley groups.

Let $\mathfrak{g}$ be a simple finite dimensional Lie algebra over $\mathbb{C}$. Let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$, and let Φ be the set of roots with respect to $\mathfrak{h}$. The Lie algebra $\mathfrak{g}$ admits a root decomposition $\mathfrak{g} = \mathfrak{h} \oplus \sum \mathfrak{l}_\alpha$, where the $\mathfrak{l}_\alpha$ are the root subspaces. We choose an order on Φ and let Φ^+, Φ^- and $\Pi = \{\alpha_1, \ldots, \alpha_l\}$ denote the sets of positive, negative and fundamental roots, respectively. We denote by $(,)$ the restriction of the Killing form of $\mathfrak{g}$ on $\mathfrak{h}$, which is nondegenerate, so allows us to

identify $\mathfrak{h}$ with $\mathfrak{h}^*$. For each root α we define a corresponding coroot $h_\alpha \in \mathfrak{h}$ as follows: $h_\alpha := 2\alpha/(\alpha, \alpha)$. We pick elements $e_\alpha \in \mathfrak{l}_\alpha$ and $e_{-\alpha} \in \mathfrak{l}_{-\alpha}$ such that $[e_\alpha, e_{-\alpha}] = h_\alpha$.
This gives us a basis

$$\{e_\alpha, \alpha \in \Phi \; ; \; h_\alpha, \alpha \in \Pi\}$$

of $\mathfrak{g}$. It is possible to choose the elements e_α carefully so that the structure constants with respect to this basis are integers. Such a choice is called a **Chevalley basis**.
Let $\mathfrak{g}_\mathbb{Z}$ be the integral span of a Chevalley basis and let R be a commutative ring. Set $\mathfrak{g}_R = \mathfrak{g}_\mathbb{Z} \otimes_\mathbb{Z} R$. Then $\mathfrak{g}_R$ is a Lie algebra over R, which as an R-module is a free module, with the basis $\bar{e}_\alpha = e_\alpha \otimes 1$, $\bar{h}_\beta = h_\beta \otimes 1$, and Lie bracket given by $[\bar{e}_\alpha, \bar{h}_\beta] = [e_\alpha, h_\beta] \otimes 1$. The Lie algebra $\mathfrak{g}_R$ is called the **Chevalley Lie algebra** of type Φ over R.
If D is a nilpotent derivation of the Lie algebra $\mathfrak{g}$, where $D^n = 0$, then it can be shown that $\exp(D) = 1 + D + \frac{D^2}{2} + \ldots + \frac{D^{n-1}}{(n-1)!}$ is an automorphism of $\mathfrak{g}$. It is known that the adjoint maps $\operatorname{ad} e_\alpha$ are nilpotent derivations of $\mathfrak{g}$. If $\xi \in \mathbb{C}$, we have that $\operatorname{ad}(\xi e_\alpha) = \xi \operatorname{ad} e_\alpha$ is also a nilpotent derivation, so we can define

$$x_\alpha(\xi) := \exp(\xi \operatorname{ad} e_\alpha).$$

These are then automorphisms of $\mathfrak{g}$. It can be shown that the elements $x_\alpha(\xi)$ act on the Chevalley basis as follows.

$$\begin{aligned}
x_\alpha(\xi)(e_\alpha) &= e_\alpha \\
x_\alpha(\xi)(h_\alpha) &= h_\alpha - 2\xi e_\alpha \\
x_\alpha(\xi)(e_{-\alpha}) &= e_{-\alpha} + \xi h_\alpha - \xi^2 e_\alpha \\
x_\alpha(\xi)(h_\beta) &= h_\beta - A_{\beta\alpha} \xi e_\alpha \\
x_\alpha(\xi)(e_\beta) &= e_\beta + M_{\alpha\beta 1} \xi e_{\alpha+\beta} + M_{\alpha\beta 2} \xi^2 e_{\beta+2\alpha} + \ldots + M_{\alpha\beta k} \xi^k e_{\beta+k\alpha}.
\end{aligned}$$

Here α and β are assumed to be linearly independent, and the numbers $A_{\beta\alpha}$, k and $M_{\alpha\beta k}$ are certain integers. So the automorphisms $x_\alpha(\xi)$ send each element of the Chevalley basis to a linear combination of basis elements whose coefficients are integer multiples of nonnegative powers of ξ. This allows us to define automorphisms $x_\alpha(\xi)$ of $\mathfrak{g}_R$, where R is an arbitrary commutative ring, and $\xi \in R$.
The group of automorphisms of $\mathfrak{g}_R$ generated by all the automorphisms of the form $x_\alpha(\xi)$ is called the **elementary adjoint Chevalley group** of type Φ over R.

The more sophisticated approach to Chevalley groups uses group schemes. Broadly speaking, for a commutative ring R and a Dynkin diagram of type X, there are several Chevalley-Demazure group functors taking the ring R to a group $\mathbf{G}^X(R)$.

We note that we get different groups $\mathbf{G}^X(R)$ for different functors.
For example the simply connected functor with Dynkin diagram of type A_n is isomorphic to the functor

$$\mathbf{SL_{n+1}} : R \mapsto SL_{n+1}(R)$$

(taking ring homomorphisms to the corresponding group homomorphisms).
The knowledge that these functors exist will be sufficient for our purposes.

2.2 Generalised Cartan matrices

Now we begin to define Kac-Moody groups, and the first step towards this is generalising the definition of a Cartan matrix.

Definition 2.1. Let I be a finite set. A **generalised Cartan matrix** (abbreviated **GCM**) is a matrix $A = (A_{ij})_{i,j\in I}$ with integer coefficients such that $A_{ii} = 2$, $A_{ij} \leq 0$ if $i \neq j$ and $A_{ij} = 0$ if and only if $A_{ji} = 0$.

Ordinary Cartan matrices are examples of GCMs. GCMs can be classified into three types, namely **finite**, **affine** or **indefinite** (cf. [Car05] Theorem 15.1). The ones of finite type are Cartan matrices and precisely the ones that lead to finite dimensional Lie algebras, whereas the other two lead to infinite dimensional ones.
Two GCMs are said to be **equivalent** when we can obtain one from the other by relabelling the indices of the rows and columns. A GCM is said to be **indecomposable** if it is not equivalent to the diagonal sum of two smaller GCMs. Recall that a **submatrix** of a matrix is a matrix obtained by deleting some rows and columns of the matrix, a **minor** is a determinant of some square submatrix of the matrix, a **principal submatrix** is a submatrix obtained by deleting the i-th row if and only if one deletes i-th column, a **principal minor** is a determinant of some principal submatrix of the matrix, and a **proper principal minor** is a principal minor that is not the determinant of the whole matrix.
The following result allows us to determine the type of a GCM.

Proposition 2.2 ([Car05] Theorem 15.18)**.** *Let A be an indecomposable GCM. Then*

(i) A is of finite type if and only if all of its principal minors are positive.

(ii) A is of affine type if and only if det A = 0 and all of its proper principal minors are positive.

(iii) A is of indefinite type in all other cases.

Definition 2.3. Let $A = (A_{ij})_{i,j\in I}$ be a GCM. We define the **rank** of A to be its dimension, i.e. the cardinality of the indexing set I.

Note that this rank is not necessarily equal to the rank of A as a matrix. Indeed, Proposition 2.2 says that if A is of finite or indefinite type, then it is nonsingular, so it has full rank. Hence its dimension, GCM rank and matrix rank all coincide. Whereas if A is of affine type, then A is singular but all of its proper submatrices are nonsingular, so A has corank 1 as a matrix. We will usually denote this matrix rank by n, and the GCM rank by l, so then A has dimensions $(n+1)\times(n+1)$ and we have $l = n + 1$. Which rank we are referring to will usually be clear from context, or explicitly specified.

In what follows we will be concentrating on the affine case. It is well known that finite GCMs (i.e. ordinary Cartan matrices) have been completely classified in the Cartan-Killing classification. Similarly, affine GCMs have also been completely classified (cf. [Car05] Theorem 15.23). There are, up to equivalence, 7 infinite families as follows

$$\widetilde{A}_n\,(n \geq 2),\;\; \widetilde{B}_n\,(n \geq 3),\;\; \widetilde{C}_n\,(n \geq 2),\;\; \widetilde{D}_n\,(n \geq 4),\;\; \widetilde{B}^t_n\,(n \geq 3),\;\; \widetilde{C}'_n\,(n \geq 2),\;\; \widetilde{C}^t_n\,(n \geq 2),$$

as well as the following 9 exceptional cases

$$\widetilde{A}_1,\quad \widetilde{E}_6,\quad \widetilde{E}_7,\quad \widetilde{E}_8,\quad \widetilde{F}_4,\quad \widetilde{G}_2,\quad \widetilde{A}'_1,\quad \widetilde{F}^t_4,\quad \widetilde{G}^t_2.$$

Note that the subscript n in the name again denotes the ordinary rank of the matrix.

Example 2.4. A possible representative for the Cartan matrix (or finite GCM) of type G_2 is the following 2×2 matrix with matrix rank $n = 2$ and GCM rank $l = 2$.

$$\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}.$$

And a representative for the affine GCM $\widetilde{G}_2$ is the following 3×3 matrix of ordinary matrix rank $n = 2$ and GCM rank $l = 2 + 1 = 3$.

$$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -3 & 2 \end{pmatrix}.$$

We list representatives for each type of affine GCM in Appendix C.

Note that the bottom right 2×2 submatrix in the $\widetilde{G}_2$ example above is equal to the Cartan matrix of type G_2. This is a special case of a general phenomenon: the affine GCMs of types

$$\widetilde{A}_n\,(n \geq 1),\;\; \widetilde{B}_n\,(n \geq 3),\;\; \widetilde{C}_n\,(n \geq 2),\;\; \widetilde{D}_n\,(n \geq 4),\;\; \widetilde{E}_6,\;\; \widetilde{E}_7,\;\; \widetilde{E}_8,\;\; \widetilde{F}_4,\;\; \widetilde{G}_2$$

are called **extended Cartan matrices** (or affine GCMs of **untwisted type**) because they can be obtained from the ordinary Cartan matrices via the following process. We start with an ordinary indecomposable Cartan matrix $A = (A_{ij})_{i,j \in I}$, where $I = \{1, \ldots, n\}$. Let $\mathfrak{g}$ be the finite dimensional simple Lie algebra over $\mathbb{C}$ with Cartan matrix A. We construct a matrix $\widetilde{A}$ from A by adding an extra row and column, indexed by 0. Let $\{\alpha_i\}_{i \in I}$ be the simple roots of $\mathfrak{g}$ and let $\{h_i\}_{i \in I}$ be the simple coroots. Let $\theta = \sum_{i=1}^n a_i \alpha_i$ be the highest root of $\mathfrak{g}$ and let $h_\theta = \sum_{i=1}^n c_i h_i$ be the coroot of θ. Now we define $\widetilde{A}$ by:

$$\begin{aligned}
\widetilde{A}_{ij} &= A_{ij} \quad \text{if } i, j \in \{1 \ldots n\} \\
\widetilde{A}_{i0} &= -\sum_{j=1}^n a_j A_{ij} \quad \text{if } i, j \in \{1 \ldots n\} \\
\widetilde{A}_{0j} &= -\sum_{i=1}^n c_i A_{ij} \quad \text{if } i, j \in \{1 \ldots n\} \\
\widetilde{A}_{00} &= 2.
\end{aligned}$$

The remaining affine GCMs are said to be of **twisted type**. These are the following matrices.

$$\widetilde{A}'_1, \;\; \widetilde{B}^t_n\,(n \geq 3), \;\; \widetilde{C}'_n\,(n \geq 2), \;\; \widetilde{C}^t_n\,(n \geq 2), \;\; \widetilde{F}^t_4, \;\; \widetilde{G}^t_2.$$

2.3 Kac-Moody data, the Weyl group and roots

Definition 2.5. A **Kac-Moody datum** $\mathcal{D}$ associated to a GCM $A = (A_{ij})_{i,j \in I}$ is a 6-tuple

$$\mathcal{D} = (I, A, \mathcal{X}, \mathcal{Y}, \{\alpha_i\}_{i \in I}, \{\alpha_i^\vee\}_{i \in I}),$$

where I is a finite indexing set with $|I| = n$, $\mathcal{X}$ is a finitely generated free abelian group with $\mathbb{Z}$-dual $\mathcal{Y}$, $\alpha_i \in \mathcal{X}$, $\alpha_i^\vee \in \mathcal{Y}$, such that $\alpha_j(\alpha_i^\vee) = A_{ij}$.

The set $\Pi = \{\alpha_i\}$ is called the set of **simple roots**, while the set $\Pi^\vee = \{\alpha_i^\vee\}$ is called the set of **simple coroots**.

Definition 2.6. The root datum $\mathcal{D}$ is called **simply connected** if the simple coroots form a basis for $\mathcal{Y}$, i.e. if we have

$$\mathcal{Y} = \bigoplus_{i \in I} \mathbb{Z}\alpha_i^\vee.$$

Definition 2.7. The root datum $\mathcal{D}$ is called **adjoint** if the simple roots form a basis for $\mathcal{X}$, i.e. if we have

$$\mathcal{X} = \bigoplus_{i \in I} \mathbb{Z}\alpha_i.$$

Definition 2.8. The **Coxeter matrix** $M = (m_{ij})_{i,j\in I}$ associated to a generalised Cartan matrix $A = (A_{ij})_{i,j\in I}$ is given by: $m_{ii} = 1$ and if $i \neq j$ then $m_{ij} = 2, 3, 4, 6$ or ∞ as $A_{ij}A_{ji} = 0, 1, 2, 3$ or is ≥ 4.

Using the Coxeter matrix we define the associated **Weyl group** to be the reflection group with presentation based on the entries of M:

$$W = \langle \{w_i\} \mid (w_i w_j)^{m_{ij}} \text{ for } m_{ij} \neq \infty \rangle.$$

Note that the w_i are elements of order two since w_i^2 will always be a relator.

The Weyl group acts on $\mathcal{X}$ via the maps $w_i : \beta \mapsto \beta - \beta(\alpha_i^\vee) \cdot \alpha_i$ for each $\beta \in \mathcal{X}$ and $i \in I$. So in particular we see that if β is a simple root α_j we have

$$w_i(\alpha_j) = \alpha_j - \alpha_j(\alpha_i^\vee) \cdot \alpha_i = \alpha_j - A_{ij}\alpha_i$$

and w_i applied to the corresponding root α_i gives us

$$w_i(\alpha_i) = \alpha_i - \alpha_i(\alpha_i^\vee) \cdot \alpha_i = \alpha_i - 2\alpha_i = -\alpha_i.$$

The set of **real roots** Φ is defined by

$$\Phi = W \cdot \Pi.$$

In general, the Weyl group and set of real roots are infinite. The term real root comes from the fact that Kac-Moody theory also has so-called imaginary roots, which we will not need here. Each element of Φ is a $\mathbb{Z}$-linear combination of elements of Π with coefficients all ≥ 0 or all ≤ 0. We define Φ^+, the set of **positive real roots**, as the subset of Φ for which all coefficients are ≥ 0 and Φ^-, the set of **negative real roots**, as the subset for which all coefficients are ≤ 0. We have

$$\Phi = \Phi^+ \sqcup \Phi^-.$$

2.4 Dynkin diagrams

We now introduce the concept of a Dynkin diagram associated to a GCM.

Definition 2.9. Let $A = (A_{ij})_{i,j\in I}$ be a GCM. The **Dynkin diagram** of A, written $\Delta(A)$, is a graph defined as follows.
The graph has $|I|$ vertices, each corresponding to one of the simple roots.
If $A_{ij}A_{ji} \leq 4$ and $|A_{ij}| \geq |A_{ji}|$, the vertices i and j are connected by $|A_{ij}|$ lines, and

these lines are equipped with an arrow pointing from j to i if $|A_{ij}| > 1$.
If $A_{ij}A_{ji} > 4$, the vertices i and j are connected by a bold-faced edge indexed by an ordered pair of integers $|A_{ij}|, |A_{ji}|$.

Note that we always have $A_{ij}A_{ji} \leq 4$ for GCMs of finite and affine type. From the definition it follows that $\Delta(A)$ is a connected graph if and only if A is an indecomposable GCM. We also note that A is determined by the Dynkin diagram $\Delta(A)$ and an enumeration of its vertices. If A is of finite, affine or indefinite type, then we say $\Delta(A)$ is as well.
We list all connected Dynkin diagrams of affine type in Appendix C.

2.5 Minimal Kac-Moody groups

Definition 2.10. Two roots α and β in Φ are said to be **prenilpotent** if there exist $w, w' \in W$ such that $w(\alpha) \in \Phi_+$, $w(\beta) \in \Phi_+$, $w'(\alpha) \in \Phi_-$ and $w'(\beta) \in \Phi_-$.

Note that in the finite case all non-opposite pairs of roots are prenilpotent.

We can now define the minimal Kac-Moody group associated to a Kac-Moody datum, over an arbitrary field $\mathbb{K}$. We define this group using a set of generators and relations. There are several versions of this group corresponding to different types of root data. The version constructed below is the simply connected version of the group. It is called minimal to contrast it from the maximal or topological versions of the group.

Definition 2.11. Let $\mathcal{D} = (I, A, \mathcal{X}, \mathcal{Y}, \{\alpha_i\}_{i\in I}, \{\alpha_i^\vee\}_{i\in I})$ be a simply connected Kac-Moody datum and $\mathbb{K}$ a field. The associated **minimal** or **incomplete Kac-Moody group $\mathbf{G}_{\mathcal{D}}(\mathbb{K})$** over $\mathbb{K}$ is generated by **root subgroups**

$$U_\alpha = U_\alpha(\mathbb{K}) = \langle x_\alpha(t) \mid t \in \mathbb{K}\rangle,$$

one for each real root $\alpha \in \Phi$.
For each $u \in \mathbb{K}$ and $i \in I$, we write $x_i(u)$ for $x_{\alpha_i}(u)$ and $x_{-i}(u)$ for $x_{-\alpha_i}(u)$. Let $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$. For each $u \in \mathbb{K}^\times$ and $i \in I$ we put

$$\tilde{w}_i(u) = x_i(u)x_{-i}(u^{-1})x_i(u)$$

$$\tilde{w}_i = \tilde{w}_i(1)$$

and

$$h_i(u) = \tilde{w}_i(u) \cdot \tilde{w}_i^{-1}.$$

A defining set of relations for $\mathbf{G}_{\mathcal{D}}(\mathbb{K})$ is then:

(i) $x_\alpha(t)x_\alpha(u) = x_\alpha(t+u)$ for all roots $\alpha \in \Phi$ and all $t, u \in \mathbb{K}$.

(ii) If $\alpha, \beta \in \Phi$ is a prenilpotent pair of roots, then for all $t, u \in \mathbb{K}$:

$$[x_\alpha(t), x_\beta(u)] = \prod_{i\alpha+j\beta\in\Phi\ ,\ i,j\in\mathbb{N}} x_{i\alpha+j\beta}(C_{ij\alpha\beta}t^i u^j)$$

where the $C_{ij\alpha\beta}$ are integers that are uniquely determined by $i, j, \alpha, \beta, \Phi$ and how the terms on the right hand side are ordered.

(iii) $h_i(t)h_i(u) = h_i(tu)$ for all $t, u \in \mathbb{K}^\times$ and $i \in I$.

(iv) $[h_i(t), h_j(u)] = 1$ for all $t, u \in \mathbb{K}^\times$ and $i, j \in I$.

(v) $h_j(u)x_i(t)h_j(u)^{-1} = x_i(u^{A_{ij}}t)$ for all $t \in k, u \in \mathbb{K}^\times$ and $i, j \in I$.

(vi) $\tilde{w}_i h_j(u)\tilde{w}_i^{-1} = h_j(u)h_i(u^{-A_{ij}})$ for all $u \in \mathbb{K}^\times$ and $i, j \in I$.

(vii) $\tilde{w}_i x_\alpha(u)\tilde{w}_i^{-1} = x_{w_i(\alpha)}(\epsilon u)$ where $\epsilon \in \{\pm 1\}$ for all $u \in \mathbb{K}$.

In what follows we will be considering Kac-Moody groups defined over finite fields, i.e. when $\mathbb{K} = \mathbb{F}_q$ where q is some power of a prime p.

Remark. We will use several different notations for these Kac-Moody groups, depending on context. If the root datum $\mathcal{D}$ is associated to a GCM A and the type of the root datum is implied, then we may use the shorter notation $\mathbf{G}^A(\mathbb{K})$ to refer to $\mathbf{G}_{\mathcal{D}}(\mathbb{K})$. We use the notation $\mathbf{G}^A_{sc}(\mathbb{K})$ ($\mathbf{G}^A_{ad}(\mathbb{K})$) if $\mathcal{D}$ is some simply connected (adjoint) root datum associated to A. If we want to refer to a general minimal Kac-Moody group of affine type we may use the notation $\widetilde{\mathbf{G}}(\mathbb{K})$, and if we have $\mathbb{K} = \mathbb{F}_q$ we use the shorter notation $\widetilde{\mathbf{G}}(q)$.
This notation is chosen to reflect the similarities with algebraic groups and Chevalley-Demazure group schemes. If highlighting these similarities is not necessary for the context, we will refer to the groups $\mathbf{G}_{\mathcal{D}}(\mathbb{F}_q)$ as $X(q)$ (or $\widetilde{X}(q)$ if we want to emphasise the fact that the groups are of affine type).

We explain more about the construction of Kac-Moody groups, and in particular of the ones that are not simply connected, in Section 3.6.

2.6 Chevalley groups over $\mathbb{F}_p[[t]]$

Let p be a prime. We summarise the main features of the ring $\mathbb{F}_p[[t]]$, the **ring of formal power series** with coefficients in $\mathbb{F}_p$. It consists of the set of formal expressions of the form

$$\sum_{i=0}^{\infty} a_i t^i = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \dots,$$

where the coefficients a_i are in the field $\mathbb{F}_p$, together with addition defined by

$$\sum_{i=0}^{\infty} a_i t^i + \sum_{i=0}^{\infty} b_i t^i = \sum_{i=0}^{\infty} c_i t^i \quad \text{where} \quad c_i = a_i + b_i$$

and multiplication given by

$$\sum_{i=0}^{\infty} a_i t^i \cdot \sum_{i=0}^{\infty} b_i t^i = \sum_{j=0}^{\infty} c_j t^j \quad \text{where} \quad c_j = \sum_{i=0}^{j} a_i b_{j-i}.$$

$\mathbb{F}_p[[t]]$ is a local ring. Its unique maximal ideal is $t\mathbb{F}_p[[t]]$, the set of formal power series with zero constant term. We have $\mathbb{F}_p[[t]]/(t\mathbb{F}_p[[t]]) \cong \mathbb{F}_p$. There is a canonical surjective ring homomorphism from $\mathbb{F}_p[[t]]$ to the quotient $\mathbb{F}_p[[t]]/(t\mathbb{F}_p[[t]])$ - it maps each expression $\sum_{i=0}^{\infty} a_i t^i$ in $\mathbb{F}_p[[t]]$ to its first coefficient a_0.
Any subset of form $t^n\mathbb{F}_p[[t]]$ is an ideal of $\mathbb{F}_p[[t]]$. It consists of the formal power series where the coefficients $a_0, a_1, \dots a_{n-1}$ are all zero. We have $\mathbb{F}_p[[t]]/(t^n\mathbb{F}_p[[t]]) \cong \mathbb{F}_p[t]/\langle t^n \rangle$. There is a canonical surjective ring homomorphism

$$\rho_n : \mathbb{F}_p[[t]] \twoheadrightarrow \mathbb{F}_p[[t]]/(t^n\mathbb{F}_p[[t]]),$$

mapping each expression $\sum_{i=0}^{\infty} a_i t^i$ in $\mathbb{F}_p[[t]]$ to its corresponding truncated polynomial $\sum_{i=0}^{n-1} a_i t^i$.
The ring of units of $\mathbb{F}_p[[t]]$ consists of the formal power series for which $a_0 \neq 0$.
The field of fractions of $\mathbb{F}_p[[t]]$ is

$$\mathbb{F}_p((t)) := \{\sum_{i=k}^{\infty} a_i t^i \mid k \in \mathbb{Z},\ a_i \in \mathbb{F}_p\},$$

the **field of formal Laurent series** over $\mathbb{F}_p$.

We can now form groups over $\mathbb{F}_p[[t]]$ via the Chevalley-Demazure group schemes. For each Dynkin diagram of type X, where $X \in \{A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2\}$, we thus obtain a group $\mathbf{G}^X(\mathbb{F}_p[[t]])$.

2.7 Congruence subgroups

The canonical surjective ring homomorphism $\rho_n : \mathbb{F}_p[[t]] \twoheadrightarrow \mathbb{F}_p[[t]]/(t^n\mathbb{F}_p[[t]])$ induces a surjective group homomorphism of Chevalley groups, which we by abuse of notation also call ρ_n:

$$\rho_n : \mathbf{G}^X(\mathbb{F}_p[[t]]) \twoheadrightarrow \mathbf{G}^X(\mathbb{F}_p[[t]]/(t^n\mathbb{F}_p[[t]]).$$

Definition 2.12. The kernel of the homomorphisn ρ_n is called the **n-congruence subgroup** of $\mathbf{G}^X(\mathbb{F}_p[[t]])$. We denote this group by G_n.
In particular the **first congruence subgroup** of $\mathbf{G}^X(\mathbb{F}_p[[t]])$, G_1, is the kernel of the homomorphism

$$\rho : \mathbf{G}^X(\mathbb{F}_p[[t]]) \twoheadrightarrow \mathbf{G}^X(\mathbb{F}_p[[t]]/(t\mathbb{F}_p[[t]]) \cong \mathbf{G}^X(\mathbb{F}_p).$$

The first thing to note about these subgroups is that they are nested, that is that we have

$$G_1 \supseteq G_2 \supseteq G_3 \supseteq G_4 \dots$$

Another basic property of these groups is the following (see for example [BG01]).

Proposition 2.13. *For all $n, m \in \mathbb{N}$, we have $[G_n, G_m] \subseteq G_{n+m}$ and $G_n^p \subseteq G_{n+1}$.*

We will need this is Chapter 4 where we will construct a graded Lie algebra using successive quotients G_n/G_{n+1}. The above proposition implies that $[G_n, G_n] \subseteq G_{n+1}$, so G_n/G_{n+1} is abelian, and $G_n^p \subseteq G_{n+1}$ implies that every nontrivial element of G_n/G_{n+1} has order p, so each such quotient is an elementary abelian p-group.

The group G_1 is a pro-p group, so we briefly explain what this means. See [Kl07] for more details.
A **directed set** is a partially ordered set I with an ordering $\succeq$ such that for all $i, j \in I$ there exists a $k \in I$ such that $k \succeq i$ and $k \succeq j$.
An **inverse system** $(H_i; \phi_{ij})$ of groups over I consists of a family of groups H_i, with $i \in I$, and homomorphisms $\phi_{ij} : H_i \to H_j$ for all $i \succeq j$, such that ϕ_{ii} is the identity homomorphism on H_i and such that for all $i, j, k \in I$ with $i \succeq j \succeq k$ we have $\phi_{ij}\phi_{jk} = \phi_{ik}$.
The **inverse limit** of the inverse system $(H_i; \phi_{ij})$ is the group

$$H = \varprojlim H_i := \left\{ (g_i)_{i\in I} \in \prod_{i\in I} H_i \mid g_i\phi_{ij} = g_j \text{ when } i \succeq j \right\}$$

together with the natural coordinate maps $\phi_i : H \to H_i$.

If the H_i are finite groups, then we can give each of them the discrete topology, and their product $\prod_{i \in I} H_i$ the product topology. By doing so $\varprojlim H_i$ becomes a topological group under the induced topology. Such a group is called a **profinite group**. If the H_i are all finite p-groups, then $\varprojlim H_i$ is called a **pro-p group**.
An equivalent definition is that a profinite group is a Hausdorff, compact, totally disconnected topological group, and a pro-p group is a profinite group such that the quotient by any open normal subgroup is a p-group.

A basic property of a topological group is that every open subgroup is closed. Since pro-p groups are compact, the open subgroups are exactly the closed subgroups of finite index. Thus pro-p groups can be studied by looking at their family of finite quotients, which naturally form an inverse system for the group. For the groups G_1 defined above, we saw that the quotients G_1/G_n are finite, so a key step in studying the groups G_1 is understanding how the other subgroups of finite index are related to the congruence subgroups. We will look at this in Chapter 4.

2.8 Connection

Here we explain how the Kac-Moody groups $\widetilde{\mathbf{G}}(p)$ are related to the Chevalley groups $\mathbf{G}(\mathbb{F}_p[[t]])$. The two main chapters of this thesis are largely separate so it will suffice to give a brief overview of this connection, but it will become more relevant in the short final chapter.

Let A be a Cartan matrix and $\widetilde{A}$ the corresponding extended Cartan matrix. Let $\mathbf{G}_{sc}^{\widetilde{A}}(\mathbb{K})$ denote the minimal simply connected Kac-Moody group associated to the GCM $\widetilde{A}$ over the field $\mathbb{K}$, and let $\mathbf{G}_{sc}^{A}(\mathbb{K}([t,t^{-1}])$ denote the minimal simply connected Kac-Moody group associated to the Cartan matrix A over the ring of Laurent polynomials $\mathbb{K}([t,t^{-1}])$. Since A is a Cartan matrix, the definition of Kac-Moody groups coincides with that of Chevalley-Demazure group schemes, so $\mathbf{G}_{sc}^{A}(\mathbb{K}([t,t^{-1}])$ is also a Chevalley group (cf. [Ra92] section 2.5). Then it can be shown that there is a normal subgroup K of $\mathbf{G}_{sc}^{\widetilde{A}}(\mathbb{K})$ isomorphic to $\mathbb{K}^\times$ such that

$$\mathbf{G}_{sc}^{\widetilde{A}}(\mathbb{K})/K \cong \mathbf{G}_{sc}^{A}(\mathbb{K}([t,t^{-1}]).$$

Having obtained the groups $\mathbf{G}_{sc}^{A}(\mathbb{K}([t,t^{-1}])$ we can define various topologies on them, and complete them with respect to one of these topologies. The groups we obtain by this procedure are $\mathbf{G}_{sc}^{A}(\mathbb{K}((t)))$. These are called the **topological Kac-Moody groups**. Inside these groups we find the subgroups $\mathbf{G}_{sc}^{A}(\mathbb{K}[[t]])$, which can be seen as maximal parabolic subgroups of the topological groups.

Chapter 3

Bounded presentations of affine Kac-Moody groups

3.1 Preliminaries

3.1.1 Results about generating sets and presentation length

Definition 3.1. A **Tietze transformation** is a way of changing a given presentation $\langle X \mid R \rangle$ of a group into another presentation $\langle X' \mid R' \rangle$ of the same group. Let $F := \langle X \mid \ \rangle$. The four Tietze transformations are defined as follows (cf. [J97, Section 4.4]):

$R+$, adjoining a relator: $X' = X$, $R' = R \cup \{r\}$, where $r \in \overline{R} \backslash R$ (normal closure in F).

$R-$, removing a relator: $X' = X$, $R' = R \backslash \{r\}$, where $r \in R \cap \overline{R \backslash \{r\}}$.

$X+$, adjoining a generator: $X' = X \cup \{y\}$, $R' = R \cup \{wy^{-1}\}$, where $y \notin X$ and $w \in F$.

$X-$, removing a generator: $X' = X \backslash \{y\}$, $R' = R \backslash \{wy^{-1}\}$, where $y \in X$, $w \in \langle X \backslash \{y\} \rangle$ and wy^{-1} is the only member of R involving y.

These transformations are usually used in combination with each other, and given any two finite presentations of the same group, one can be obtained from the other using a finite sequence of Tietze transformations (cf. [J97, 4.4, Prop 6]). In particular, the following lemma illustrates how to change the generating set of a presentation. Theorem 1.3 is proved by constructing small presentations for each family of groups of Lie type, and then using a variant of this reduction lemma to obtain the main result.

Lemma 3.2 ([GKaKasL11], Lemma 2.3). *Let $\sigma = \langle X \mid R\rangle$ be a finite presentation of a group G, $\pi : F\langle X\rangle \to G$ the corresponding natural map from a free group. If D is a finite subset of G such that $G = \langle D\rangle$, then G also has a presentation $\langle D \mid R'\rangle$ such that $|R'| = |D| + |R| - |\pi(X) \cap D|$.*

Proof. Let $D = \{d_1, d_2, ..., d_l\}$. The new presentation is obtained by a sequence of Tietze transformations. First we repeatedly use transformation $X+$ to add generators:

$$\sigma' = \langle X \cup D \mid R \cup \{d_i = \delta_i(X) \mid d_i \in D \setminus \pi(X)\} \cup \{d_j = x_{j^*} \mid d_j \in D \cap \pi(X)\}\rangle$$

where the second set in the union contains one relation for each $d_i \in D \setminus \pi(X)$ expressing d_i as a word $\delta_i(X)$ in X, while the third set in the union contains one relation for each $d_j \in D \cup \pi(X)$ where $d_j = \pi(x_{j^*})$ for some $x_j^* \in X$. We then repeatedly apply transformation $X-$ to remove the generators in X:

$$\sigma'' = \langle D \mid R|_{x_j=\chi_j(D)} \cup \{d_i = \delta_i(\chi_1(D), \ldots, \chi_k(D)) \text{ for } d_i \in D \setminus \pi(X)\}\rangle$$

where each $x_j \in X$ is expressed as a word $\chi_j(D)$ in D and $R|_{x_j=\chi_j(D)}$ is a result of this substitution in the relations R. □

We now state some results on 2-generation.

Proposition 3.3. *Every finite simple group can be generated by two elements.*

This is obvious for cyclic groups of prime order and is a classical result in the case of the simple alternating groups. It was proved by Steinberg ([St62]) for the finite groups of Lie type and by Aschbacher and Guralnick ([AsG84, Theorem B]) for the sporadic groups.
Recall that a group G is said to be **quasisimple** if it is perfect, that is $G = [G, G]$, and $G/Z(G)$ is simple (where $Z(G)$ is the centre of G). Proposition 3.3 can be extended to quasisimple groups, using the following lemma. Recall that $\Phi(G)$ denotes the **Frattini subgroup** of G, that is the intersection of all the maximal subgroups of G.

Lemma 3.4. *If G finite and perfect, then $Z(G) \leq \Phi(G)$.*

Proof. Assume for a contradiction that there is a maximal subgroup M of G that doesn't contain $Z(G)$. We have $M < MZ(G) \leq G$, hence we must have $MZ(G) = G$. Let $g \in G$, $g = mz$ with $m \in M$ and $z \in Z(G)$, and let $m' \in M$. Then we have $g^{-1}m'g = z^{-1}m^{-1}m'mz = m^{-1}m'm \in M$ hence $M \trianglelefteq G$. M is maximal and G is finite, so G/M has prime order and is thus abelian, hence M contains $[G, G] = G$, contradiction. □

An equivalent definition of $\Phi(G)$ is that it is the set of all non-generators of G, i.e. the set of elements $g \in G$ such that if X is a generating set for G containing g, then $X \backslash \{g\}$ is a generating set for G as well. Hence we have shown that elements of $Z(G)$ in a finite perfect group G are non-generators of G and so the above proposition implies the following.

Proposition 3.5. *Every finite quasisimple group can be generated by two elements.*

Together with Lemma 3.2 this implies the following.

Corollary 3.6. *If a finite quasisimple group has a presentation with n generators and m relations, then it also has a presentation with 2 generators and $m+2$ relations.*

For G a group, we denote by G^m the direct product of m copies of G.

Proposition 3.7 (Maróti and Tamburini, [MarT13], Theorem 1.1)**.** *Let G be a non-abelian finite simple group. We let $h(G)$ denote the largest non-negative integer such that $G^{h(G)}$ can be generated by two elements. Then we have*

$$h(G) > 2\sqrt{|G|}.$$

Proposition 3.8 (Kantor and Lubotzky, [KaL90], Lemma 5 a))**.** *Let H be a finite group with $H = G_1^{m_1} \times ... \times G_t^{m_t}$ where the $G_1, \ldots, G_t$ are pairwise non-isomorphic simple groups and $m_1, \ldots, m_t$ are positive integers.*
Then a subset of H generates H if and only if its projection into $G_i^{m_i}$ generates $G_i^{m_i}$ for each i.

We can now prove the following summarising statement.

Proposition 3.9. *Let $G = G_1^a \times G_2^b$ where G_1 and G_2 are finite non-abelian non-isomorphic quasisimple groups and a and b are non-negative integers with $0 \leq a, b \leq 3$. Then G is 2-generated.*

Proof. By Proposition 3.5, G_1 and G_2 are 2-generated. The smallest order of a finite non-abelian simple group is 60. Hence Proposition 3.7 implies that, for any finite simple group, $h(G) > 2\sqrt{60} \approx 15.49$ so $h(G) \geq 16$. Hence, since $a, b \leq 3 < 16$, we have in particular that G_1^a and G_2^b are 2-generated.
Finally Proposition 3.8 says that if g_1, g_1' are generators for G_1^a and g_2, g_2' are generators for G_2^b, then (g_1, g_2) and (g_1', g_2') are generators for G. So G is 2-generated. $\square$

In some of our proofs we will need to know how much freedom we have in choosing these two generators. In particular we will need the following result of Guralnick and Kantor. Recall that a group G is said to be **almost simple** if there exists a non-abelian simple group S such that $S \leq G \leq \mathrm{Aut}\,(S)$, where $\mathrm{Aut}\,(S)$

is the automorphism group of S. The **socle** of a group G is defined to be the subgroup of G generated by its minimal normal subgroups. If G has no minimal normal subgroups then the socle of G is defined to be $\{1_G\}$.

Proposition 3.10 ([GKa00], p. 745, Corollary). *Any nontrivial element of a finite almost simple group G belongs to a pair of elements generating at least the socle of G.*

A non-abelian finite simple group is trivially almost simple and has trivial socle so this result implies that any nontrivial element of a non-abelian finite simple group G belongs to a generating pair of G. If G is now quasisimple, then we explained above that the elements of $Z(G)$ are non-generators of G, so together with the last proposition this implies

Corollary 3.11. *Any non-central element of a finite quasisimple group G belongs to a generating pair of G.*

To get our main result, Theorem A, from the more detailed Theorem B we need to use Lemma 3.2 together with the fact that the Kac-Moody groups in question are themselves 2-generated (or 3-generated in the two special cases). This fact was proved by Capdeboscq in [C15] for large enough q and clarified by Capdeboscq and Rémy in [CRe] to include the small values of p and q. We can state it as follows.

Theorem 3.12. *Let $\widetilde{X}(q)$ be a simply connected affine Kac-Moody group of rank at least 3 defined over a finite field $\mathbb{F}_q$. Then $\widetilde{X}(q)$ is generated by 2 elements, with the possible exceptions of $\widetilde{A}_2(2)$ and $\widetilde{A}_2(3)$ in which case it is generated by at most 3 elements.*

This and Lemma 3.2 imply that if such a group has a presentation with n generators and m relations, then it also has a presentation with 2 generators and $m+2$ relations (3 generators and $m+3$ relations in the $\widetilde{A}_2(2)$ and $\widetilde{A}_2(3)$ cases).

3.1.2 Presentations of finite simple and quasisimple groups

The series of papers [GKaKasL07], [GKaKasL08] and [GKaKasL11] establish various bounds on the lengths of presentations of finite simple and quasisimple groups. Recall Theorem 1.3, saying that all finite quasisimple groups, with the possible exception of ${}^2G_2(3^{2e+1})$, have presentations with at most 2 generators and 51 relations. They obtain better bounds for the individual groups and we summarise the ones we will need in Table A.1 (cf. Table 1 of [GKaKasL11]).

Theorem 4.5 of [GKaKasL11] gives a presentation σ_1 of $\mathrm{SL}(2,q)$ with 3 generators and 9 relations, and they show that this presentation can be reduced to a presentation ρ_1 with 3 generators and 5 relations if q is even. They also explain that similar reductions are possible for q prime, and when $q \leq 16$. All the other presentations in Table A.1 are based on the presentation of $\mathrm{SL}(2,q)$, so in the special cases with q even, q prime, or $q \leq 16$ it is possible to obtain smaller presentations of these quasisimple groups (and hence also of the affine Kac-Moody groups). In what follows we will consider the general case as well as the special case when q is even.

We now explain how the various presentations in Table A.1 are connected.

Definition 3.13. Let B be a group and A its subgroup. Suppose further that B has a finite presentation $\sigma_B = \langle X_B \mid R_B \rangle$ and A has a presentation $\sigma_A = \langle X_A \mid R_A \rangle$ such that $X_A \subset X_B$ and $R_A \subseteq R_B$. Then we say that σ_A is **contained in** σ_B and write

$$\sigma_A \subseteq \sigma_B.$$

The presentation σ_1 of $\mathrm{SL}(2,q)$ (respectively ρ_1 for even q) is given in Theorem 4.5 of [GKaKasL11]. Consider a group $G = \mathrm{SL}(3,q)$. If $\{\alpha_1, \alpha_2\}$ is the set of simple roots of $\mathrm{SL}(3,q)$, then G contains a subgroup $L = \langle X_{\alpha_1}, X_{-\alpha_1} \rangle \cong \mathrm{SL}(2,q)$, where X_{α_1} and $X_{-\alpha_1}$ are the root subgroups of $\mathrm{SL}(3,q)$ (cf. [Car72]). Theorem 5.1 of [GKaKasL11] gives a presentation σ_2 of $\mathrm{SL}(3,q)$ that contains $\sigma_L = \sigma_1$ (respectively ρ_2 for even q contains $\sigma_L = \rho_1$) . We will use this several times so we restate it as a result.

Lemma 3.14. *For odd q, the presentation σ_1 of $\mathrm{SL}(2,q)$ is contained in the presentation σ_2 of $\mathrm{SL}(3,q)$.*
For even q, the presentation ρ_1 of $\mathrm{SL}(2,q)$ is contained in the presentation ρ_2 of $\mathrm{SL}(3,q)$.

Theorem 6.1 of [GKaKasL11] gives explicit presentations of $\mathrm{SL}(n,q)$ for $n \geq 4$. First the authors construct the presentations σ_4 of $\mathrm{SL}(4,q)$, σ_6 of $\mathrm{SL}(n,q)$ for $5 \leq n \leq 8$, and σ_8 of $\mathrm{SL}(n,q)$ for $n \geq 9$ (respectively ρ_4, ρ_6 and ρ_8 for even q). If $\{\alpha_1, \alpha_2, ..., \alpha_{n-1}\}$ is the set of simple roots of $\mathrm{SL}(n,q)$, the group $\mathrm{SL}(n,q)$ contains a subgroup $M = \langle X_{\alpha_1}, X_{-\alpha_1}, X_{\alpha_2}, X_{-\alpha_2} \rangle$, isomorphic to $\mathrm{SL}(3,q)$. The initial presentations given in the proof of Theorem 6.1 all contain a copy of the presentation of $\mathrm{SL}(3,q)$ given in Theorem 5.1. That is, we have $\sigma_2 \subseteq \sigma_i$ for $i = 4, 6$ and 8 where σ_2 is the presentation of M (respectively $\rho_2 \subseteq \rho_i$ for $i = 4, 6$ and 8 for even q).
As explained above, σ_2 contains the presentation σ_1 of $\mathrm{SL}(2,q)$. In the proof of Theorem 6.1 the generators in σ_1 are called $\{u, t, h\}$, and the generators in σ_2 are $\{u, t, h, c\}$. The authors reduce their presentations of $\mathrm{SL}(n,q)$ by showing that c is in fact redundant and can be removed. By doing so, and removing redundant relations, they obtain the shorter presentations σ_3 of $\mathrm{SL}(4,q)$, σ_5 of $\mathrm{SL}(n,q)$ for

$5 \le n \le 8$, and σ_7 of $\mathrm{SL}(n,q)$ for $n \ge 9$ (respectively ρ_3, ρ_5 and ρ_7 for even q). Hence these shorter presentations no longer contain σ_2 (respectively ρ_2), but they still contain the σ_1 that was contained in σ_2 (respectively the ρ_1 that was contained in ρ_2). Again we restate this as a result.

Lemma 3.15. *The presentations σ_1, ρ_1 of $\mathrm{SL}(2,q)$ and σ_2, ρ_2 of $\mathrm{SL}(3,q)$ are contained in the various presentations of $\mathrm{SL}(n,q)$ as follows.*

$$\begin{aligned} \textit{For } q \textit{ odd}, &\quad \sigma_1 \subseteq \sigma_i \quad \textit{for } i = 3,4,5,6,7,8. \\ \textit{For } q \textit{ even}, &\quad \rho_1 \subseteq \rho_i \quad \textit{for } i = 3,4,5,6,7,8. \\ \textit{For } q \textit{ odd}, &\quad \sigma_2 \subseteq \sigma_i \quad \textit{for } i = 4,6,8. \\ \textit{For } q \textit{ even}, &\quad \rho_2 \subseteq \rho_i \quad \textit{for } i = 4,6,8. \end{aligned}$$

So each of these groups has a longer presentation that contains σ_2 (respectively ρ_2), and a shorter one that does not. We will use the longer presentations when we need this containment, and the shorter presentations otherwise.

Theorem 7.1 and Remark 7.4 of [GKaKasL11] give presentations σ_9, σ_{10} and ρ_{10} of $\mathrm{Sp}(4,q)$ (σ_9, σ_{10} in the case when q is odd, and ρ_{10} in the case when q is even). Let α_2 be a short root, α_1 a long root. Both σ_9 and σ_{10} contain a presentation σ_1 of its short-root subgroup $L_2 = \langle X_{\alpha_2}, X_{-\alpha_2}\rangle \cong \mathrm{SL}(2,q)$, and σ_{10} also contains a presentation σ_1 of its long-root subgroup $L_1 = \langle X_{\alpha_1}, X_{-\alpha_1}\rangle \cong \mathrm{SL}(2,q)$. When q is even there is no distinction between short and long roots, but ρ_{10} contains two copies of the presentation ρ_1, one for each simple root. Again we summarise as follows.

Lemma 3.16. *The presentations σ_1, ρ_1 of $SL(2,q)$ and σ_9, σ_{10} and ρ_{10} of $\mathrm{Sp}(4,q)$ are related via the containments:*

$$\sigma_1(L_1) \subseteq \sigma_{10}, \quad \sigma_1(L_2) \subseteq \sigma_9,\ \sigma_{10}.$$

$$\rho_1(L_1),\ \rho_1(L_2) \subseteq \rho_{10}.$$

The results of [GKaKasL11] give a presentation for the family of groups $\mathrm{Spin}(2n,q)$, $n \ge 4$, $q = p^a$ with 9 generators and 42 relations. We will show how to shorten this estimate to 7 generators and 34 relations (or smaller for small n or even q) in Section 3.2. In that section we will also show that the presentations of $\mathrm{SL}(2,q)$ are contained in the presentations of $\mathrm{Spin}(2n,q)$. We summarise this here.

Lemma 3.17. *The presentations σ_1, ρ_1 of $\mathrm{SL}(2,q)$ are contained in the various presentations of $\mathrm{Spin}(2n,q)$ as follows.*

$$\textit{For } q \textit{ odd}, \quad \sigma_1 \subseteq \sigma_i \quad \textit{for } i = 13,14,15.$$

For q even, $\rho_1 \subseteq \rho_i$ *for* $i = 13, 14, 15$.

All these containments are summarised in Table A.1.

3.1.3 Presentations of affine Kac-Moody groups

We now return to the specific scenario of affine Kac-Moody groups over finite fields. Recall that the groups $\mathbf{G}_{\mathcal{D}}(\mathbb{K})$ we have defined were said to be simply connected because the set $\Pi^\vee = \{\alpha_i^\vee\}$ of simple coroots was a basis for $\mathcal{Y}$.
A GCM A is said to be **2-spherical** if for each $J \subseteq I$ with $|J| = 2$, the submatrix $A_J := (A_{ij})_{i,j \in J}$ is a classical Cartan matrix. Note that all GCMs of affine type satisfy this condition, apart from those of rank 2 (types $\widetilde{A}_1$ and $\widetilde{A}_1'$).
A Kac-Moody group arising from a 2-spherical GCM is also said to be 2-spherical.

Now, for each $\alpha \in \Pi \cup -\Pi$, let X_α be a root subgroup of $\mathbf{G}_{\mathcal{D}}(\mathbb{K})$. Then $X_\alpha \cong (\mathbb{F}_q, +)$, and for all $i, j \in I$ with $i \neq j$, we set

$$L_i \coloneqq \langle X_{\alpha_i} \cup X_{-\alpha_i} \rangle \quad \text{and} \quad L_{ij} \coloneqq \langle L_i \cup L_j \rangle = L_{ji}.$$

In what follows we will need to exclude some special cases, so we define the following condition:

$$L_{ij}/Z(L_{ij}) \ncong B_2(2), G_2(2), G_2(3), {}^2F_4(2) \quad \text{for all } i, j \in I. \tag{$\bigstar$}$$

We can now state an observation which will be useful for us in section 3.

Proposition 3.18. *Let A be a 2-spherical generalised Cartan matrix and $\mathcal{D}$ a simply connected root datum corresponding to A. Suppose that the field $\mathbb{K}$ is finite and that condition ($\bigstar$) holds.*
Let $J \subseteq I$ and

$$L_J = \langle L_i \mid i \in J \rangle.$$

Then L_J is a simply connected Kac-Moody group $\mathbf{G}_{\mathfrak{D}(J)}(\mathbb{K})$ with a root datum of type $A_J = (A_{ij})_{i,j \in J}$.

Proof. This becomes clear once we construct the root datum for L_J. If $J \subseteq I$, let $\Theta = \{\alpha_i \mid i \in J\}$. Then $\Theta^\vee = \{\alpha_i^\vee \mid i \in J\}$ is the corresponding subset of $\Pi^\vee$. Since $\mathcal{D}$ is simply connected, the simple coroots form a basis for $\mathcal{Y}$, so the coroot lattice $\langle \Pi^\vee \rangle = \bigoplus_{i \in I} \mathbb{Z}\alpha_i^\vee = \mathcal{Y}$ splits into a direct sum

$$\mathcal{Y} = \langle \Theta^\vee \rangle \oplus \langle \Pi^\vee \setminus \Theta^\vee \rangle.$$

Hence, the root datum for L_J is

$$\mathcal{D}(J) = (J, A_J, X/\langle\Theta^\vee\rangle^\perp, \langle\Theta^\vee\rangle, \Theta, \Theta^\vee).$$

$\Theta^\vee$ is clearly a basis for $\langle\Theta^\vee\rangle$, so $\mathcal{D}(J)$ is simply connected. $\square$

In particular this means that for each i,

$$L_i \cong SL(2, q).$$

We will also need the following result on generation by the subgroups L_i.

Lemma 3.19 (Capdeboscq [C15], Lemma 2.1)**.** *Let G be a simply connected Kac-Moody group over a finite field $\mathbb{K}$. Then the L_i generate G.*

In particular, if $G = \mathrm{SL}\,(3, q)$, this implies that G is generated by two copies of $\mathrm{SL}\,(2, q)$, one for each simple root.

Abramenko and Mühlherr's result stated as Theorem 1.1 above is a corollary of another of their results (cf. [AbrM97], [Ca07, Th. 3.7]) which can now be stated as follows:

Theorem 3.20. *(Abramenko, Mühlherr) Let A be a 2-spherical generalised Cartan matrix and $\mathcal{D}$ a simply connected root datum corresponding to A. Suppose that the field $\mathbb{K}$ is finite and condition ($\bigstar$) holds.*
Let $\widetilde{G}$ be the direct limit of the inductive system formed by the L_i and L_{ij} for $i, j \in I$, with the natural inclusions.
Then the canonical homomorphism $\widetilde{G} \to \mathbf{G}_{\mathcal{D}}(\mathbb{K})$ is an isomorphism.

A direct consequence of this result is that $\mathbf{G}_{\mathcal{D}}(\mathbb{F}_q)$ has a presentation whose generators are the generators of the root subgroups X_i, $i \in I$, and whose relations are the defining relations of all L_i's and L_{ij}'s with $i, j \in I, i \neq j$. More specifically we have the following observation (cf. proof of [C13] Th 2.1):

Proposition 3.21. *Let $\widetilde{X}(q)$ be a simply connected 2-spherical split Kac-Moody group of rank $n \geq 3$ over the field of q elements. Let Δ be the Dynkin diagram of $\widetilde{X}(q)$ with the vertices labelled by $\beta_1, ..., \beta_n$. Suppose further that if Δ contains a subdiagram of type B_2, then $q \geq 3$, and if it contains a subdiagram of type G_2, $q \geq 4$.*

Suppose that Δ contains k proper subdiagrams Δ_1, Δ_2, ..., Δ_k such that $\Delta = \cup_{i=1}^k \Delta_i$, and each pair of vertices of Δ is contained in Δ_i for some $i \in \{1, ..., k\}$. Let $X_i(q) := \langle L_j \mid \alpha_j \in \Delta_i \rangle$. If $\sigma_{X_i(q)} = \langle D_i \mid R_i \rangle$ is a presentation of $X_i(q)$, then

$\widetilde{X}(q)$ has a presentation

$$\sigma_{\widetilde{X}(q)} = \langle D_1 \cup D_2 \cup \ldots \cup D_k \mid R_1 \cup \ldots \cup R_k \cup \bigcup_{1 \leq i < j \leq k} R_{ij} \rangle$$

where R_{ij} are the relations coming from identifying the generators of $X_{ij}(q) := \langle L_k \mid \alpha_k \in \Delta_i \cap \Delta_j \rangle$ in $X_i(q)$ and in $X_j(q)$.

Definition 3.22. Let $J \subseteq I$. We say that Δ' is a **subdiagram of Δ based on the vertices** α_i for $i \in J$ if Δ' is a subgraph of Δ with the α_i, $i \in J$, as its vertices, and with vertices having the same number of edges and arrows between them as they do in Δ. This is equivalent to Δ' being the Dynkin diagram corresponding to the reduced GCM $(A_{ij})_{i,j \in J}$.

We now consider the special case where $\Delta = \Delta_1 \cup \Delta_2$ on the level of vertices. That is, Δ may contain edges not included in Δ_1 or Δ_2. We cannot use Proposition 3.21 immediately because it is not necessarily true that any pair of vertices is contained in some Δ_i. To remedy this we introduce Δ_3.
Let Δ_3 be a subdiagram of Δ based on the vertices of

$$\Delta \setminus (\Delta_1 \cap \Delta_2) = (\Delta_1 \setminus \Delta_2) \cup (\Delta_2 \setminus \Delta_1).$$

Now any pair of vertices of Δ is contained in some Δ_i. Proposition 3.21 gives a presentation

$$\sigma_{\widetilde{X}(q)} = \langle D_1 \cup D_2 \cup D_3 \mid R_1 \cup R_2 \cup R_3 \cup R_{12} \cup R_{13} \cup R_{23} \rangle.$$

In order to reduce this presentation we now pick a special presentation of $X_3(q)$ by considering two of its subgroups.
Let $X_3^1(q)$ be the subgroup of $\widetilde{X}(q)$ corresponding to $\Delta_1 \setminus \Delta_2$, and let

$$\sigma_{X_3^1(q)} = \langle D_3^1 \mid R_3^1 \rangle$$

be its presentation. Likewise, let

$$\sigma_{X_3^2(q)} = \langle D_3^2 \mid R_3^2 \rangle$$

be a presentation of the subgroup $X_3^2(q)$ of $\widetilde{X}(q)$ corresponding to $\Delta_2 \setminus \Delta_1$. Now we can choose a special presentation of $X_3(q)$:

$$\sigma_{X_3(q)} = \langle D_3^1 \cup D_3^2 \mid R_3^1 \cup R_3^2 \cup R_3^{**} \rangle,$$

where R_3^{**} are those relations that include generators in both D_3^1 and D_3^2, i.e. the relations that express how the subgroups $X_3^1(q)$ and $X_3^2(q)$ are related inside $X_3(q)$.

Using $\sigma_{X_3(q)}$ in $\sigma_{\widetilde{X}(q)}$ we get

$$\sigma_{\widetilde{X}(q)} = \langle D_1 \cup D_2 \cup D_3^1 \cup D_3^2 \ \mid \ R_1 \cup R_2 \cup R_3^1 \cup R_3^2 \cup R_3^{**} \cup R_{12} \cup R_{13} \cup R_{23} \rangle.$$

Since $\Delta_1 \supseteq \Delta_1 \setminus \Delta_2$, $X_3^1(q)$ is also a subgroup of $X_1(q)$. So the generators D_3^1 are expressible in terms of D_1, and the relations R_3^1 already hold since they are enforced by R_1. So we can use Tietze transformations to remove D_3^1 and R_3^1 from $\sigma_{\widetilde{X}(q)}$. Similarly, since $\Delta_2 \supseteq \Delta_2 \setminus \Delta_1$, we can remove D_3^2 and R_3^2 from $\sigma_{\widetilde{X}(q)}$.
Finally we have $\Delta_1 \cap \Delta_3 = \Delta_1 \setminus \Delta_2$, so $X_{13}(q) = X_3^1(q)$. The relations R_{13} come from needing to identify the generators of $X_3^1(q)$ in $X_1(q)$ and $X_3(q)$, since the original presentation generated $X_3^1(q)$ twice. But we have now removed D_3^1, so the generators we need to equate are both written in terms of D_1, hence they are already equal and the relations R_{13} become superfluous. So we can remove R_{13}, and we can similarly remove R_{23}.
We can now summarise the above in the next corollary.

Corollary 3.23. *Let $\widetilde{X}(q)$ be a simply connected affine Kac-Moody group of rank at least 3 over the field of q elements. Let Δ be the Dynkin diagram of $\widetilde{X}(q)$ with the vertices labelled by $\alpha_0, ..., \alpha_n$. Suppose further that if Δ contains a subdiagram of type B_2, then $q \geq 3$, and if it contains a subdiagram of type G_2, $q \geq 4$.*

Suppose that Δ contains three proper subdiagrams Δ_1, Δ_2 and Δ_3 such that $\alpha_1, ..., \alpha_n \in \Delta_1 \cup \Delta_2$ and Δ_3 is a subdiagram of Δ based on the vertices of $(\Delta_1 \setminus \Delta_2) \cup (\Delta_2 \setminus \Delta_1)$. If for $i = 1, 2$, $\sigma_{X_i(q)} = \langle D_i \mid R_i \rangle$ is a presentation of $X_i(q)$ and $\sigma_{X_3(q)}$ is as defined above, then $\widetilde{X}(q)$ has a presentation

$$\sigma_{\widetilde{X}} = \langle D_1 \cup D_2 \mid R_1 \cup R_2 \cup R_3^* \cup R_{12} \rangle$$

where the relations in R_3^* are obtained from the relations in R_3^{**} by substituting generators in D_3 with their expressions via generators in D_1 or D_2. In particular we have $|R_3^*| = |R_3^{**}|$.

We will use this corollary many times in our calculations, and in practice we will always choose Δ_1 and Δ_2 to have an overlap. Corollary 3.23 holds more generally for 2-spherical split Kac-Moody groups - we state it for affine groups because this is how we will use it.

3.1.4 General strategy

We now proceed to find presentation lengths for the 7 infinite families and 7 exceptional types of affine simply connected Kac-Moody groups of rank greater than or equal to 3 (i.e. $n \geq 2$), as well as for the groups $\mathrm{Spin}\,(2n, q)$. We will be following the same general strategy in each case:

Step 1: Split the Dynkin diagram Δ into overlapping subdiagrams Δ_i such that $\Delta = \cup_i \Delta_i$ and every subdiagram of rank 2 is contained in some Δ_i.

Step 2: Apply Proposition 3.21 or Corollary 3.23 as appropriate to obtain a presentation of the group.

Step 3: Make use of presentation containments to remove redundant generators and relations.

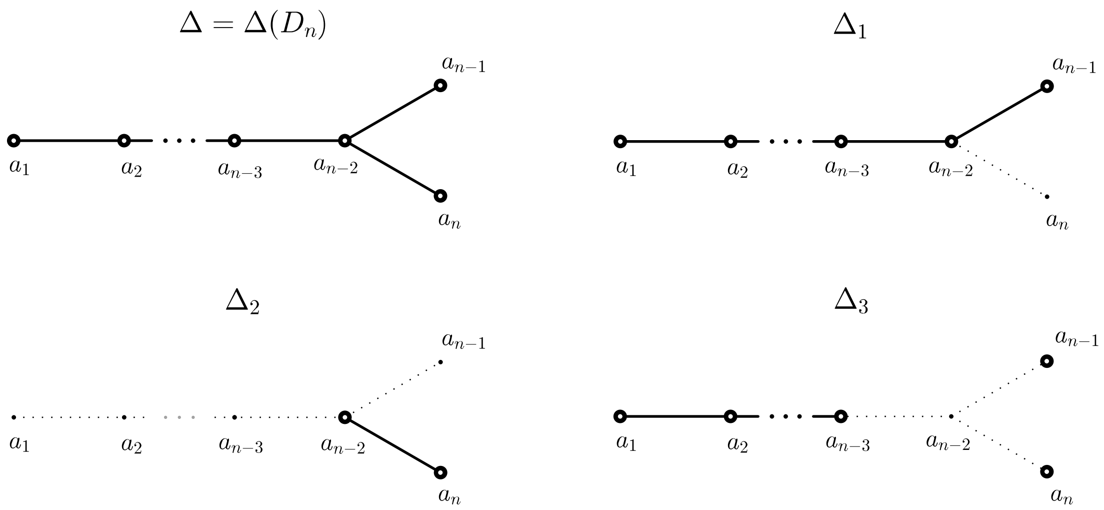
Step 4: Calculate the length of the obtained presentation using the presentation lengths of quasisimple groups given in Table A.1.

Several of the cases with smaller values of n will need to be done separately because we have smaller presentations of the quasisimple groups available in those cases, or because the choice of subdiagrams is different to the general case.

3.2 Presentation of $\mathrm{Spin}\,(2n, q)$

A presentation of the groups $\mathrm{Spin}\,(2n, q)$, $n \geq 4$ is given in [GKaKasL11]. Their presentation has 9 generators and 42 relations. In this section we show how to shorten this estimate using our general strategy. In the next section we will move on to calculating presentations of the affine Kac-Moody groups using the same strategy.

To obtain an initial presentation of $G = \mathrm{Spin}\,(2n, q)$, $n \geq 4$, we use Corollary 3.23.



Let Δ_1 be the subdiagram of Δ whose vertices are the $n-1$ nodes $a_1, \ldots, a_{n-1}$. Let Δ_2 be the subdiagram of Δ whose vertices are the nodes a_{n-2} and a_n. Then Δ_3 is the subdiagram of Δ based on all vertices but a_{n-2}.
By Proposition 3.18, the corresponding groups $X_1(q)$, $X_2(q)$ and $X_3(q)$ are simply connected. Δ_1 has type A_{n-1} and so

$$X_1(q) \cong \mathrm{SL}\,(n, q).$$

Δ_2 is of type A_2 and so

$$X_2(q) \cong \mathrm{SL}\,(3, q).$$

Finally, Δ_3 is of type $A_{n-3} \times A_1 \times A_1$, hence

$$X_3(q) \cong \mathrm{SL}\,(n-2, q) \times \mathrm{SL}\,(2, q) \times \mathrm{SL}\,(2, q).$$

Clearly, $\Delta = \Delta_1 \cup \Delta_2$. Therefore G has a presentation

$$\sigma_G = \langle D_1 \cup D_2 \mid R_1 \cup R_2 \cup R_3^* \cup R_{12} \rangle,$$

as described in Corollary 3.23.

We take a presentation $\sigma_{X_1(q)}$ of $X_1(q)$ from Table A.1. If $n \geq 9$, $\sigma_{X_1(q)} = \sigma_7$ (or ρ_7 if q is even), if $5 \leq n \leq 8$, $\sigma_{X_1(q)} = \sigma_5$ (or ρ_5 if q is even), and if $n = 4$, $\sigma_{X_1(q)} = \sigma_3$ (or ρ_3 is q is even). Consider the subgroup $X = L_{n-2}$ of G. Its Dynkin diagram is of type A_1 and Proposition 3.18 asserts that the corresponding subgroup is simply connected, so $X \cong \mathrm{SL}\,(2, q)$. From Table A.1 we know that X has a presentation $\sigma_X = \langle D_X \mid R_X \rangle = \sigma_1$ with $|D_X| = 3$ and $|R_X| = 9$ (or ρ_1 with $|D_X| = 3$, $|R_X| = 5$ if q is even).
Now X is a subgroup of both $X_1(q)$ and $X_2(q)$. The group $X_2(q)$ has a presentation $\sigma_{X_2(q)} = \sigma_2$ (or ρ_2 if q even) with $\sigma_X \subseteq \sigma_{X_2(q)}$. Since $X \leq X_1(q)$, clearly the generators D_X are contained in $X_1(q)$. Thus elements of D_X can be expressed in terms of elements of D_1. Moreover, the relations R_X automatically hold, since they hold in $X_1(q)$. We can thus use Tietze transformations to eliminate D_X and R_X. This makes the relations R_{12} superfluous so we can remove them too, obtaining:

$$\sigma'_G = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus R_X) \cup R_3^* \rangle.$$

If $n \geq 9$, we use σ_7 for $\sigma_{X_1(q)}$, which requires 6 generators and 25 relations, so that $|D_1 \cup (D_2 \setminus D_X)| = 6 + (4 - 3) = 7$ and $|R_1 \cup (R_2 \setminus R_X)| = 25 + (14 - 9) = 30$. For q even we use ρ_7, which requires 6 generators and 21 relations, giving us $|D_1 \cup (D_2 \setminus D_X)| = 6 + (4 - 3) = 7$ and $|R_1 \cup (R_2 \setminus R_X)| = 21 + (10 - 5) = 26$.

Now consider $X_3(q) = (X_3(q) \cap X_1(q)) \times (X_3(q) \cap X_2(q))$ where $X_3(q) \cap$

$X_1(q) \cong \mathrm{SL}\,(n-2,q) \times \mathrm{SL}\,(2,q)$ and $X_3(q) \cap X_2(q) \cong \mathrm{SL}\,(2,q)$. Each factor has two generators (Proposition 3.9). Denote them by a_1, a_2 and b_1, b_2 respectively. R_3^* is the set of relations that ensure that $X_3(q) \cap X_1(q)$ commutes with $X_3(q) \cap X_2(q)$. So we have

$$R_3^* = \{[a_1, b_1] = [a_1, b_2] = [a_2, b_1] = [a_2, b_2] = 1\}$$

and $|R_3^*| = 4$.

Therefore if $n \geq 9$, G has a presentation with 7 generators and $30 + 4 = 34$ relations (or 7 generators and $26 + 4 = 30$ relations if q is even). We call this presentation σ_{15} (ρ_{15} in the even case) of Table A.1.

Similarly, if $n = 4$ then we use the presentation σ_3 for $\sigma_{X_1(q)}$, which requires 5 generators and 20 relations, so G has a presentation with $5+(4-3) = 6$ generators and $20 + (14 - 9) + 4 = 29$ relations. We call this presentation σ_{13} of Table A.1. For q even we use the presentation ρ_3 for $\sigma_{X_1(q)}$, which requires 5 generators and 16 relations, so G has a presentation with $5+(4-3) = 6$ generators and $16+(10-5)+4 = 25$ relations. We call this presentation ρ_{13} of Table A.1.

Finally, if $5 \leq n \leq 8$ then we use the presentation σ_5 for $\sigma_{X_1(q)}$, which requires 5 generators and 21 relations, so G has a presentation with $5 + (4 - 3) = 6$ generators and $21 + (14 - 9) + 4 = 30$ relations. We call this presentation σ_{14} of Table A.1. For q even we use the presentation ρ_5 for $\sigma_{X_1(q)}$, which requires 5 generators and 17 relations, so G has a presentation with $5 + (4 - 3) = 6$ generators and $17 + (10 - 5) + 4 = 26$ relations. We call this presentation ρ_{14} of Table A.1.

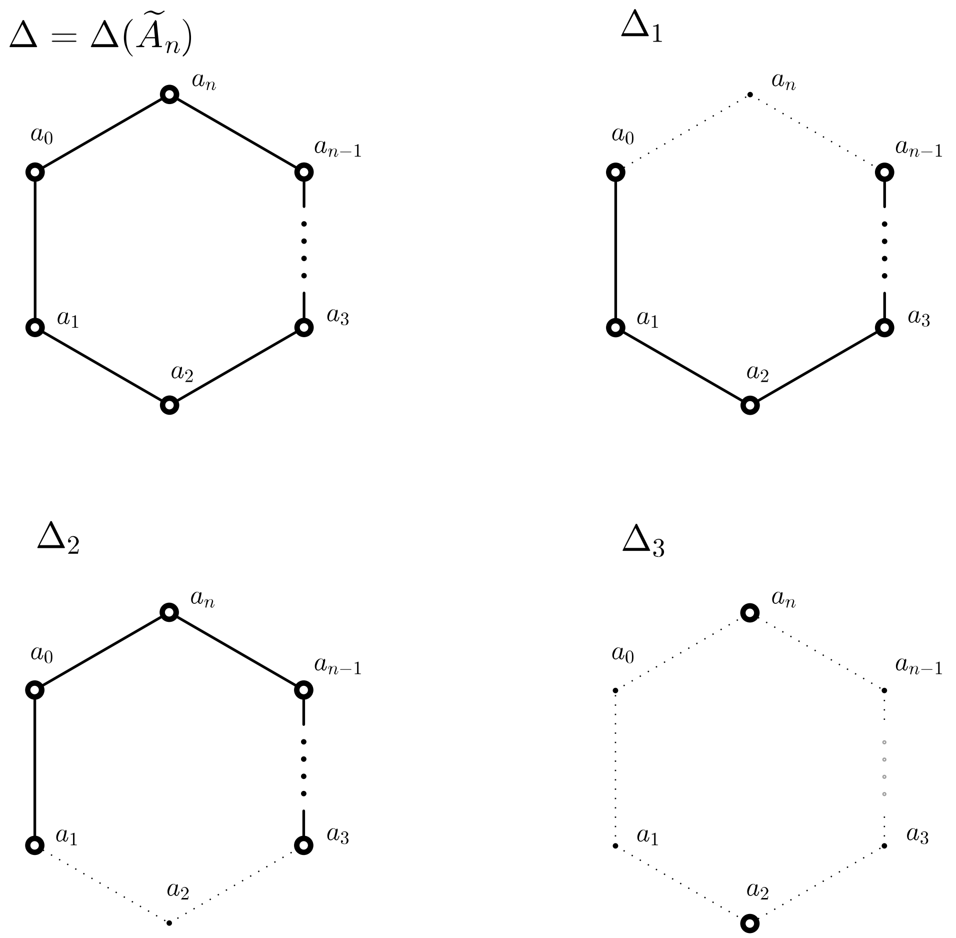
Note that our final presentations contain $\sigma_{X_1(q)}$ in its entirety, and the latter contains σ_1 (respectively ρ_1 for q even), so our presentations σ_{13}, σ_{14} and σ_{15} also contain σ_1 (respectively ρ_{13}, ρ_{14}, ρ_{15} also contain ρ_1).

3.3 Untwisted affine Kac-Moody groups

We now go through the calculations for the 4 infinite families and 5 exceptional types of affine untwisted simply connected Kac-Moody groups of rank greater than or equal to 3.

3.3.1 $\widetilde{A}_n(q), n \geq 4$

We begin by considering the case $n \geq 8$. The Dynkin diagram Δ of $G = \widetilde{A}_n(q)$ consists of $n + 1$ vertices:



We now use Corollary 3.23. Let Δ_1 be the subdiagram of Δ whose vertices are the n nodes a_0, a_1, $a_2, \ldots, a_{n-1}$. Let Δ_2 be the subdiagram of Δ whose vertices are the n nodes a_1, a_0, $a_n, a_{n-1} \ldots, a_3$. Then Δ_3 is the subdiagram of Δ whose vertices are the two nodes a_2 and a_n.
By Proposition 3.18, the corresponding groups $X_1(q)$, $X_2(q)$ and $X_3(q)$ are simply connected. Δ_1 and Δ_2 are both of type A_n so we have

$$X_1(q) \cong X_2(q) \cong \mathrm{SL}\,(n+1, q).$$

Δ_3 is of type $A_1 \times A_1$ and so

$$X_3(q) \cong \mathrm{SL}\,(2, q) \times \mathrm{SL}\,(2, q).$$

Clearly, $\Delta = \Delta_1 \cup \Delta_2$. Therefore, following the notation of Corollary 3.23,

G has a presentation

$$\sigma_G = \langle D_1 \cup D_2 \mid R_1 \cup R_2 \cup R_3^* \cup R_{12} \rangle.$$

We now proceed to find the required presentations for $X_1(q), X_2(q)$ and $X_3(q)$.

Consider the subgroup X of G that is generated by L_0 and L_1. Its Dynkin diagram is of type A_2. Proposition 3.18 asserts that this subgroup is simply connected, and thus $X \cong \mathrm{SL}\,(3, q)$.

From Table A.1 we know that X has a presentation $\sigma_X = \langle D_X \mid R_X \rangle$ of type σ_2 with 4 generators and 14 relations (respectively ρ_2 with 4 generators and 10 relations when q is even).

Now X is a subgroup of both $X_1(q)$ and $X_2(q)$. Both of these are isomorphic to $\mathrm{SL}\,(n+1, q)$ and Table A.1 says this group has two presentations σ_7 and σ_8, with σ_8 containing σ_2 (for q even the two presentations are ρ_7 and ρ_8, with ρ_8 containing ρ_2). In particular $X_1(q)$ has a presentation $\sigma_{X_1(q)}$ of type σ_7 that requires 6 generators and 25 relations (respectively ρ_7 with 6 generators and 21 relations for q even), and $X_2(q)$ has a presentation $\sigma_{X_2(q)}$ of type σ_8, with 7 generators and 26 relations (respectively ρ_8 with 7 generators and 22 relations for q even), and

$$\sigma_X \subseteq \sigma_{X_2(q)}.$$

Since $X \leq X_1(q)$, the generators D_X are in $X_1(q)$ and the relations R_X already hold. We now use Tietze transformations to eliminate D_X and R_X:

$$\sigma'_G = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus R_X) \cup R_3^* \cup R_{12} \rangle.$$

We have $|D_1 \cup (D_2 \setminus D_X)| = 6 + (7-4) = 9$ and $|R_1 \cup (R_2 \setminus R_X)| = 25 + (26-14) = 37$ (for q even we have $|D_1 \cup (D_2 \setminus D_X)| = 6 + (7-4) = 9$ and $|R_1 \cup (R_2 \setminus R_X)| = 21 + (22-10) = 33$), and so it remains to compute $|R_3^*|$ and $|R_{12}|$.

Consider $X_3(q) = L_2 \times L_n$. Since $L_2 \cong L_n \cong \mathrm{SL}\,(2, q)$, each factor has 2 generators (Proposition 3.9). Denote them by a_1, a_2 and b_1, b_2 respectively. In the notation of Corollary 3.23, R_3^* is the set of relations that ensure $X_3^1(q) = L_2$ commutes with $X_3^2(q) = L_n$, and so

$$R_3^* = \{[a_1, b_1] = [a_1, b_2] = [a_2, b_1] = [a_2, b_2] = 1\}$$

and hence $|R_3^*| = 4$.

Finally, $\Delta_1 \cap \Delta_2$ is of type $A_2 \times A_{n-3}$. By Proposition 3.9, the corresponding group $\mathrm{SL}\,(3, q) \times \mathrm{SL}\,(n-2, q)$ has 2 generators. We call them c_1, d_1 as elements of $X_1(q)$ and c_2, d_2 as elements of $X_2(q)$. Then R_{12} is the set of relations equating the corresponding generators of this group so

$$R_{12} = \{c_1 = c_2, d_1 = d_2\}$$

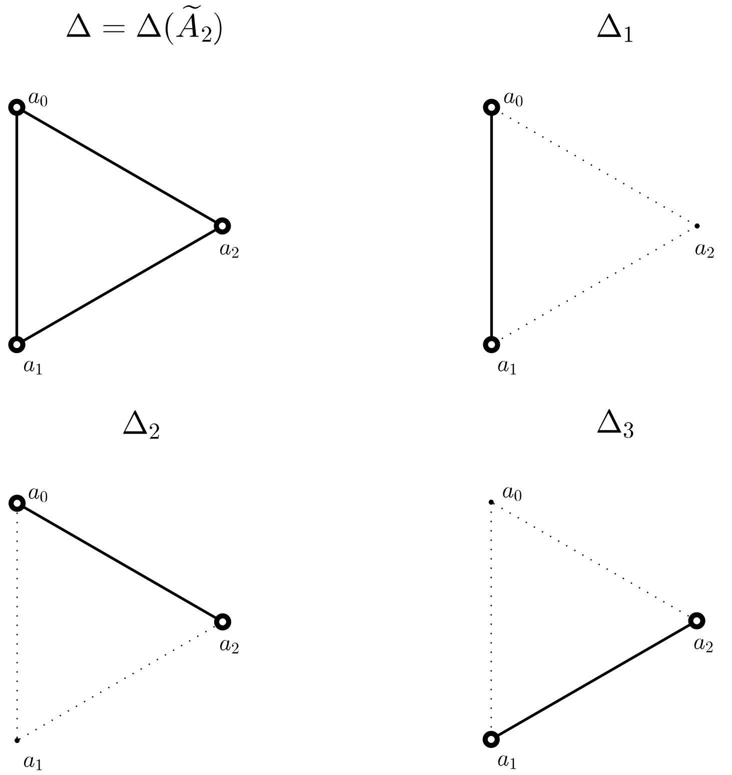
and hence $|R_{12}| = 2$.

It follows that the presentation σ'_G of G has 9 generators and $37+4+2 = 43$ relations (9 generators and $33+4+2 = 39$ relations for q even).

If $4 \leq n \leq 7$, according to Table A.1 we may use the presentations σ_5 and σ_6 instead of σ_7 and σ_8 (respectively ρ_5 and ρ_6 instead of ρ_7 and ρ_8 for q even). The presentation σ_5 has 5 generators and 21 relations while σ_6 (containing σ_2) has 6 generators and 22 relations, so G has a presentation with $5 + (6 - 4) = 7$ generators and $21 + (22 - 14) + 4 + 2 = 35$ relations. For q even, the presentation ρ_5 has 5 generators and 17 relations while ρ_6 (containing ρ_2) has 6 generators and 18 relations, so G has a presentation with $5+(6-4) = 7$ generators and $17+(18-10)+4+2 = 31$ relations.

3.3.2 $\widetilde{A}_2(q)$

To obtain a presentation of $G = \widetilde{A}_2(q)$, we start with Proposition 3.21.



We let Δ_1 be the subdiagram of Δ based on the vertices a_0 and a_1, Δ_2 be the subdiagram based on the vertices a_0 and a_2, and Δ_3 be the subdiagram based on the vertices a_1 and a_2.
Clearly, $\Delta = \cup_{i=1}^{3} \Delta_i$ and every pair of vertices is contained in at least one of the Δ_i.
Thus G has a presentation

$$\sigma_G = \langle D_1 \cup D_2 \cup D_3 \mid R_1 \cup R_2 \cup R_3 \cup R_{12} \cup R_{13} \cup R_{23} \rangle.$$

By Proposition 3.18, the corresponding groups $X_1(q)$, $X_2(q)$ and $X_3(q)$ are simply connected. Δ_1, Δ_2 and Δ_3 all have type A_2, so we have

$$X_1(q) \cong X_2(q) \cong X_3(q) \cong \mathrm{SL}(3, q),$$

and Table A.1 tells us that each $X_i(q)$ has a presentation $\sigma_{X_i(q)} = \sigma_2$ $(i = 1, 2, 3)$ with 4 generators and 14 relations (or ρ_2 with 4 generators and 10 relations if q is even).

Now consider the group $X = L_0$. It is isomorphic to $\mathrm{SL}(2, q)$, and thus has a presentation $\sigma_X = \sigma_1$ with 3 generators and 9 relations (or ρ_1 with 3 generators and 5 relations if q is even). Moreover X is a subgroup of both $X_1(q)$ and $X_2(q)$. Table A.1 says that σ_1 is contained in σ_2 (respectively $\rho_1 \subseteq \rho_2$), so we can choose presentations $\sigma_{X_1(q)}$ and $\sigma_{X_2(q)}$ of type σ_2 (respectively ρ_2) such that $\sigma_X \subseteq \sigma_{X_1(q)}$ and $\sigma_X \subseteq \sigma_{X_2(q)}$. It follows that $|D_1 \cup D_2| = 4 + 4 - 3 = 5$ and $|R_1 \cup R_2| = 14 + 14 - 9 = 19$ (for q even this becomes $|D_1 \cup D_2| = 4 + 4 - 3 = 5$ and $|R_1 \cup R_2| = 10 + 10 - 5 = 15$).
Also, R_{12} is by definition the set of relations that identify the generators of $X_{12}(q) = \langle L_i \mid \alpha_i \in \Delta_1 \cap \Delta_2 \rangle$ in $X_1(q)$ and in $X_2(q)$, and we have $X_{12}(q) = X$, so these relations are superfluous.

Take now $Y = L_1$. It is also isomorphic to $\mathrm{SL}(2, q)$, and thus has a presentation $\sigma_Y = \sigma_1$ with 3 generators and 9 relations (respectively ρ_1 with 3 generators and 5 relations if q is even). σ_1 is contained in σ_2 (respectively $\rho_1 \subseteq \rho_2$), so without loss of generality we may assume that $\sigma_Y \subseteq \sigma_{X_3(q)}$. Then by Theorem 5.1 of [GKaKasL11],

$$\sigma_{X_3(q)} = \langle D_Y \cup \{c\} \mid R_Y \cup R_3^c \rangle,$$

where $D_Y = \{u, t, h\}$ (in the notation of Theorem 5.1 of [GKaKasL11]) and R_3^c is a set of 5 relations involving c and elements of D_Y. Y is a subgroup of $X_1(q)$, so in particular the elements D_Y are contained in $X_1(q)$. Thus u, t and h can be expressed in terms of elements of D_1. Moreover, the relations R_Y hold, since they hold in $X_1(q)$. And since $Y = X_{13}(q) := \langle L_i \mid \alpha_i \in \Delta_1 \cap \Delta_3 \rangle$, the relations R_{13} identify the generators of Y inside $X_1(q)$ and $X_3(q)$. But these are now both written in terms of D_1 and are already equal so these relations are superfluous. Now we can use Tietze transformations to eliminate the redundant generators and relations D_Y, R_Y, R_{13} and R_{12}:

$$\sigma'_G = \langle D_1 \cup D_2 \cup \{c\} \mid R_1 \cup R_2 \cup R_3^c \cup R_{23} \rangle.$$

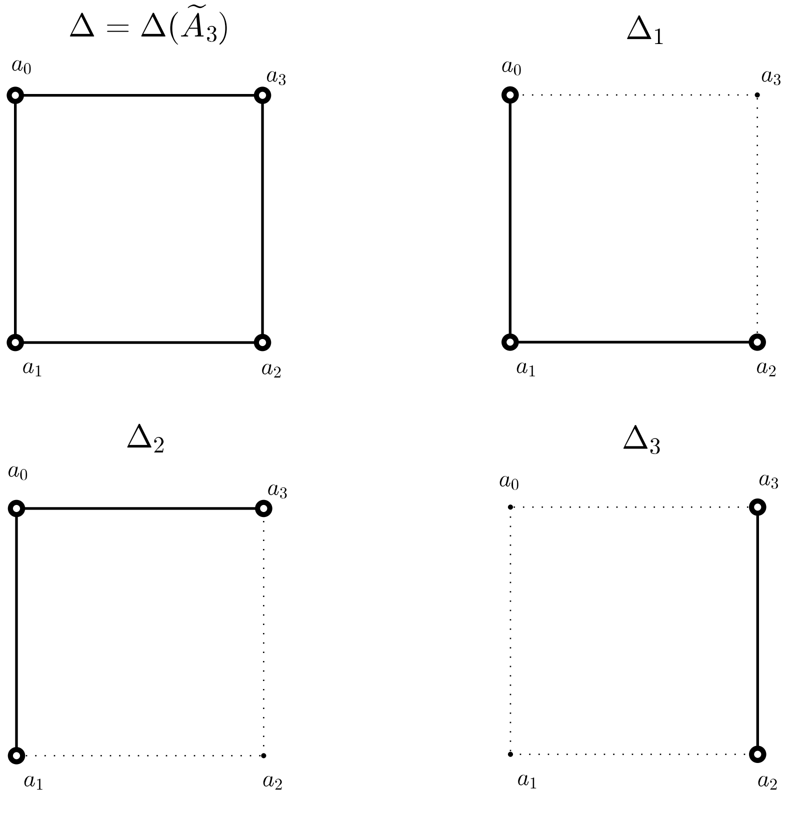
By Lemma 3.19, $X_3(q) \cong \mathrm{SL}\,(3,q)$ is generated by its subgroups $L_1 = Y$ and L_2. Y is a subgroup of $X_1(q)$ and L_2 is a subgroup of $X_2(q)$. Hence c can be expressed in terms of elements of $D_1 \cup D_2$, so we can eliminate it. We obtain

$$\sigma^*_G = \langle D_1 \cup D_2 \ \mid R_1 \cup R_2 \cup R_3^c \cup R_{23} \rangle.$$

Finally, since $\Delta_2 \cap \Delta_3 = A_1$ and the corresponding simply connected group $X_{23}(q) \cong \mathrm{SL}\,(2,q)$ is 2-generated (Proposition 3.9), the relations R_{23} need to pairwise identify these two generators in $X_2(q)$ and $X_3(q)$, so $|R_{23}| = 2$.
So G has a presentation with 5 generators and $19+5+2 = 26$ relations (5 generators and $15+5+2 = 22$ relations when q is even).

3.3.3 $\widetilde{A}_3(q)$

To obtain a presentation of $G = \widetilde{A}_3(q)$, we start with Proposition 3.21.



We let Δ_1 be the subdiagram of Δ based on the vertices a_0, a_1 and a_2, Δ_2 be the subdiagram of Δ based on a_0, a_1 and a_3, and Δ_3 be the subdiagram of Δ based on a_2 and a_3.
Now $\Delta = \cup_{i=1}^{3}\Delta_i$ and every pair of vertices is contained in at least one of the Δ_i, so G has a presentation

$$\sigma_G = \langle D_1 \cup D_2 \cup D_3 \mid R_1 \cup R_2 \cup R_3 \cup R_{12} \cup R_{13} \cup R_{23}\rangle.$$

By Proposition 3.18, the corresponding groups $X_1(q)$, $X_2(q)$ and $X_3(q)$ are simply connected. Δ_1 and Δ_2 have type A_3, so we have

$$X_1(q) \cong X_2(q) \cong \mathrm{SL}\,(4, q).$$

In particular, Table A.1 tells us that $X_1(q)$ has a presentation $\sigma_{X_1(q)} = \sigma_3$ with 5 generators and 20 relations (respectively ρ_3 with 5 generators and 16 relations if q is even).

Let us consider the subgroup X of G generated by L_0 and L_1. Its Dynkin diagram is of type A_2 and Proposition 3.18 says that it is simply connected, so $X \cong \mathrm{SL}\,(3, q)$. From Table A.1 we know that X has a presentation $\sigma_X = \langle D_X \mid R_X\rangle = \sigma_2$ with 4 generators and 14 relations (respectively ρ_2 with 4 generators and 10 relations if q is even).
Now X is a subgroup of both $X_1(q)$ and $X_2(q)$. Moreover Table A.1 says that $X_2(q)$ has a presentation $\sigma_{X_2(q)} = \sigma_4$ (respectively ρ_4 for q even) with $\sigma_X \subseteq \sigma_{X_2(q)}$. Since X is a subgroup of $X_1(q)$, $D_X \subseteq X_1(q)$ and the relations R_X already hold, so we can use Tietze transformations to remove them both from σ_G. And by definition R_{12} is the set of relations identifying the generators of $X_{12}(q) = X$ inside $X_1(q)$ and $X_2(q)$, but both of these are now written in terms of D_1, so these relations are superfluous and we can remove them too, obtaining:

$$\sigma_G' = \langle D_1 \cup (D_2 \setminus D_X) \cup D_3 \mid R_1 \cup (R_2 \setminus R_X) \cup R_3 \cup R_{13} \cup R_{23}\rangle.$$

Since σ_4 requires 6 generators and 21 relations, $|D_1 \cup (D_2 \setminus D_X)| = 5 + (6-4) = 7$ and $|R_1 \cup (R_2 \setminus R_X)| = 20 + (21-14) = 27$. For q even, ρ_4 requires 6 generators and 17 relations, so we have $|D_1 \cup (D_2 \setminus D_X)| = 5 + (6-4) = 7$ and $|R_1 \cup (R_2 \setminus R_X)| = 16 + (17-10) = 23$.

Take now $Y = L_3$. By Proposition 3.18 we have $Y \cong \mathrm{SL}\,(2, q)$ and $X_3(q) \cong \mathrm{SL}\,(3, q)$. Y is a subgroup of $X_3(q)$ and, without loss of generality, using Table A.1, we may assume that $\sigma_Y \subseteq \sigma_{X_3(q)}$ with $\sigma_Y = \sigma_1$ and $\sigma_{X_3(q)} = \sigma_2$ (respectively $\sigma_Y = \rho_1$ and $\sigma_{X_3(q)} = \rho_2$ for q even). Then by Theorem 5.1 of [GKaKasL11], $\sigma_{X_3(q)} = \langle D_Y \cup \{c\} \mid R_Y \cup R_3^c\rangle$ where $D_Y = \{u, t, h\}$ (in the notation of Theorem 5.1

of [GKaKasL11]) and R_3^c is a set of 5 relations involving c and elements of D_Y. Since Y is a subgroup of $X_2(q)$, the elements D_Y are obviously in $X_2(q)$. By the above, every element of $X_2(q)$ can be expressed in terms of elements of $D_1 \cup (D_2 \setminus D_X)$,thus u, t and h can be expressed in terms of elements of $D_1 \cup (D_2 \setminus D_X)$. Moreover, the relations R_Y hold, as they hold in $X_2(q)$. So we can use Tietze transformations to eliminate D_Y and R_Y. Finally, as above, the relations R_{23} are no longer required since they now identify subgroups that are already equal, so we get

$$\sigma''_G = \langle D_1 \cup (D_2 \setminus D_X) \cup \{c\} \mid R_1 \cup (R_2 \setminus D_X) \cup R_3^c \cup R_{13} \rangle.$$

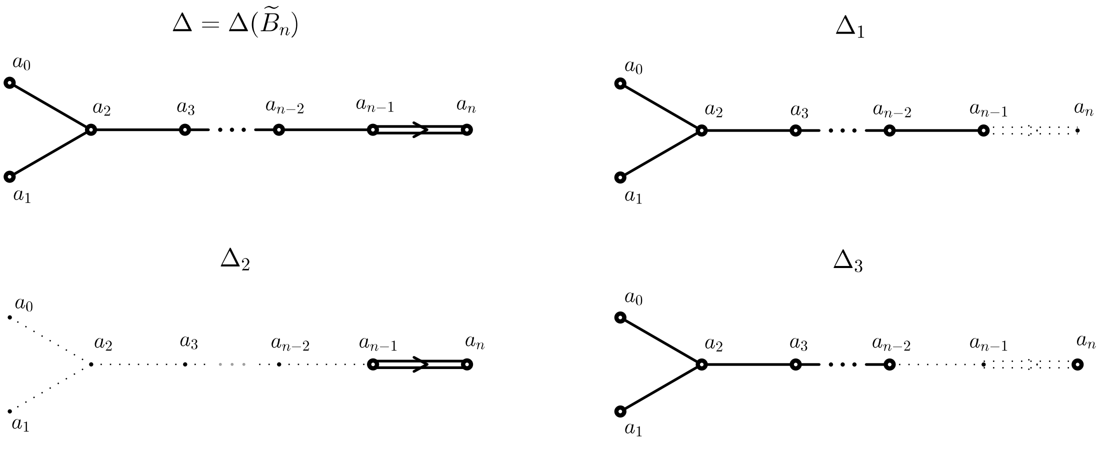
Recall that Lemma 3.19 says that $X_3(q) \cong \mathrm{SL}\,(3,q)$ is generated by its subgroups L_2 and L_3. L_2 is a subgroup of $X_1(q)$ and L_3 is a subgroup of $X_2(q)$, hence c can be expressed in terms of elements of $D_1 \cup (D_2 \setminus D_X)$, so we can remove it. Finally, since $\Delta_1 \cap \Delta_3 = A_1$ and the corresponding simply connected group $X_{13} = L_2 \cong \mathrm{SL}\,(2,q)$ is 2-generated (Proposition 3.9), we need two relations to pairwise identify these two generators inside $X_1(q)$ and $X_3(q)$, hence $|R_{13}| = 2$. Therefore

$$\sigma^*_G = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus D_X) \cup R_3^c \cup R_{13} \rangle,$$

and so G has a presentation with 7 generators and $27 + 5 + 2 = 34$ relations (respectively 7 generators and $23 + 5 + 2 = 30$ relations if q is even).

3.3.4 $\widetilde{B}_n(q)$, $n \geq 9$

To obtain a presentation of $G = \widetilde{B}_n(q)$, $n \geq 9$, we use Corollary 3.23.
Let Δ_1 be the subdiagram of Δ whose vertices are the n nodes $a_0, a_1, \ldots, a_{n-1}$. Let Δ_2 be the subdiagram of Δ whose vertices are the nodes a_{n-1} and a_n. Then Δ_3 is the subdiagram of Δ based on all vertices but a_{n-1}.



By Proposition 3.18, the corresponding groups $X_1(q)$, $X_2(q)$ and $X_3(q)$ are simply connected. Δ_1 has type D_n so we have

$$X_1(q) \cong \mathrm{Spin}\,(2n, q).$$

Δ_2 has type C_2 and so

$$X_2(q) \cong \mathrm{Sp}\,(4, q).$$

Δ_3 is of type $D_{n-1} \times A_1$ hence

$$X_3(q) \cong \mathrm{Spin}\,(2n-2, q) \times \mathrm{SL}\,(2, q).$$

Clearly, $\Delta = \Delta_1 \cup \Delta_2$. Therefore, as described in Corollary 3.23, G has a presentation

$$\sigma_G = \langle D_1 \cup D_2 \mid R_1 \cup R_2 \cup R_3^* \cup R_{12} \rangle.$$

Consider a subgroup $X = L_{n-1}$ of G. Its Dynkin diagram is of type A_1. Proposition 3.18 asserts that this subgroup is simply connected, and thus $X \cong \mathrm{SL}\,(2, q)$. From Table A.1 we know that X has a presentation $\sigma_X = \langle D_X \mid R_X \rangle = \sigma_1$ with $|D_X| = 3$ and $|R_X| = 9$ (respectively ρ_1 with $|D_X| = 3$ and $|R_X| = 5$ if q is even).
Now X is a subgroup of both $X_1(q)$ and $X_2(q)$. The group $X_2(q)$ has a presentation $\sigma_{X_2(q)} = \sigma_9$, with 5 generators and 27 relations, if q is odd, and $\sigma_{X_2(q)} = \rho_{10}$, with 6 generators and 20 relations, if q is even. From Section 3.2 we know that $X_1(q)$ has a presentation $\sigma_{X_1(q)} = \sigma_{15}$, with 7 generators and 34 relations (respectively ρ_{15}, with 7 generators and 30 relations, if q is even), and that $\sigma_X \subseteq \sigma_{X_1(q)}$.

Since X is a subgroup of $X_2(q)$, the elements D_X are obviously in $X_2(q)$, so we can write them in terms of D_2. Moreover, the relations R_X hold, as they already hold in $X_2(q)$. So we can use Tietze transformations to eliminate D_X and R_X. This causes the relations R_{12} to become redundant, so we can remove them too, obtaining:

$$\sigma_G' = \langle (D_1 \setminus D_X) \cup D_2 \mid (R_1 \setminus R_X) \cup R_2 \cup R_3^* \rangle.$$

We have $|(D_1 \setminus D_X) \cup D_2| = (7-3)+5 = 9$ and $|(R_1 \setminus R_X) \cup R_2| = (34-9)+27 = 52$ if q is odd, and $|(D_1 \setminus D_X) \cup D_2| = (7-3)+6 = 10$ and $|(R_1 \setminus R_X) \cup R_2| = (30-5)+20 = 45$ if q is even.

It only remains to compute $|R_3^*|$. Consider $X_3(q) \cong \mathrm{Spin}\,(2n-2, q) \times \mathrm{SL}\,(2, q)$. Each factor has two generators (Proposition 3.9). Denote them by a_1, a_2 and b_1, b_2 respectively. Then R_3^* is the set of relations that ensure that $X_3^1(q) \cong \mathrm{Spin}\,(2n-2, q)$

commutes with $X_3^2(q) \cong \mathrm{SL}\,(2,q)$ and so

$$R_3^* = \{[a_1,b_1] = [a_1,b_2] = [a_2,b_1] = [a_2,b_2] = 1\}$$

and hence $|R_3^*| = 4$.

Therefore G has a presentation with 9 generators and $52 + 4 = 56$ relations if q is odd, and 10 generators and $45 + 4 = 49$ relations if q is even.

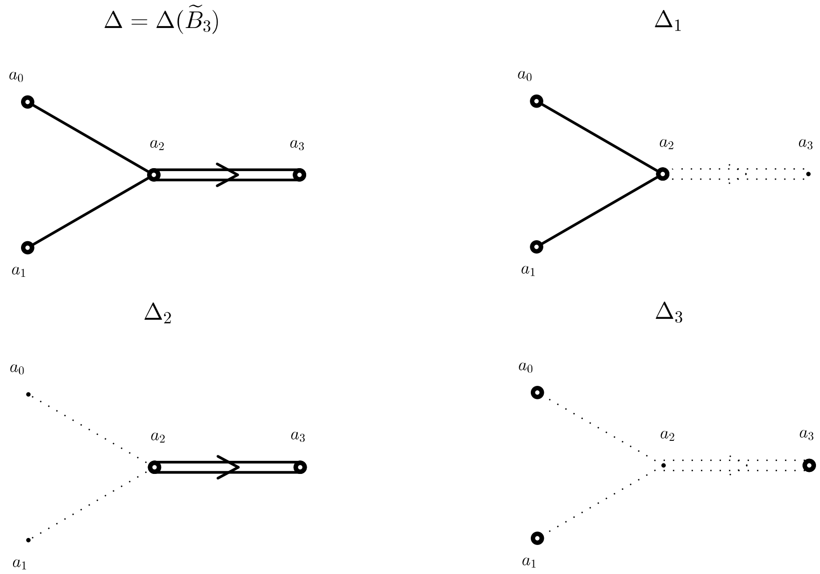
3.3.5 $\widetilde{B}_n(q),\ 3 \leq n \leq 8$

To obtain a presentation of $G = \widetilde{B}_n(q)$ for $4 \leq n \leq 8$, we use Corollary 3.23 just as in the previous case, making use of the smaller presentations of $X_1(q) \cong \mathrm{Spin}\,(2n,q)$ now available to us.

If $G = \widetilde{B}_4(q)$, Δ_1 is of type D_4, and so $X_1(q) \cong \mathrm{Spin}\,(8,q)$ and has a presentation $\sigma_{X_1(q)} = \sigma_{13}$ with 6 generators and 29 relations (or ρ_{13} with 6 generators and 25 relations if q is even). Using this in place of the σ_{15} (or ρ_{15}) we used previously gives us a presentation of G with $(6-3)+5 = 8$ generators and $(29-9)+27+4 = 51$ relations if q is odd, and $(6-3)+6 = 9$ generators and $(25-5)+20+4 = 44$ relations if q is even.

For $G = \widetilde{B}_n(q)$ with $5 \leq n \leq 8$, Δ_1 is of type D_n, and so $X_1(q) \cong \mathrm{Spin}\,(2n,q)$ and has a presentation $\sigma_{X_1(q)} = \sigma_{14}$ with 6 generators and 30 relations (or ρ_{14} with 6 generators and 26 relations if q is even). Using this in place of the σ_{15} (or ρ_{15}) in the general case gives us a presentation of G with $(6-3)+5 = 8$ generators and $(30-9)+27+4 = 52$ relations if q is odd, and $(6-3)+6 = 9$ generators and $(26-5)+20+4 = 45$ relations if q is even.

Now we do the final case of $G = \widetilde{B}_3(q)$. We use Corollary 3.23 again as in the previous case.



As before we take Δ_1 to be the subdiagram of Δ based on the vertices α_0, α_1 and α_2, and Δ_2 to be based on the vertices α_2 and α_3. Then Δ_3 consists of the three disconnected vertices α_0, α_1 and α_3.
Now Δ_1 is of type A_3 and Proposition 3.18 asserts that the corresponding subgroup is simply connected so we have

$$X_1(q) \cong \mathrm{SL}\,(4, q),$$

and Table A.1 gives us a presentation $\sigma_{X_1(q)} = \sigma_3$ with 5 generators and 20 relations (or ρ_3 with 5 generators and 16 relations if q is even). Δ_2 is again of type C_2 so we have

$$X_2(q) \cong \mathrm{Sp}\,(4, q),$$

and this group has a presentation $\sigma_{X_2(q)} = \sigma_{10}$, with 6 generators and 28 relations, if q is odd and $\sigma_{X_2(q)} = \rho_{10}$, with 6 generators and 20 relations, if q is even. Note that we have chosen the larger presentation σ_{10} instead of σ_9 as in the previous case, since by Lemma 3.16 this presentation contains two copies of σ_1, corresponding to both a short and a long root.
Taking $X = L_2$ again, we have that X is a subgroup of both $X_1(q)$ and $X_2(q)$, $X \cong \mathrm{SL}\,(2, q)$, and X has a presentation $\sigma_X = \langle D_X \mid R_X \rangle = \sigma_1$ (or ρ_1 if q is even) with $\sigma_X \subseteq \sigma_{X_2(q)}$. Since X is a subgroup of $X_1(q)$, the generators D_X are themselves in $X_1(q)$, and the relations R_X hold, since they already hold in $X_1(q)$. So we can use Tietze transformations to remove R_X and D_X. As before this causes the relations R_{12} to become superfluous, so we can eliminate them too.

We obtain that G has a presentation

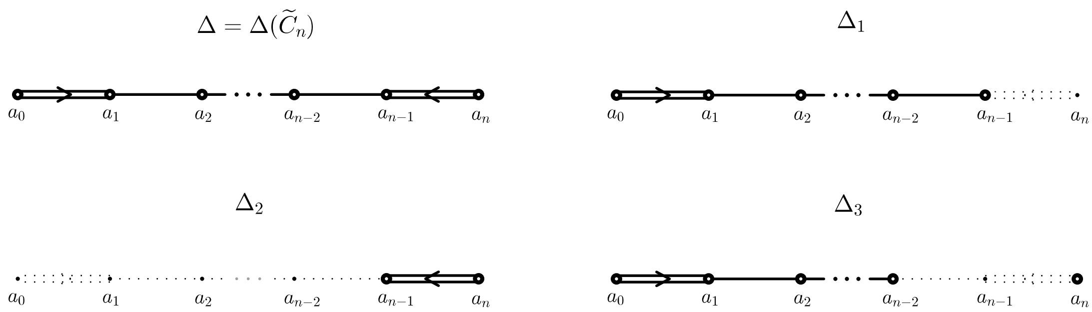
$$\sigma'_G = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus R_X) \cup R_3^* \rangle.$$

Finally, we have $X_3(q) = (X_1(q) \cap X_3(q)) \times (X_2(q) \cap X_3(q)) = (\mathrm{SL}\,(2,q) \times \mathrm{SL}\,(2,q)) \times \mathrm{SL}\,(2,q)$. Each factor is 2-generated (using Proposition 3.9), so as before we obtain that $|R_3^*| = 4$.

So G has a presentation with $5 + (6-3) = 8$ generators and $20 + (28-9) + 4 = 43$ relations if q is odd, and $5 + (6-3) = 8$ generators and $16 + (20-5) + 4 = 35$ relations if q is even.

3.3.6 $\widetilde{C}_n(q)$, $n \geq 3$

To obtain a presentation of $G = \widetilde{C}_n(q)$, $n \geq 3$, we use Corollary 3.23.



Let Δ_1 be the subdiagram of Δ whose vertices are the n nodes $a_0, \ldots, a_{n-1}$. Let Δ_2 be the subdiagram of Δ whose vertices are the nodes a_{n-1} and a_n. Then Δ_3 is the subdiagram of Δ based on all vertices but a_{n-1}.

By Proposition 3.18, the groups $X_1(q)$, $X_2(q)$ and $X_3(q)$ are simply connected.

Δ_1 has type C_n so

$$X_1(q) \cong \mathrm{Sp}\,(2n, q).$$

Δ_2 is of type C_2 and so

$$X_2(q) \cong \mathrm{Sp}\,(4, q).$$

Finally Δ_3 is of type $A_1 \times C_{n-1}$ hence

$$X_3(q) \cong \mathrm{SL}\,(2,q) \times \mathrm{Sp}\,(2n-2, q).$$

Clearly, $\Delta = \Delta_1 \cup \Delta_2$. Therefore G has a presentation

$$\sigma_G = \langle D_1 \cup D_2 \mid R_1 \cup R_2 \cup R_3^* \cup R_{12} \rangle.$$

as described in Corollary 3.23.

From Table A.1 we take a presentation $\sigma_{X_1(q)} = \sigma_{11}$, with 8 generators and 47 relations, if q is odd, and $\sigma_{X_1(q)} = \rho_{11}$, with 9 generators and 40 relations, if q is even.

Consider a subgroup $X = L_{n-1}$ of G. Its Dynkin diagram is of type A_1 and by Proposition 3.18 the corresponding subgroup is simply connected, so we have $X \cong \mathrm{SL}\,(2,q)$. We also know that X has a presentation $\sigma_X = \langle D_X \mid R_X \rangle = \sigma_1$ with $|D_X| = 3$ and $|R_X| = 9$ (or ρ_1 with $|D_X| = 3$ and $|R_X| = 5$ if q is even).

Now X is a subgroup of both $X_1(q)$ and $X_2(q)$. The group $X_2(q)$ has a presentation $\sigma_{X_2(q)} = \sigma_9$, with 5 generators and 27 relations, if q is odd, and $\sigma_{X_2(q)} = \rho_{10}$, with 6 generators and 20 relations, if q is even. X corresponds to the short root of $X_2(q)$, so recall from Lemma 3.16 that $\sigma_X \subseteq \sigma_{X_2(q)}$. Since $X \leq X_1(q)$, obviously, $D_X \subseteq X_1(q)$. Thus elements of D_X can be expressed in terms of elements of D_1. Moreover, the relations R_X hold, as they hold in $X_1(q)$. We use Tietze transformations to eliminate D_X and R_X. As before, this causes the relations R_{12} to be redundant, so we can remove them too.

We obtain that G has a presentation

$$\sigma'_G = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus R_X) \cup R_3^* \rangle.$$

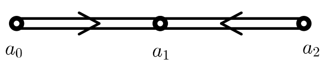
We have $|D_1 \cup (D_2 \setminus D_X)| = 8+(5-3) = 10$ and $|R_1 \cup (R_2 \setminus R_X)| = 47+(27-9) = 65$ if q is odd, and $|D_1 \cup (D_2 \setminus D_X)| = 9+(6-3) = 12$ and $|R_1 \cup (R_2 \setminus R_X)| = 40+(20-5) = 55$ if q is even.

Finally, consider $X_3(q) \cong \mathrm{Sp}\,(2n-2,q) \times \mathrm{SL}\,(2,q)$. Each factor has two generators (Proposition 3.9). Thus as in the previous cases we obtain $|R_3^*| = 4$.

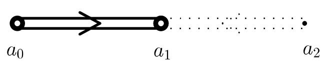
Therefore G has a presentation with 10 generators and $65+4 = 69$ relations if q is odd, and 12 generators and $55+4 = 59$ relations if q is even.

3.3.7 $\widetilde{C}_2(q)$

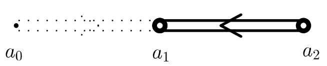
$\Delta = \Delta(\widetilde{C}_2)$



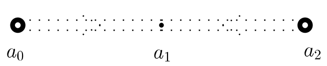
Δ_1



Δ_2



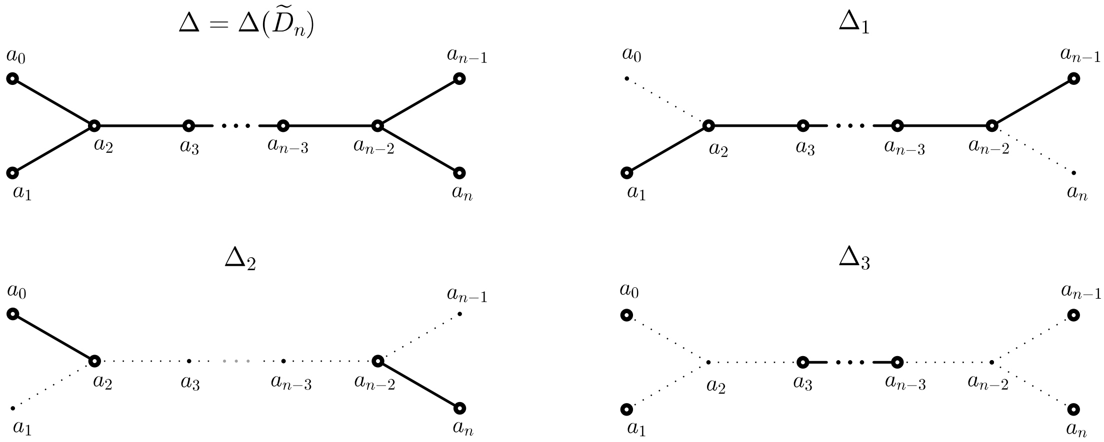
Δ_3



The only difference with the previous case is that $\Delta_1 = C_2$, and thus $X_2(q)$ has a presentation $\sigma_{X_1(q)} = \sigma_9$ if q is odd and $\sigma_{X_1(q)} = \rho_{10}$ if q is even. Replacing σ_{11} and ρ_{11} by these, we obtain that $G = \widetilde{C}_2(q)$ has a presentation with $5 + (5-3) = 7$ generators and $27 + (27-9) + 4 = 49$ relations if q is odd, and with $6 + (6-3) = 9$ generators and $20 + (20-5) + 4 = 39$ relations is q is even.

3.3.8 $\widetilde{D}_n(q), n \geq 6$

We start by assuming that $n \geq 9$. To obtain a presentation of $G = \widetilde{D}_n(q)$ we use Corollary 3.23.
Let Δ_1 be the subdiagram of Δ based on the $n-1$ vertices $a_1, a_2, ..., a_{n-1}$. Let Δ_2 be the subdiagram of Δ based on the vertices a_0, a_2, a_{n-2} and a_n. Then Δ_3 is the subdiagram of Δ based on all vertices but a_2 and a_{n-2}.



By Proposition 3.18, the corresponding groups $X_1(q)$, $X_2(q)$ and $X_3(q)$ are simply connected. Δ_1 has type A_{n-1} so we have

$$X_1(q) \cong \mathrm{SL}\,(n, q).$$

Δ_2 has type $A_2 \times A_2$ and so

$$X_2(q) \cong \mathrm{SL}\,(3, q) \times \mathrm{SL}\,(3, q).$$

Δ_3 is of type $(A_1)^4 \times A_{n-5}$ hence

$$X_3(q) \cong (\mathrm{SL}\,(2, q))^4 \times \mathrm{SL}\,(n-4, q).$$

Clearly we have $\Delta = \Delta_1 \bigcup \Delta_2$. Therefore, as described in Corollary 3.23, G

has a presentation

$$\sigma_G = \langle D_1 \cup D_2 \mid R_1 \cup R_2 \cup R_3^* \cup R_{12} \rangle.$$

Now $X_1(q)$ has a presentation $\sigma_{X_1(q)} = \sigma_7$ with 6 generators and 25 relations (or ρ_7 with 6 generators and 21 relations if q is even).
Consider a subgroup X of G generated by L_2 and L_{n-2}. Its Dynkin diagram is of type $A_1 \times A_1$ and by Proposition 3.18 the corresponding group is simply connected, so we have $X \cong \mathrm{SL}\,(2,q) \times \mathrm{SL}\,(2,q)$. From Table A.1 it follows that X has a presentation

$$\sigma_X = \langle D_X^2 \cup D_X^{n-2} \mid R_X^2 \cup R_X^{n-2} \cup R_X^* \rangle$$

where $\sigma_X^2 = \langle D_X^2 \mid R_X^2 \rangle$ is a presentation of $L_2 \cong \mathrm{SL}\,(2,q)$, $\sigma_X^2 = \sigma_1$ (or ρ_1 if q is even), $\sigma_X^{n-2} = \langle D_X^{n-2} \mid R_X^{n-2} \rangle$ is a presentation of $L_{n-2} \cong \mathrm{SL}\,(2,q)$, $\sigma_X^{n-2} = \sigma_1$ (or ρ_1), and R_X^* are the relations that ensure that $[L_2, L_{n-2}] = 1$. Proposition 3.9 says that both L_2 and L_{n-2} are 2-generated, so we may chose $c_1, c_2 \in L_2$ and $d_1, d_2 \in L_{n-2}$ so that $R_X^* = \{[c_i, d_j] = 1, 1 \le i, j \le 2\}$. Hence, $|R_X^*| = 4$.

Now X is a subgroup of both $X_1(q)$ and $X_2(q)$. Moreover $X_2(q)$ has a presentation $\sigma_{X_2(q)}$ with $\sigma_X \subseteq \sigma_{X_2(q)}$. Indeed, take $\sigma_{X_2(q)} = \langle D_2 \mid R_2 \rangle$ such that $D_2 = D_2^2 \cup D_2^{n-2}$ and $R_2 = R_2^2 \cup R_2^{n-2} \cup R_2^*$ where for $i = 2$ and $n-2$, $\sigma_{X_2(q)}^i = \langle D_2^i \mid R_2^i \rangle$ is a presentation of a subgroup $L_{0,2}$ of $X_2(q)$ if $i = 2$, and $L_{n-2,n}$ if $i = n-2$, $\sigma_{X_2(q)}^i = \langle D_2^i \mid R_2^i \rangle = \sigma_2$ and R_2^* are the relations that ensure that $[L_{0,2}, L_{n-2,n}] = 1$. Now Proposition 3.9 says that both $L_{0,2}$ and for $L_{n-2,n}$ are 2-generated, and Corollary 3.11 says that we can freely choose one of the generators in the corresponding generating pairs, so we may take $c_1', c_2' \in L_{0,2}$ and $d_1', d_2' \in L_{n-2,n}$ with $c_1' = c_1$, $d_1' = d_1$. Then let $R_2^* = R_X^* \cup \{[c_1', d_2'] = [c_2', d_1'] = [c_2', d_2'] = 1\}$. Then $R_X^* \subseteq R_2^*$ and $|R_2^* \setminus R_X^*| = 3$.

Since $X \le X_1(q)$, $D_X \subseteq X_1(q)$ and relations R_X already hold in $X_1(q)$. We use Tietze transformations to eliminate D_X, R_X and R_{12}:

$$\sigma_G' = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus R_X) \cup R_3^* \rangle.$$

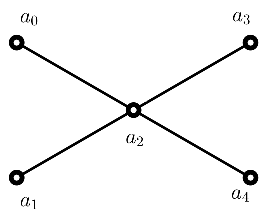
Notice that $|D_1 \cup (D_2 \setminus D_X)| = 6 + (4-3) + (4-3) = 8$ and $|R_1 \cup (R_2 \setminus R_X)| = 25 + (14-9) + (14-9) + 3 = 38$.

Finally, $X_3(q) = (X_3(q) \cap X_1(q)) \times (X_3(q) \cap X_2(q))$ where $X_3(q) \cap X_1(q) = L_1 \times \langle L_3, ..., L_{n-3} \rangle \times L_{n-1} \cong \mathrm{SL}\,(2,q) \times \mathrm{SL}\,(n-4,q) \times \mathrm{SL}\,(2,q)$ and $X_3(q) \cap X_2(q) = L_0 \times L_n \cong \mathrm{SL}\,(2,q) \times \mathrm{SL}\,(2,q)$. Since each of the factors requires only two generators (Proposition 3.9), we obtain that $|R_3^*| = 4$. Therefore G has a presentation with 8 generators and 42 relations if q is odd. For even q the corresponding calculation gives 8 generators and $21 + ((10-5) + (10-5) + 3) + 4 = 38$ relations.

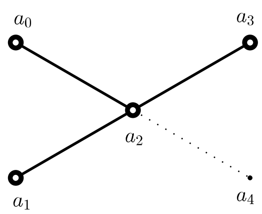
If $6 \le n \le 8$, then the above argument works with little variation. The subgroup $X_1(q) \cong \mathrm{SL}\,(n,q)$ has a presentation $\sigma_{X_1(q)} = \sigma_5$ with 5 generators and 21 relations. The rest of the argument does not change, producing a presentation of G with 7 generators and 38 relations if q is odd and 7 generators and 34 relations if q is even.

3.3.9 $\widetilde{D}_n(q), n = 4, 5$

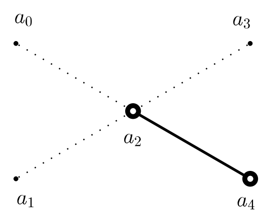
$\Delta = \Delta(\widetilde{D}_4)$



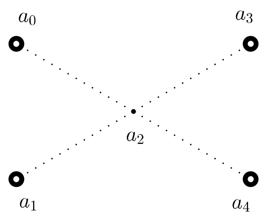
Δ_1



Δ_2



Δ_3



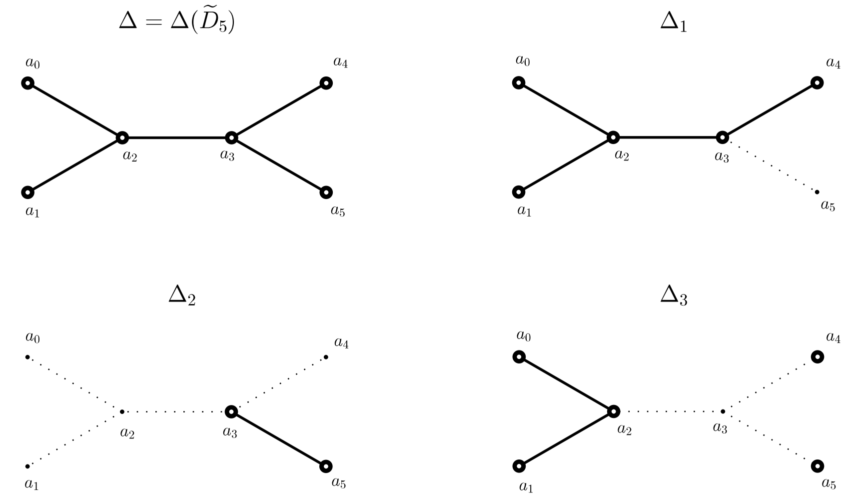
This time we use Corollary 3.23 with $\Delta_1 = D_n$ based on all vertices but a_0, and $\Delta_2 = A_2$ based on vertices a_0 and a_2. Then $X_1(q) \cong \mathrm{Spin}\,(2n,q)$ and $X_2(q) \cong \mathrm{SL}\,(3,q)$. Thus $\Delta_3 = A_1^4$ if $n = 4$, and $\Delta_3 = A_1^2 \times A_3$ if $n = 5$, giving $X_3(q) \cong \mathrm{SL}\,(2,q)^4$ and $X_3(q) \cong \mathrm{SL}\,(2,q)^2 \times \mathrm{SL}\,(4,q)$ respectively.

Consider a subgroup $X = L_2$ of G. Then $X \leq X_i(q)$ for $i = 1, 2$, $X \cong \mathrm{SL}\,(2,q)$ and X has a presentation $\sigma_X = \langle D_X \mid R_X \rangle = \sigma_1$. Now $X_1(q)$ has a presentation $\sigma_{X_1(q)} = \sigma_{13}$ if $n = 4$ and $\sigma_{X_1(q)} = \sigma_{14}$ if $n = 5$. The group $X_2(q)$ has a presentation $\sigma_{X_2(q)} = \sigma_2$ and $\sigma_X \subseteq \sigma_{X_2(q)}$. Since $X \leq X_1(q)$, $D_X \subseteq X_1(q)$ and R_X hold as they hold in $X_1(q)$. We use Tietze transformations to eliminate D_X, R_X and R_{12} to obtain a presentation

$$\sigma_G = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus R_X) \cup R_3^* \rangle$$

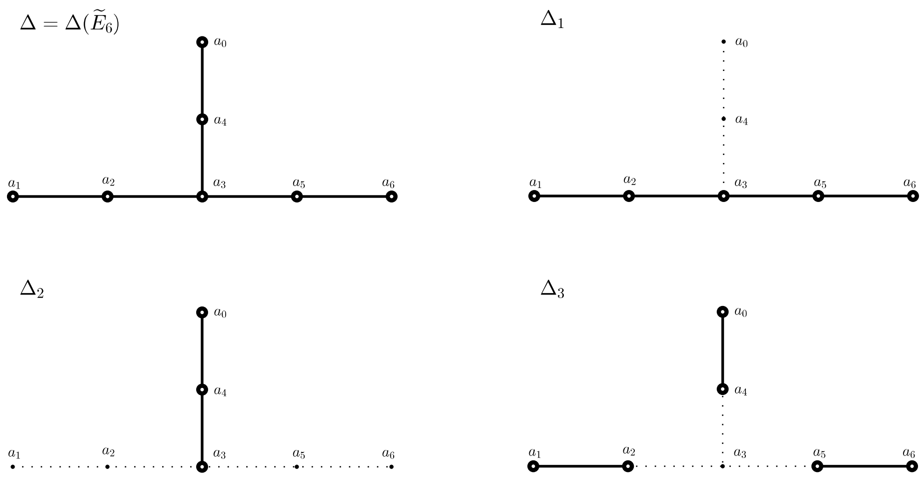
where as usual $|R_3^*| = 4$ (using Proposition 3.9). Thus G has a presentation with $6 + (4-3) = 7$ generators and $29 + (14-9) + 4 = 38$ relations if $n = 4$, and $6 + (4-3) = 7$ generators and $30 + (14-9) + 4 = 39$ relations if $n = 5$. For even

q the corresponding calculations give $25 + (10 - 5) + 4 = 34$ relations if $n = 4$ and $26 + (10 - 5) + 4 = 35$ relations if $n = 5$.



3.3.10 $\widetilde{E}_6(q)$

This time we use Corollary 3.23. Take $\Delta_1 = A_5$ on vertices a_1, a_2, a_3, a_5 and a_6, $\Delta_2 = A_3$ on vertices a_0, a_4 and a_3. Then $\Delta_3 = A_2 \times A_2 \times A_2$ is based on all vertices but a_3.



Hence, $G = \widetilde{E}_6(q)$ has a presentation

$$\sigma_G = \langle D_1 \cup D_2 \mid R_1 \cup R_2 \cup R_3^* \cup R_{12} \rangle.$$

Using Proposition 3.18 and Table 3 we have that $X_1 \cong \mathrm{SL}\,(6, q)$ has a presentation $\sigma_{X_1(q)} = \sigma_5$, and $X_2 \cong \mathrm{SL}\,(4, q)$ has a presentation $\sigma_{X_2(q)} = \sigma_3$.

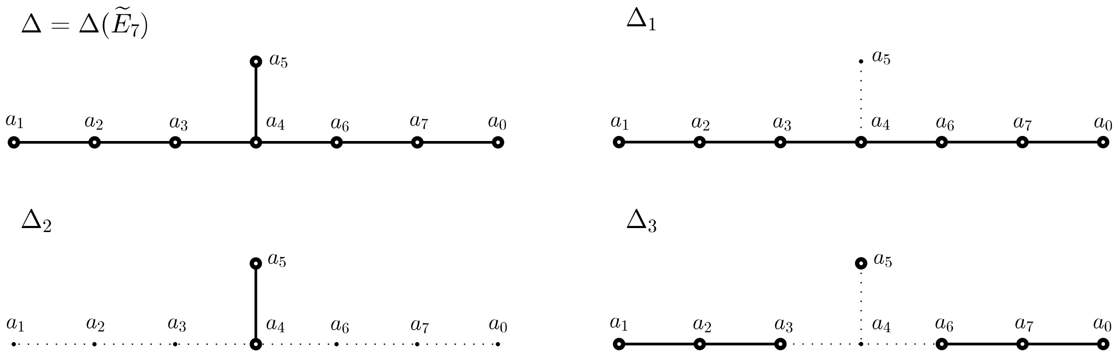
Consider a subgroup $X = L_3 \cong \mathrm{SL}\,(2,q)$ of G. Then X has a presentation $\sigma_X = \langle D_X \mid R_X \rangle = \sigma_1$. Now $X \leq X_i(q)$ for $i = 1,2$, and Lemma 3.15 implies that $\sigma_X \subseteq \sigma_{X_2(q)}$. Since $X \leq X_1(q)$, $D_X \subseteq X_1(q)$ and the relations R_X hold (as they hold in $X_1(q)$). We use Tietze transformations to eliminate D_X, R_X and R_{12}. Hence, G has a presentation

$$\sigma'_G = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus R_X) \cup R_3^* \rangle.$$

Finally, $X_3(q) = (X_3(q) \cap X_1(q)) \times (X_3(q) \cap X_2(q)) \cong (\mathrm{SL}\,(3,q) \times \mathrm{SL}\,(3,q)) \times \mathrm{SL}\,(3,q)$. Both factors require 2 generators (Proposition 3.9), implying $|R_3^*| = 4$. Therefore G has a presentation with $5 + (5-3) = 7$ generators and $21 + (20-9) + 4 = 36$ relations if q is odd. For even q the corresponding calculation gives 7 generators and $17 + (16-5) + 4 = 32$ relations.

3.3.11 $\widetilde{E}_7(q)$

Again we use Corollary 3.23. Take $\Delta_1 = A_7$ based on all vertices but a_5, and $\Delta_2 = A_3$ based on vertices a_4 and a_5. Then $\Delta_3 = A_3 \times A_3 \times A_1$ is based on all vertices but a_4.



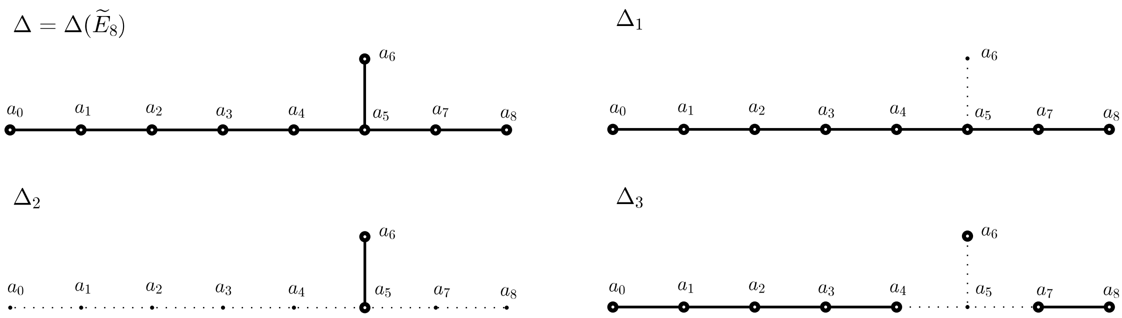
Hence, $G = \widetilde{E}_7(q)$ has a presentation as described in Corollary 3.23. Using Proposition 3.18 and Table 3 we have that $X_1 \cong \mathrm{SL}\,(8,q)$ has a presentation $\sigma_{X_1(q)} = \sigma_5$, $X_2 \cong \mathrm{SL}\,(3,q)$ has a presentation $\sigma_{X_2(q)} = \sigma_2$. Consider a subgroup $X = L_4 \cong \mathrm{SL}\,(2,q)$ of G. Then X has a presentation $\sigma_X = \langle D_X \mid R_X \rangle = \sigma_1$. Now $X \leq X_i(q)$ for $i = 1,2$, and $\sigma_X \subseteq \sigma_{X_2(q)}$. Since $X \leq X_1(q)$, $D_X \subseteq X_1(q)$ and the relations R_X hold (as they hold in $X_1(q)$). We use Tietze transformations to eliminate D_X, R_X and R_{12}. Hence, G has a presentation

$$\sigma'_G = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus R_X) \cup R_3^* \rangle.$$

Finally, $X_3(q) = (X_3(q) \cap X_1(q)) \times (X_3(q) \cap X_2(q)) \cong (\mathrm{SL}\,(4,q) \times \mathrm{SL}\,(4,q)) \times \mathrm{SL}\,(2,q)$. Both factors require 2 generators (Proposition 3.9), implying $|R_3^*| = 4$. Therefore G has a presentation with $5 + (4-3) = 6$ generators and $21 + (14-9) + 4 = 30$ relations if q is odd. If q is even the corresponding calculation gives 6 generators and $17 + (10-5) + 4 = 26$ relations.

3.3.12 $\widetilde{E}_8(q)$

We use Corollary 3.23. Take $\Delta_1 = A_8$ based on all vertices but a_6, and $\Delta_2 = A_2$ based on vertices a_5 and a_6. Then $\Delta_3 = A_5 \times A_2 \times A_1$ is based on all vertices but a_5.



Hence, $G = \widetilde{E}_8(q)$ has a presentation as described in Corollary 3.23. Using Proposition 3.18 and Table 3 we have that $X_1 \cong \mathrm{SL}\,(9,q)$ has a presentation $\sigma_{X_1(q)} = \sigma_7$, $X_2 \cong \mathrm{SL}\,(3,q)$ has a presentation $\sigma_{X_2(q)} = \sigma_2$. Consider a subgroup $X = L_5 \cong \mathrm{SL}\,(2,q)$ of G. Then X has a presentation $\sigma_X = \langle D_X \mid R_X \rangle = \sigma_1$. Now $X \leq X_i(q)$ for $i = 1,2$, and $\sigma_X \subseteq \sigma_{X_2(q)}$. Since $X \leq X_1(q)$, $D_X \subseteq X_1(q)$ and the relations R_X hold (as they hold in $X_1(q)$). We use Tietze transformations to eliminate D_X, R_X and R_{12}. Hence, G has a presentation

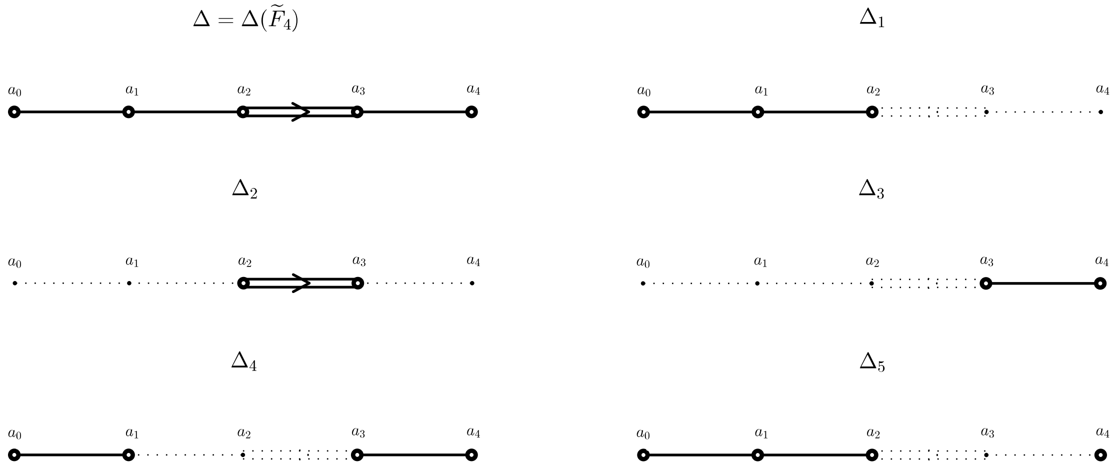
$$\sigma'_G = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus R_X) \cup R_3^* \rangle.$$

Finally, $X_3(q) = (X_3(q) \cap X_1(q)) \times (X_3(q) \cap X_2(q)) \cong (\mathrm{SL}\,(6,q) \times \mathrm{SL}\,(3,q)) \times \mathrm{SL}\,(2,q)$. Both factors require 2 generators (Proposition 3.9), implying $|R_3^*| = 4$. Therefore G has a presentation with $6 + (4-3) = 7$ generators and $25 + (14-9) + 4 = 34$ relations if q is odd. If q is even we get 7 generators and $21 + (10-5) + 4 = 30$ relations.

3.3.13 $\widetilde{F}_4(q)$

The following proof is somewhat more convoluted than the ones we have seen so far. It is possible to find a presentation of $\widetilde{F}_4(q)$ using Corollary 3.23, but the more careful method described here gives us a smaller presentation.

We apply Proposition 3.21 with $k = 5$. Take $\Delta_1 = A_3$ based on vertices a_0, a_1 and a_2, $\Delta_2 = C_2$ based on vertices a_2 and a_3, $\Delta_3 = A_2$ based on vertices a_3 and a_4, $\Delta_4 = A_2 \times A_2$ based on all vertices but a_2, and finally $\Delta_5 = A_3 \times A_1$ based on all vertices but a_3.



Taking subgroups $X_i(q)$ corresponding to Δ_i for $1 \leq i \leq 5$, we obtain a presentation of G

$$\sigma_G = \langle D_1 \cup D_2 \cup D_3 \cup D_4 \cup D_5 \mid R_1 \cup R_2 \cup R_3 \cup R_4 \cup R_5 \cup \bigcup_{i<j} R_{ij} \rangle$$

as described in Proposition 3.21. Notice that $R_{13} = \emptyset$.

Using Proposition 3.18 and Table 3 we have that $X_1(q) \cong \mathrm{SL}\,(4, q)$ has a presentation $\sigma_{X_1(q)} = \sigma_3$, $X_2(q) \cong \mathrm{Sp}\,(4, q)$ has a presentation $\sigma_{X_2(q)} = \sigma_9$ (or ρ_{10} if q is even), and $X_3(q) \cong \mathrm{SL}\,(3, q)$ has a presentation $\sigma_{X_3(q)} = \sigma_2$.

Take $X = L_2 \cong \mathrm{SL}\,(2, q)$. Then $X \leq X_i(q)$ for $i = 1, 2$ and Lemma 3.15 implies that $\sigma_X \subseteq \sigma_{X_1(q)}$. Since $X \leq X_2(q)$, $D_X \subseteq X_2(q)$ and R_X hold as they hold in $X_2(q)$. We use Tietze transformations to eliminate D_X, R_X and R_{12} to obtain a presentation

$$\sigma_G^{(1)} = \langle (D_1 \setminus D_X) \cup D_2 \cup D_3 \cup D_4 \cup D_5 \mid (R_1 \setminus R_X) \cup R_2 \cup R_3 \cup R_4 \cup R_5 \cup \bigcup_{i<j} R_{ij} \setminus R_{12} \rangle.$$

Take $Y = L_3 \cong \mathrm{SL}\,(2, q)$. Then $Y \leq X_i(q)$ for $i = 2, 3$ and $\sigma_Y \subseteq \sigma_{X_3(q)}$. Again we use Tietze transformations. This time we eliminate D_Y, R_Y and R_{23} to obtain

$$\sigma_G^{(2)} = \langle (D_1 \setminus D_X) \cup D_2 \cup (D_3 \setminus D_Y) \cup D_4 \cup D_5 \mid \\ (R_1 \setminus R_X) \cup R_2 \cup (R_3 \setminus R_Y) \cup R_4 \cup R_5 \cup \bigcup_{i<j} R_{ij} \setminus (R_{12} \cup R_{23}) \rangle.$$

By Proposition 3.18, $X_4(q) = (X_4(q) \cap X_1(q)) \times X_3(q) \cong \mathrm{SL}\,(3,q) \times \mathrm{SL}\,(3,q)$. Each factor is 2-generated (Proposition 3.9). Let us denote these pairs of generators by c_1, c_2 and d_1, d_2 respectively. In fact, Corollary 3.11 allows us to choose $c_1 \in L_0 \leq X_4(q) \cap X_1(q)$ and $d_1 \in L_4 \leq X_3(q)$. Then $X_4(q)$ has a presentation $\sigma_{X_4(q)} = \langle c_1, c_2, d_1, d_2 \mid R_{c_1,c_2} \cup R_{d_1,d_2} \cup R_4^* \rangle$ where $\langle c_1, c_2 \mid R_{c_1,c_2} \rangle$ is a presentation of $X_4(q) \cap X_1(q) \cong \mathrm{SL}\,(3,q)$, $\langle d_1, d_2 \mid R_{d_1,d_2} \rangle$ is a presentation of $X_4(q) \cap X_3(q) = X_3(q) \cong \mathrm{SL}\,(3,q)$, and $R_4^* = \{[c_1,d_1] = [c_1,d_2] = [c_2,d_1] = [c_2,d_2] = 1\}$. Since $X_4(q) \cap X_1(q) \leq X_1(q)$, $c_1, c_2 \in X_1(q)$ and the relations R_{c_1,c_2} hold as they hold in $X_1(q)$. Similarly, $d_1, d_2 \in X_3(q)$ and relations R_{d_1,d_2} hold as they hold in $X_3(q)$. We now use Tietze transformations to eliminate c_1, c_2, d_1, d_2, $R_{c_1,c_2} \cup R_{d_1,d_2}$ and $R_{14} \cup R_{34}$. Now we may eliminate relations R_{24}: R_{24} identify $X_2(q) \cap X_4(q)$. Note that $X_2(q) \cap X_4(q) = (X_2(q) \cap X_3(q)) \cap (X_3(q) \cap X_4(q))$, and we have already identified $X_2(q) \cap X_3(q)$ and $X_3(q) \cap X_4(q)$. Thus G has a presentation

$$\sigma_G^{(3)} = \langle (D_1 \setminus D_X) \cup D_2 \cup (D_3 \setminus D_Y) \cup D_5 \mid \\ (R_1 \setminus R_X) \cup R_2 \cup (R_3 \setminus R_Y) \cup R_4^* \cup R_5 \cup \bigcup_{i=1}^{5} R_{i5} \rangle.$$

Finally, by Proposition 3.18, $X_5(q) = X_1(q) \times (X_3(q) \cap X_5(q)) \cong \mathrm{SL}\,(4,q) \times \mathrm{SL}\,(2,q)$. Each factor is 2-generated (Proposition 3.9). Let us denote these pairs of generators by c_1', c_2' and d_1', d_2' respectively. Notice that Corollary 3.11 implies that we may choose $c_1' = c_1$ and $d_1' = d_1$. Then $X_5(q)$ has a presentation $\sigma_{X_5(q)} = \langle c_1, c_2', d_1, d_2' \mid R_{c_1,c_2'} \cup R_{d_1,d_2'} \cup R_5^* \rangle$ where $\langle c_1, c_2' \mid R_{c_1,c_2'} \rangle$ is a presentation of $X_5(q) \cap X_1(q) = X_1(q) \cong \mathrm{SL}\,(4,q)$, $\langle d_1, d_2' \mid R_{d_1,d_2'} \rangle$ is a presentation of $X_3(q) \cap X_5(q) \cong \mathrm{SL}\,(2,q)$, and $R_5^* = \{[c_1,d_1] = [c_1,d_2'] = [c_2',d_1] = [c_2',d_2'] = 1\}$. Since $X_5(q) \cap X_1(q) = X_1(q)$, $c_1, c_2' \in X_1(q)$ and relations $R_{c_1,c_2'}$ hold as they hold in $X_1(q)$. Similarly, $d_1, d_2' \in X_3(q)$ and relations $R_{d_1,d_2'}$ hold as they hold in $X_3(q)$. We use Tietze transformations to eliminate c_1, c_2', d_1, d_2', $R_{c_1,c_2'} \cup R_{d_1,d_2'}$ and $R_{15} \cup R_{35}$ to obtain

$$\sigma_G^{(4)} = \langle (D_1 \setminus D_X) \cup D_2 \cup (D_3 \setminus D_Y) \mid (R_1 \setminus R_X) \cup R_2 \cup (R_3 \setminus R_Y) \cup R_4^* \cup R_5^* \cup R_{25} \cup R_{45} \rangle.$$

Now we may eliminate relations R_{25}: R_{25} identify $X_2(q) \cap X_5(q)$. Note that $X_2(q) \cap X_5(q) = (X_1(q) \cap X_2(q)) \cap (X_1(q) \cap X_5(q))$, and we have already identified $X_1(q) \cap X_2(q)$ and $X_1(q) \cap X_5(q)$. We may also eliminate relations R_{45}. Relations R_{45} identify $X_4(q) \cap X_5(q)$ which is a direct product of two components: $L_{01} = (X_1(q) \cap$

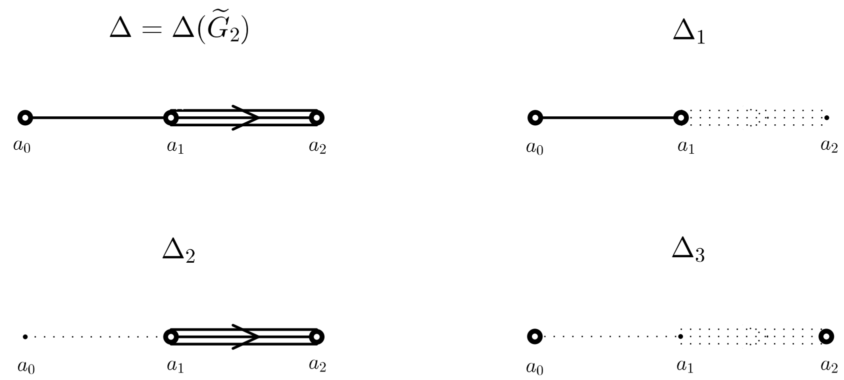
$X_4(q)) \cap (X_1(q) \cap X_5(q))$ and $L_4 = (X_3(q) \cap X_4(q)) \cap (X_3(q) \cap X_5(q))$, and we have already identified those.

Notice that $|R_4^* \cap R_5^*| = 1$ and so $|R_4^* \cup R_5^*| = 7$. Thus we have obtained a presentation

$$\sigma_G^{(5)} = \langle (D_1 \setminus D_X) \cup D_2 \cup (D_3 \setminus D_Y) \mid (R_1 \setminus R_X) \cup R_2 \cup (R_3 \setminus R_Y) \cup R_4^* \cup R_5^* \rangle$$

with $(5-3)+5+(4-3) = 8$ generators and $(20-9)+27+(14-9)+7 = 50$ relations if q is odd. If q is even the corresponding calculation gives $(5-3)+6+(4-3) = 9$ generators and $(16-5)+20+(10-5)+7 = 43$ relations.

3.3.14 $\widetilde{G}_2(q)$



We now use Corollary 3.23. Let Δ_1 be the subdiagram of Δ based on a_0 and a_1 and Δ_2 the subdiagram based on a_1 and a_2. Then Δ_3 is the subdiagram based on a_0 and a_2.
By Proposition 3.18, the corresponding groups $X_1(q)$, $X_2(q)$ and $X_3(q)$ are simply connected. Δ_1 is of type A_2 so we have

$$X_1(q) \cong \mathrm{SL}\,(3, q)$$

Δ_2 is of type G_2 so we have

$$X_2(q) \cong G_2(q).$$

And finally Δ_3 has type $A_1 \times A_1$ so

$$X_3(q) \cong \mathrm{SL}\,(2, q) \times \mathrm{SL}\,(2, q).$$

$X_1(q)$ has a presentation $\sigma_{X_1(q)} = \sigma_2$ and $X_2(q)$ has a presentation $\sigma_{X_2(q)} = \sigma_{17}$. We have $\Delta = \Delta_1 \cup \Delta_2$, therefore, in the notation of Corollary 3.23, G has a presentation

$$\sigma_G = \langle D_1 \cup D_2 \mid R_1 \cup R_2 \cup R_3^* \cup R_{12} \rangle.$$

Now take $X = L_1 \cong \mathrm{SL}\,(2, q)$. Then X is a subgroup of both $X_1(q)$ and $X_2(q)$. Also, X has a presentation $\sigma_X = \sigma_1$ which is contained in $\sigma_{X_1(q)}$, so we may use Tietze transformations to remove D_X, R_X and R_{12}, thus obtaining

$$\sigma_G = \langle (D_1 \setminus D_X) \cup D_2 \mid (R_1 \setminus R_X) \cup R_2 \cup R_3^* \rangle.$$

Since each $\mathrm{SL}\,(2, q)$ factor of $X_3(q)$ is 2-generated (Proposition 3.9), we obtain $|R_3^*| = 4$, and so σ_G has $4 - 3 + 6 = 7$ generators and $14 - 9 + 31 + 4 = 40$ relations.

We now use Corollary 3.23. Take Δ_1 based on a_0 and a_1, Δ_2 based on a_1 and a_2, and Δ_3 based on a_0 and a_2.

Then $X_1(q) \cong \mathrm{SL}\,(3, q)$ has a presentation $\sigma_{X_1(q)} = \sigma_2$, $X_2(q) \cong G_2(q)$ has a presentation $\sigma_{X_2(q)} = \sigma_{16}$. Take $X = L_1 \cong \mathrm{SL}\,(2, q)$. Then $X \leq X_i(q)$ for $i = 1, 2$. Since $X \leq X_2(q)$ and $\sigma_X \subseteq \sigma_{X_1(q)}$, we may use Tietze transformations to remove D_X, R_X and R_{12}, thus obtaining

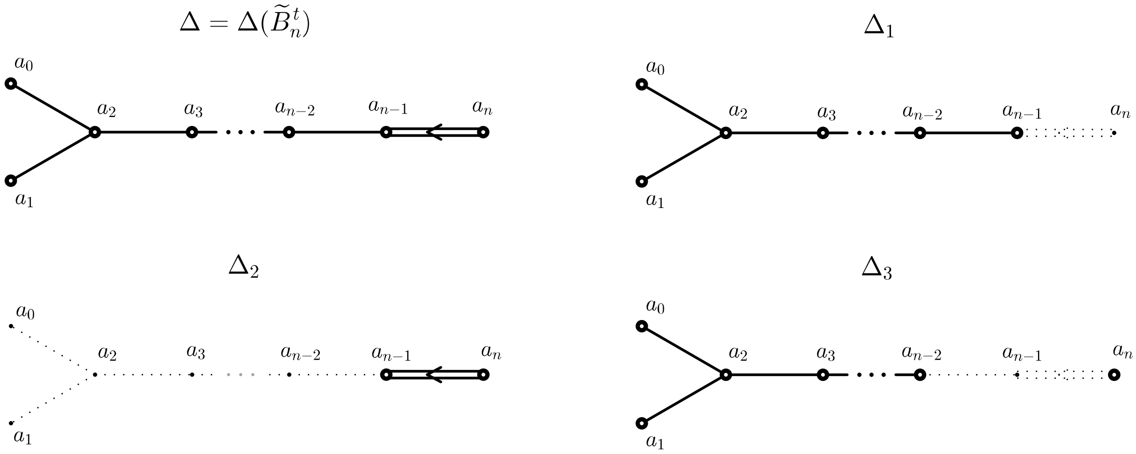
$$\sigma_G = \langle (D_1 \setminus D_X) \cup D_2 \mid (R_1 \setminus R_X) \cup R_2 \cup R_3^* \rangle.$$

Since $X_3(q) \cong \mathrm{SL}\,(2, q) \times \mathrm{SL}\,(2, q)$ and $\mathrm{SL}\,(2, q)$ is 2-generated (Proposition 3.9), we obtain $|R_3^*| = 4$, and so σ_G has $(4-3)+6 = 7$ generators and $(14-9)+31+4 = 40$ relations if q is odd. If q is even we get 7 generators and $(10 - 5) + 23 + 4 = 32$ relations.

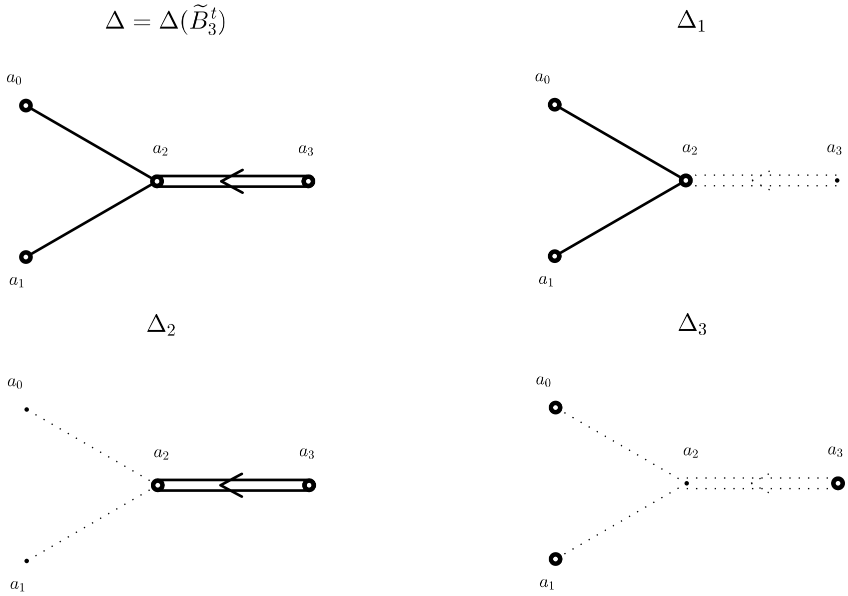
3.4 Twisted affine Kac-Moody groups

We briefly go through the calculations for the 3 infinite families and 2 exceptional types of twisted affine Kac-Moody groups of rank at least 3.

3.4.1 $\widetilde{B}_n^t(q)$



For $n \neq 3$, the proof is line by line repetition of the case $G = \widetilde{B}_n(q)$ giving us the same result: a presentation of G with 9 generators and 56 relations when q is odd, and with 10 generators and 49 relations when q is even, for $n \geq 9$, and the same results as for $\widetilde{B}_n(q)$ for $4 \leq n \leq 8$.

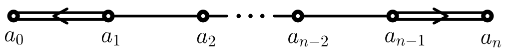


Now for $G = \widetilde{B}_3^t(q)$, we repeat the proof of the case $\widetilde{B}_3(q)$ line by line with one change: in the case when q is odd, we take $\sigma_{X_2(q)} = \sigma_9$, thus obtaining a presentation of G with $5+(5-3) = 7$ generators and $20+(27-9)+4 = 42$ relations if q is odd, and 8 generators and 35 relations if q is even.

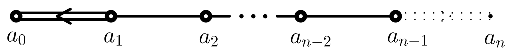
3.4.2 $\widetilde{C}_n^t(q)$

To obtain a presentation of $G = \widetilde{C}_n^t(q)$, $n \geq 3$, we use Corollary 3.23.

$\Delta = \Delta(\widetilde{C}_n^t)$

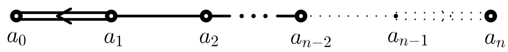


Δ_1



Δ_2

Δ_3



By Proposition 3.18, the groups $X_1(q)$, $X_2(q)$ and $X_3(q)$ are simply connected. Let $\Delta_1 = B_n$ be the subdiagram of Δ whose vertices are the n nodes $a_1, \ldots, a_n$, and $\Delta_2 = C_2$ the subdiagram of Δ whose vertices are the nodes a_0 and a_1. Then $X_1(q) \cong \mathrm{Spin}\,(2n+1, q)$ and $X_2(q) \cong \mathrm{Sp}\,(4, q)$. It follows that Δ_3 is the subdiagram of Δ based on all vertices but a_1, thus of type $A_1 \times B_{n-1}$. Hence, $X_3(q) \cong \mathrm{SL}\,(2, q) \times \mathrm{Spin}\,(2n-1, q)$. Clearly, $\Delta = \Delta_1 \cup \Delta_2$. Therefore G has a presentation

$$\sigma_G = \langle D_1 \cup D_2 \mid R_1 \cup R_2 \cup R_3^* \cup R_{12} \rangle.$$

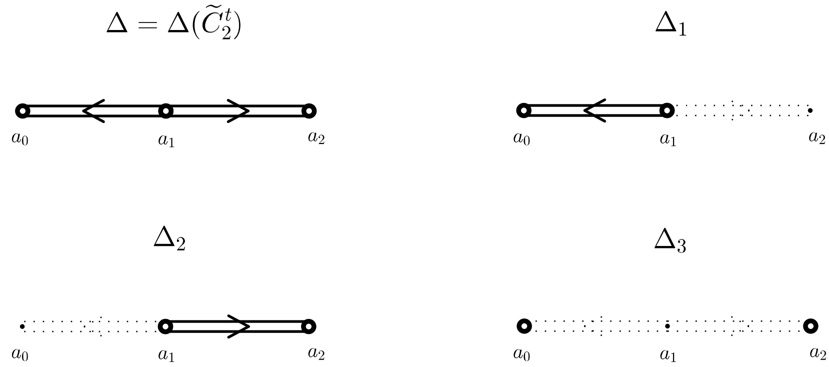
as described in Corollary 3.23.

Take a presentation $\sigma_{X_1(q)} = \sigma_{12}$ if q is odd and $\sigma_{X_1(q)} = \rho_{11}$ if q is even (notice that $B_m(2^a) \cong C_m(2^a)$). Consider a subgroup $X = L_1$ of G. Its Dynkin diagram is of type A_1 and so by Proposition 3.18, $X \cong \mathrm{SL}\,(2, q)$. From Table 3 we know that X has a presentation $\sigma_X = \langle D_X \mid R_X \rangle = \sigma_1$ with $|D_X| = 3$ and $|R_X| = 9$. Now $X \leq X_i(q)$ for $i = 1, 2$. The group $X_2(q)$ has a presentation $\sigma_{X_2(q)} = \sigma_{10}$. By Lemma 3.16, $\sigma_X \subseteq \sigma_{X_2(q)}$. Since $X \leq X_1(q)$, obviously, $D_X \subset X_1(q)$. Thus elements of D_X can be expressed in terms of elements of D_1. Moreover, the relations R_X hold, as they hold in $X_1(q)$. We use Tietze transformations to eliminate D_X, R_X and R_{12} to obtain:

$$\sigma'_G = \langle D_1 \cup (D_2 \setminus D_X) \mid R_1 \cup (R_2 \setminus R_X) \cup R_3^* \rangle.$$

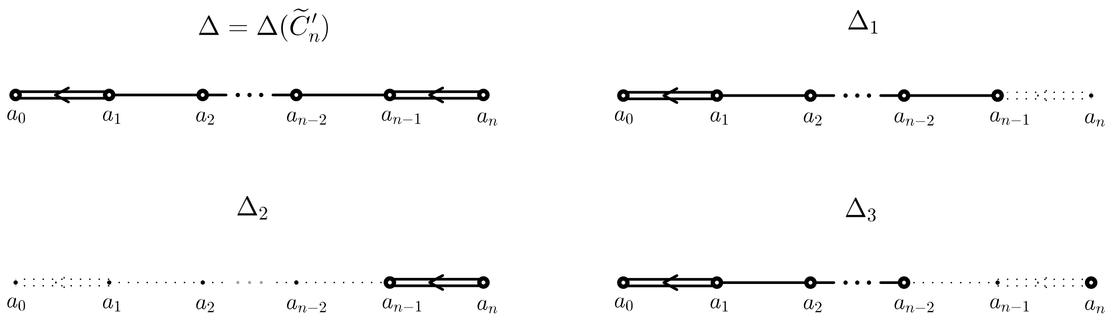
Finally, consider $X_3(q) \cong \mathrm{Sp}\,(2n-2, q) \times \mathrm{SL}\,(2, q)$. Each factor has two generators (Proposition 3.9). Thus as before we obtain $|R_3^*| = 4$.

Therefore G has a presentation with $9 + (6 - 3) = 12$ generators and $48 + (28 - 9) + 4 = 71$ relations if q is odd. For even q the corresponding calculation gives $9 + (6 - 3) = 12$ generators and $40 + (20 - 5) + 4 = 59$ relations.

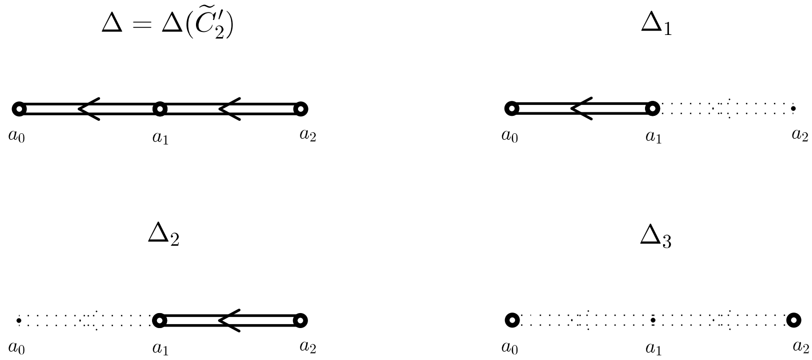


If $n = 2$, we use $\sigma_{X_1(q)} = \sigma_9$ if q is odd and $\sigma_{X_1(q)} = \rho_{10}$ if q is even, thus obtaining a presentation with $5 + (6 - 3) = 8$ generators and $27 + (28 - 9) + 4 = 50$ relations if q is odd, and $6 + (6 - 3) = 9$ generators and $20 + (20 - 5) + 4 = 39$ relations if q is even.

3.4.3 $\widetilde{C}'_n(q)$



For $n \geq 3$, the proof is a line by line repetition of the case $G = \widetilde{C}_n(q)$ with one change: in the case when q is odd, we take $\sigma_{X_2(q)} = \sigma_{10}$, thus obtaining a presentation of G with $8+(6-3) = 11$ generators and $47+(28-9)+4 = 70$ relations. In the q even case nothing changes, we have a presentation with 12 generators and 59 relations.

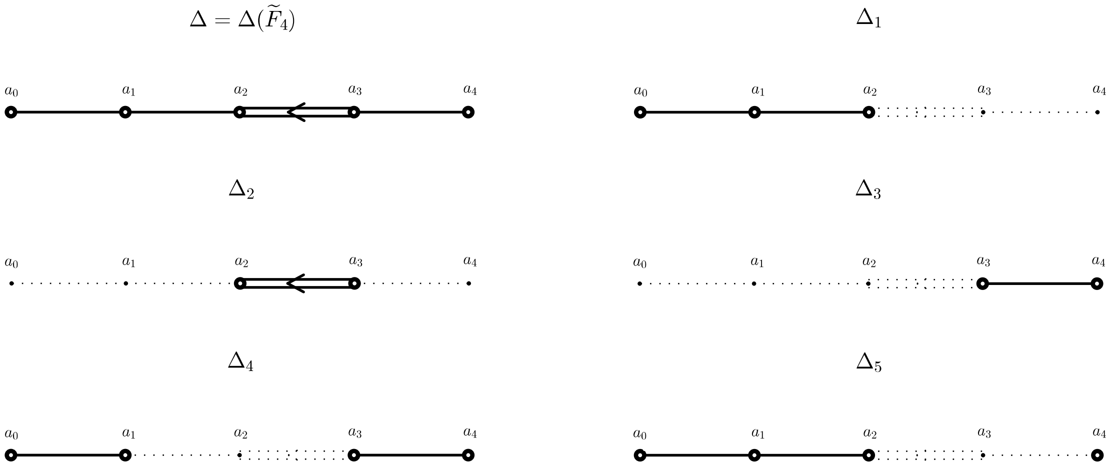


For $n = 2$ we repeat the proof of the $G = \widetilde{C}_2(q)$ case, but now $\sigma_X \subseteq \sigma_{X_1(q)}$, so our presentation becomes:

$$\sigma_G' = \langle (D_1 \setminus D_X) \cup D_2 \mid (R_1 \setminus R_X) \cup R_2 \cup R_3^* \rangle.$$

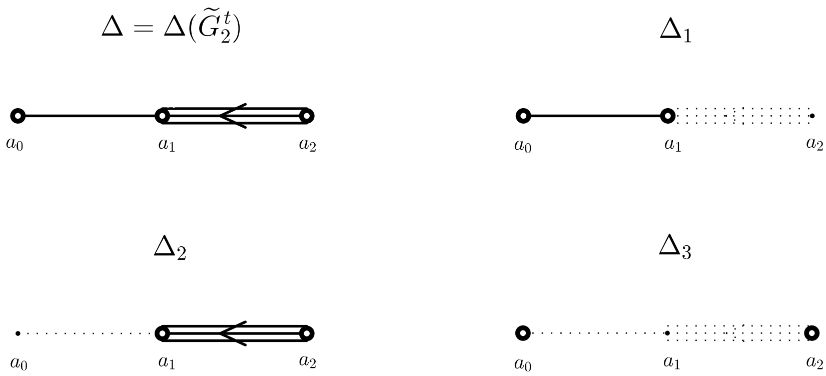
This does not change the calculation, G still has a presentation with 7 generators and 49 relations if q is odd and 9 generators and 39 relations if q is even.

3.4.4 $\widetilde{F}_4^t(q)$



The proof is line by line repetition of the case $G = \widetilde{F}_4(q)$. The outcome is the same: a presentation with 8 generators and 50 relations if q is odd and 9 generators and 43 relations if q is even.

3.4.5 $\widetilde{G}_2^t(q)$



The argument follows the proof in the case $G = \widetilde{G}_2(q)$. The outcome is the same: a presentation of G with 7 generators and 40 relations if q is odd and 7 generators and 32 relations if q is even.

3.5 Chevalley groups

As we mentioned earlier, affine Kac-Moody groups defined over $\mathbb{F}_q$ are related to Chevalley groups defined over $\mathbb{F}_q[t,t^{-1}]$: $\mathbf{G}(\mathbb{F}_q[t,t^{-1}]) \cong \widetilde{\mathbf{G}}(\mathbb{F}_q)/Z$ where $Z \cong \mathbb{F}_q^\times$ is a central subgroup of $\widetilde{\mathbf{G}}(\mathbb{F}_q)$ [MoReh91, Section 2]. For example, $\mathrm{SL}_n(\mathbb{F}_q[t,t^{-1}])$ is the quotient of the simply connected affine Kac-Moody group $\widetilde{A}_{n-1}(q)$ by its central subgroup $Z \cong \mathbb{F}_q^\times$. Therefore we can obtain a presentation of $\mathbf{G}(\mathbb{F}_q[t,t^{-1}])$ from a presentation of $\widetilde{\mathbf{G}}(\mathbb{F}_q)$ (as in Table A.2) by adding one extra relation to kill a generator of Z.

The groups $\mathbf{G}(\mathbb{F}_q[t,t^{-1}])$ can be generated by two elements (cf. Theorem 3.12). Therefore we can change our presentation to a presentation of $\mathbf{G}(\mathbb{F}_q[t,t^{-1}])$ in these two generators. This change of generators costs two extra relations (cf. Lemma 2.1). The next theorem summarises this.

Theorem 3.24. *Let* $\mathbf{G}$ *be a simple simply connected Chevalley group scheme of rank* $n \geq 2$. *Take* $q = p^a$, $a \geq 1$ *with* p *a prime and set* $G = \mathbf{G}(\mathbb{F}_q[t,t^{-1}])$. *Then* G *has a presentation with* 2 *generators and at most* 72 *relations with the possible exceptions of* $A_2(\mathbb{F}_2[t,t^{-1}])$, $B_n(\mathbb{F}_2[t,t^{-1}])$, $C_n(\mathbb{F}_2[t,t^{-1}])$, $G_2(\mathbb{F}_2[t,t^{-1}])$, $F_4(\mathbb{F}_2[t,t^{-1}])$, $A_2(\mathbb{F}_3[t,t^{-1}])$ *and* $G_2(\mathbb{F}_3[t,t^{-1}])$. *If* $G = A_2(\mathbb{F}_2[t,t^{-1}])$ *or* $A_2(\mathbb{F}_3[t,t^{-1}])$, G *has a presentation with at most* 3 *generators and* 30 *relations.*

The precise number of generators and relations in a presentation of $\mathbf{G}(\mathbb{F}_q[t,t^{-1}])$ can be deduced from Table A.2 by adding 1 relation, and for a presentation with 2 generators can be found in Table A.3.

Capdeboscq, Lubotzky and Remy connected the presentations of Chevalley groups over $\mathbb{F}_q[t, t^{-1}]$ with the profinite presentations of Chevalley groups defined over $\mathbb{F}_q[[t]]$ [CLRe16, Proposition 1.2]. An immediate consequence of their Proposition 1.2 combined with our Theorem 3.24 is the following statement.

Theorem 3.25. *Let $\mathbf{G}$ be a simple simply connected Chevalley group scheme of rank at least 2. For $q = p^a$, $a \geq 1$, p a prime, consider a profinite group $G = \mathbf{G}(\mathbb{F}_q[[t]])$. Then G has a profinite presentation with 2 generators and at most 72 relations with the possible exceptions of $A_2(\mathbb{F}_2[[t]])$, $B_n(\mathbb{F}_2[[t]])$, $C_n(\mathbb{F}_2[[t]])$, $G_2(\mathbb{F}_2[[t]])$, $F_4(\mathbb{F}_2[[t]])$, $A_2(\mathbb{F}_3[[t]])$ and $G_2(\mathbb{F}_3[[t]])$. If $G = A_2(\mathbb{F}_2[[t]])$ or $A_2(\mathbb{F}_3[[t]])$, then G has a profinite presentation with at most 3 generators and 31 relations.*

3.6 Adjoint and Classical Groups

So far we have worked with presentations of a simply connected Kac-Moody group $X(q)$ defined over a finite field $\mathbb{K} = \mathbb{F}_q$. Our method can be used to derive a presentation of a Kac-Moody group that is not necessarily simply connected. In this section we deal with adjoint and classical groups. This approach can be used to derive a presentation of an arbitrary Kac-Moody group over $\mathbb{F}_q$.

There are two different meanings of the term *adjoint group* in the literature. For a group $X(q)$, one meaning is that its adjoint group is its image under the natural homomorphism $X(q) \to \mathrm{Aut}\,(X(q))$ given by the adjoint action (that is the action on itself by conjugation). This is otherwise known as the inner automorphism group of $X(q)$, $\mathrm{Inn}\,(X(q))$, so we have $X(q)_{ad} := X(q)/Z(X(q)) \cong \mathrm{Inn}\,(X(q))$.

Besides the adjoint group $X(q)_{ad}$, there is also the group of points for an adjoint root datum. A convenient language to discuss this is the language of **group $\mathbb{K}$-functors**, the functors from the category of commutative $\mathbb{K}$-algebras to groups. A Kac-Moody group $\mathbf{G}_{\mathcal{D}}(\mathbb{K})$ with a root datum $\mathcal{D} = (I, A, \mathcal{X}, \mathcal{Y}, \Pi, \Pi^{\vee})$ is the result of applying a group functor $\mathbf{G}_{\mathcal{D}}$ to the field $\mathbb{K}$. Recall that the Kac-Moody datum $\mathcal{D}$ is said to be adjoint if Π is a basis of $\mathcal{X}$, in which case we also say the group $\mathbf{G}_{\mathcal{D}}(\mathbb{K})$ is **adjoint**. We denote the adjoint Kac-Moody group $\mathbf{G}_{\mathcal{D}}(\mathbb{K})$ by $X_{ad}(q)$. Note that the notation is chosen to be suggestive, $X_{ad}(q)$ is the result of applying a functor X_{ad} to $\mathbb{F}_q$, and $X(q)_{ad}$ is the image of $X(q)$ under the adjoint map induced from conjugation.

A homomorphism of the root data induces a homomorphism of the group $\mathbb{K}$-functors $\pi : X \to X_{ad}$. Taking points over $\mathbb{K}$ yields a group homomorphism $\pi(q) : X(q) \to X_{ad}(q)$. The kernel of $\pi(q)$ is the centre $Z(X(q))$ of $X(q)$. Hence, we have an exact sequence of groups

$$1 \to Z(X(q)) \to X(q) \xrightarrow{\pi(q)} X_{ad}(q)$$

and $X(q)_{ad}$ is observed in this sequence as the image of $\pi(q)$. For instance, if $X = A_{n-1}$, it is

$$1 \to \mu_n(\mathbb{F}_q) \to A_{n-1}(q) = \mathrm{SL}_n(q) \xrightarrow{\pi(q)} (A_{n-1})_{ad}(q) = \mathrm{PGL}_n(q)$$

where μ_n is the group scheme of the n-th roots of unity and $A_{n-1}(q)_{ad} = \mathrm{PSL}_n(q)$ is the image of $\pi(q)$ in $\mathrm{PGL}_n(q)$.

Another insightful example is $X = \widetilde{A}_{n-1}$. The key exact sequence is

$$1 \to \mu_n(\mathbb{F}_q) \times \mathbb{F}_q^\times \to \widetilde{A}_{n-1}(q) = \widetilde{\mathrm{SL}}_n(\mathbb{F}_q[t, t^{-1}]) \xrightarrow{\pi(q)} (\widetilde{A}_{n-1})_{ad}(q) = \mathbb{F}_q^\times \ltimes \mathrm{PGL}_n(\mathbb{F}_q[t, t^{-1}])$$

where the simply connected group $\widetilde{A}_{n-1}(q)$ is the Steinberg central extension of $\mathrm{SL}_n(\mathbb{F}_q[t, t^{-1}])$ by $\mathbb{F}_q^\times$ and the adjoint group $(\widetilde{A}_{n-1})_{ad}(q)$ is the semidirect product where the action of $\mathbb{F}_q^\times$ is given by $\alpha \cdot \sum_k P_k t^k = \sum_k \alpha^k P_k t^k$.

Let $\mathcal{P}$ be the weight lattice, $\mathcal{Q}$ the root lattice of the corresponding Kac-Moody Lie algebra. The weight lattice $\mathcal{P}$ is the root lattice $\mathcal{X}$ for a simply connected root datum, and similarly for $\mathcal{Q}$ and an adjoint root datum. The natural map $p : \mathcal{Q} \to \mathcal{P}$ is given by the Cartan matrix (or its transpose, depending on conventions). It is a part of an exact sequence

$$\mathcal{Q} \xrightarrow{p} \mathcal{P} \to \mathcal{Z} \to 1$$

where $\mathcal{Z} = \operatorname{coker} p$. The Cartan matrix pinpoints all the tori (of the corresponding Kac-Moody groups) of interest for us:

$$Z(q) = Z(X(q)) = \hom(\mathcal{Z}, \mathbb{F}_q^\times),\ T(q) = \hom(\mathcal{P}, \mathbb{F}_q^\times),\ T_{ad}(q) = \hom(\mathcal{Q}, \mathbb{F}_q^\times),\ \pi(q)(\mathbf{x}) = \mathbf{x} \circ p.$$

Let us examine the corresponding (not exact) sequence of tori

$$1 \to Z(X(q)) \to T(q) \xrightarrow{\pi(q)} \overline{T}(q) \hookrightarrow T_{ad}(q)$$

where $\overline{T}(q) = T(q)/Z(X(q))$ can be thought of as a torus of $X(q)_{ad}$.

Proposition 3.26. *Let $X(q)$ be a simply connected irreducible Kac-Moody group over a finite field $\mathbb{K} = \mathbb{F}_q$ (finite, affine or indefinite). Let $H(q) := \mathrm{Ext}^1(\mathcal{Z}, \mathbb{F}_q^\times)$ (in the category of abelian groups) in the finite or indefinite case and $H(q) := \mathrm{Ext}^1(\mathcal{Z}, \mathbb{F}_q^\times) \times \mathbb{F}_q^\times$ in the affine case. Then there exists a short exact sequence*

$$1 \to X(q)_{ad} \to X_{ad}(q) \to H(q) \to 1. \tag{3.1}$$

Proof. Let us assume that X is of finite or indefinite type. Then $p : \mathcal{Q} \to \mathcal{P}$ is injective and $\mathcal{Z}$ is finite. The long exact sequence in cohomology

$$1 \to \hom(\mathcal{Z}, \mathbb{F}_q^\times) \to \hom(\mathcal{P}, \mathbb{F}_q^\times) \xrightarrow{\pi(q)} \hom(\mathcal{Q}, \mathbb{F}_q^\times) \to \mathrm{Ext}^1(\mathcal{Z}, \mathbb{F}_q^\times) \to 1$$

reduces to a short exact sequence connecting the adjoint tori

$$1 \to \overline{T}(q) \to T_{ad}(q) \to H(q) \to 1. \tag{3.2}$$

This implies the existence of the short exact sequence (3.1).

If X is affine, the map $p : \mathcal{Q} \to \mathcal{P}$ is no longer injective. We can decompose $\mathcal{Q} = \mathcal{Q}' \times \mathbb{Z}$ where $\mathbb{Z} = \ker p$ and $p : \mathcal{Q}' \to \mathcal{P}$ is injective. The long exact sequence in cohomology is

$$1 \to \hom(\mathcal{Z}, \mathbb{F}_q^\times) \to \hom(\mathcal{P}, \mathbb{F}_q^\times) \xrightarrow{\pi(q)} \hom(\mathcal{Q}', \mathbb{F}_q^\times) \to \mathrm{Ext}^1(\mathcal{Z}, \mathbb{F}_q^\times) \to 1.$$

It gives a description of the tori using an auxiliary group $T'(q) = \hom(\mathcal{Q}', \mathbb{F}_q^\times)$. The sequence

$$1 \to \overline{T}(q) \to T'(q) \to \mathrm{Ext}^1(\mathcal{Z}, \mathbb{F}_q^\times) \to 1$$

is exact. Since $T_{ad}(q) = T'(q) \times \mathbb{F}_q^\times$, a direct product with $\mathbb{F}_q^\times$ establishes the exact sequence (3.2) in the affine case. This proves the existence of an exact sequence (3.1) in all cases. $\square$

Proposition 3.26 gives presentations of both $X(q)_{ad}$ and $X_{ad}(q)$. Since $X(q)_{ad} = X(q)/Z(q)$, one gets $X(q)_{ad}$ from $X(q)$ by "killing" generators of $Z(q)$. The presentation of $X_{ad}(q)$ is obtained from presentations of $X(q)_{ad}$ and $H(q)$ by P. Hall's Lemma [CLRe16, Lemma 2.2]. Observe that the right conjugations in P. Hall's Lemma are superfluous. One usually adds them for convenience.

Corollary 3.27. *Suppose we have a presentation of $X(q)$, $Z(q)$ and $H(q)$:*

$$\sigma_{X(q)} = \langle D \mid R \rangle, \quad \sigma_{Z(q)} = \langle D_1 \mid R_1 \rangle, \quad \sigma_{H(q)} = \langle D_2 \mid R_2 \rangle.$$

Then we have presentations of adjoint groups

$$\sigma_{X(q)_{ad}} = \langle D \mid R \cup D_1^\sharp \rangle \text{ and } \sigma_{X_{ad}(q)} = \langle D \cup D_2 \mid R \cup D_1^\sharp \cup R_2^\sharp \cup D_2^{act} \rangle$$

where $D_1^\sharp = \{x^\sharp = 1 \mid x \in D_1, x^\sharp$ is an expression of x in $D\}$,
$R_2^\sharp = \{w = w^\sharp \mid w \in R_2, w^\sharp \in X(q)_{ad}$ is an expression of $w(D_2)$ in $D\}$ and

$$D_2^{act} = \{xax^{-1} = {}^x a(D) \mid x \in D_2,\ a \text{ is a generator of } X(q)_{ad},$$
$${}^x a(D) \text{ is an expression of } xax^{-1} \text{ in } D\}.$$

The group $\mathcal{P}/\mathcal{Q}$ is computed by calculating the integral Smith normal forms of Cartan matrices. We summarise these calculations in Table A.4.

As an application of our techniques we write down the numbers of generators and relations of the remaining classical groups over $\mathbb{F}_q[t,t^{-1}]$ in Table A.5 (for sufficiently large q). The groups SL_n, Spin_n and Sp_{2n} are simply connected, so they are already in Tables A.2 and A.3. The group

$$\mathrm{PSL}_n(\mathbb{F}_q[t,t^{-1}]) = \widetilde{A}_{n-1}(q)_{ad}$$

is adjoint, hence its presentation follows from Tables A.2 and A.4. The groups

$$\mathrm{PGL}_n(\mathbb{F}_q[t,t^{-1}]) \lhd (\widetilde{A}_{n-1})_{ad}(q), \quad \mathrm{SO}_{2n+1}(\mathbb{F}_q[t,t^{-1}]) \lhd (\widetilde{B}_n)_{ad}(q)$$

are normal subgroups in the adjoint groups (before the semidirect product). Similarly to Proposition 3.26 they appear in an exact sequence

$$1 \to X(q)_{ad} \to \mathbf{G}(\mathbb{F}_q[t,t^{-1}]) \to \mathrm{Ext}^1(\mathcal{Z},\mathbb{F}_q^\times) \to 1,$$

hence they get a presentation as in Corollary 3.27 but with $\mathrm{Ext}^1(\mathcal{Z},\mathbb{F}_q^\times)$ instead of $H(q)$.

Finally, SO_{2n} is not related to the adjoint group. It is an intermediate quotient fitting into the exact sequence of group schemes

$$1 \to \mathbb{Z}/2 \to \mathrm{Spin}_{2n} \to \mathrm{SO}_{2n} \to 1.$$

Using our arguments, we fit the group into an exact sequence

$$1 \to \widetilde{D}_n(q)/Z \to \mathrm{SO}_{2n}(\mathbb{F}_q[t,t^{-1}]) \to \mathrm{Ext}^1(\mathbb{Z}/2,\mathbb{F}_q^\times) \to 1$$

where the central subgroup Z is isomorphic to $\hom(\mathbb{Z}/2,\mathbb{F}_q^\times)$. We get a presentation as in Corollary 3.27 where the result depends on whether q is even or odd.

Chapter 4

Subgroup growth of Chevalley groups over $\mathbb{F}_p([[t]])$

4.1 Preliminaries

References for this section are [LSh94], [BG01] and [LSe03].

Definition 4.1. Let H be a subgroup of a finitely generated group G. We define $d(H)$ to be the minimal number of generators of H.

In the case of pro-p groups, a key tool in studying their subgroup growth is associating a graded Lie algebra $\mathcal{L}$ to the group, and then deriving information about $d(H)$ for subgroups H of a given order from information about the codimensions of corresponding Lie subalgebras of $\mathcal{L}$.

4.1.1 The graded Lie algebra

We now show how to associate a graded Lie algebra to the first congruence subgroup of a Chevalley group over $\mathbb{F}_p([[t]])$.
Let $\mathbf{G}(\mathbb{F}_p[[t]])$ be a simple simply connected Chevalley group and let G_n denote its n-congruence subgroup. Let $\mathfrak{g}$ be the corresponding Lie algebra defined over $\mathbb{F}_p$.
The first step is a result about the structure of the successive quotients G_n/G_{n+1} (see for example [BG01]), the first part of which is an easy consequence of Proposition 2.13.

Proposition 4.2. *For all $n \in \mathbb{N}$, G_n/G_{n+1} is an elementary abelian p-group of order $p^{\dim \mathfrak{g}}$. It is the adjoint module for $\mathfrak{g}$.*

So each successive quotient G_n/G_{n+1} can be viewed as a vector space of dimension $\dim \mathfrak{g}$ over $\mathbb{F}_p$ and $\mathfrak{g}$ acts on it via the adjoint action.

Next we define

$$L(G_1) := \bigoplus_{n=1}^{\infty} \frac{G_n}{G_{n+1}}.$$

Since this is a direct sum, any element of $L(G_1)$ has only finitely many non-identity coordinates. Each compotent in the sum is a vector space of the same dimension over $\mathbb{F}_p$, so $L(G_1)$ becomes a vector space over $\mathbb{F}_p$ itself if we endow it with component-wise scalar multiplication by elements of $\mathbb{F}_p$. We define a product on homogeneous components of the form xG_{n+1} and yG_{m+1} where $x \in G_n$ and $y \in G_m$:

$$[xG_{n+1}, yG_{m+1}] := [x, y]G_{n+m+1}.$$

Next we have the following standard result about this product (see [BG01] or [LSe03]).

Proposition 4.3. *Extending this product by linearity gives $L(G_1)$ the structure of a Lie algebra over $\mathbb{F}_p$.*

Definition 4.4. We call $L(G_1)$ the **graded Lie algebra** associated with G_1.

We now come to a result about the structure of this graded Lie algebra.

Proposition 4.5 (cf. [BG01])**.** *We have*

$$L(G_1) \cong t\,\mathfrak{g}[t] \cong \mathfrak{g} \otimes_{\mathbb{F}_p} t\mathbb{F}_p[t],$$

Here $t\,\mathfrak{g}[t]$ is the set of polynomials with 0 constant coefficient over $\mathfrak{g}$. We will usually use the third form of expressing this graded Lie algebra, so by abuse of notation we can write

$$L(G_1) = \mathfrak{g} \otimes_{\mathbb{F}_p} t\mathbb{F}_p[t] = (\mathfrak{g} \otimes_{\mathbb{F}_p} t) \oplus (\mathfrak{g} \otimes_{\mathbb{F}_p} t^2) \oplus (\mathfrak{g} \otimes_{\mathbb{F}_p} t^3) \oplus \dots,$$

hence each element a in $L(G_1)$ can be written as $a = \Sigma_{i=1}^{\infty} a_i \otimes_{\mathbb{F}_p} t^i$ with $a_i \in \mathfrak{g}$, where it is understood that only finitely many non-zero summands are allowed.

Now let H be a closed subgroup of G_1. We define a graded subalgebra of $L(G_1)$ corresponding to H:

$$L(H) := \bigoplus_{n=1}^{\infty} \frac{(H \cap G_n)G_{n+1}}{G_{n+1}}.$$

We now quote some results about this construction (see [BG01]).

Lemma 4.6. *$L(H)$ is a graded subalgebra of $L(G_1)$.*

Lemma 4.7. *If $K \leq H$ are closed subgroups, then $L(K) \subseteq L(H)$ and $\dim(L(H)/L(K)) = \log_p[H : K]$.*

Lemma 4.8. *If H is normal in G_1, then $L(H)$ is an ideal of $L(G_1)$.*

Lemma 4.9. *$G_k \leq H$ if and only if $t^k\,\mathfrak{g}[t] \subseteq L(H)$.*

Lemma 4.10. *If $L(H)$ is generated by d homogeneous elements, then $d(H) \leq d$, where $d(H)$ is the minimal number of elements required to generate H topologically.*

A result of a similar genre is the following.

Lemma 4.11 ([LSe03], Prop 4.3.1 "Level vs. index")**.** *Let H be an open subgroup of index p^k in G_1. Then $H \geq G_{k+1}$.*

4.1.2 Subgroup growth estimates

We now quote some results that give us estimates on subgroup growth. First we need to define some notation. For two groups H, G we write $H \subseteq_o G$ when H is an open subgroup of G.

Definition 4.12. For a finitely generated pro-p group G, we define $g_n(G)$ to be the maximum of the minimum number of generators required to generate an open subgroup H of G of index n, i.e.

$$g_n = g_n(G) := \max\{d(H) \mid H \subseteq_o G,\ [G : H] = n\}.$$

Recall that $a_n(G)$ denotes the number of subgroups of index n in G. The following proposition allows us to relate the sequences $a_n(G)$ and $g_n(G)$ and will be used to prove Theorem C.

Lemma 4.13 ([LSh94], Lemma 4.1)**.** *We have*

$$a_{p^k}(G) \leq \prod_{i=0}^{k-1} \frac{p^{g_{p^i}} - 1}{p - 1} \leq p^{g_1 + g_p + \cdots + g_{p^{k-1}}}.$$

The following proposition is useful estimating codimensions in the graded Lie algebra $\mathcal{L}$.

Lemma 4.14 ([LSh94] Proposition 4.2)**.** *Let L_0 be a finite-dimensional perfect Lie algebra over $\mathbb{F}_p$, and let $L = L_0 \otimes gr(M)$. Then there exists a constant c such that, for every proper open Lie $\mathbb{F}_p$-subalgebra K of L we have*

$$\dim(K/K') \leq c \cdot \dim(L/K).$$

In this proposition M is the maximal ideal of the local ring Λ and $K' = [K, K]$. So in our situation $\Lambda = \mathbb{F}_p[[t]]$, $M = t\mathbb{F}_p[[t]]$ and $L_0 = \mathfrak{g}$. So we can let $L = \mathcal{L} = L_0 \otimes t\mathbb{F}_p[t]$, in which case this proposition concerns any proper Lie $\mathbb{F}_p$-subalgebra $\mathcal{K}$ of $\mathcal{L}$ of finite codimension.

4.1.3 Ridgeline numbers and small primes

Now we move on to the preliminaries necessary for the proof of Theorem D.

Let $\mathbf{G}$ be a simple simply connected Chevalley group scheme. We take $\mathfrak{g}_{\mathbb{Z}}$ to be the Lie algebra of $\mathbf{G}$ over the integers. Let $\mathbb{K}$ be a field of characteristic p, where p is either zero or a prime. We define a new Lie algebra by extension of scalars, $\mathfrak{g} \coloneqq \mathfrak{g}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{K}$.

Recall that a bilinear form $\eta = \langle\, , \rangle$ on $\mathfrak{g}$ is said to be **invariant** or **associative** if we have

$$\langle [x, y], z\rangle = \langle x, [y, z]\rangle$$

for all $x, y, z \in \mathfrak{g}$.

We fix an invariant bilinear form $\eta = \langle\, , \rangle$ on $\mathfrak{g}$ of maximal possible rank. Note that we do not require η to be symmetric, although η will in fact be symmetric in the cases we are interested in. The bilinear form η defines two maps from $\mathfrak{g}$ to $\mathfrak{g}*$, one mapping $x \in \mathfrak{g}$ to $y \mapsto \langle \cdot, y\rangle$, and the other to $y \mapsto \langle y, \cdot\rangle$. Since η is not assumed to be symmetric or reflexive these maps need not have the same kernel, but the dimensions of these two kernels will be equal. We let $\mathfrak{g}^0$ be a kernel for some choice of these two maps. Notice that the nullity

$$r \coloneqq \dim \mathfrak{g}^0$$

of η is independent of the choice of η.

Recall that the **centraliser** of an element $\mathbf{x}$ in $\mathfrak{g}$ is defined as

$$\mathfrak{c}(\mathbf{x}) = \{\mathbf{y} \in \mathfrak{g} \mid [\mathbf{x}, \mathbf{y}] = 0\}.$$

Clearly the elements in $\mathfrak{g}$ with centraliser of maximal dimension are those that lie in the centre of $\mathfrak{g}$. For such an element $\mathbf{x}$ we have $\dim \mathfrak{c}(\mathbf{x}) = \dim \mathfrak{g}$. In what follows we will be interested in the non-central elements of $\mathfrak{g}$ whose centralisers are of maximal dimension.

We now introduce a new parameter of the Lie algebra $\mathfrak{g}$.

Definition 4.15. Let l be the rank of $\mathfrak{g}$, m its dimension and s the maximal dimension of the centraliser $\mathfrak{c}(\mathbf{x})$ of a non-central element $\mathbf{x} \in \mathfrak{g}$. We define the **ridgeline number** of $\mathfrak{g}$ as

$$v(\mathbf{G}) = v(\mathfrak{g}) \coloneqq \frac{l}{m - s - r}.$$

We will prove that $m - s = 2(h^\vee - 1)$ where $h^\vee$ is the dual Coxeter number of $\mathfrak{g}$ (see Proposition 4.24). Therefore,

$$v(\mathfrak{g}) = \frac{l}{2(h^\vee - 1) - r}.$$

We present the values of $v(\mathfrak{g})$ in Appendix A.6. We include only Lie algebras in tolerable characteristics (see Definition 4.16) where our method produces new results.

Now we let the characteristic p be a prime, and consider when the Lie algebra $\mathfrak{g}$ behaves as in characteristic zero.

Definition 4.16. The positive characteristic p of the field $\mathbb{K}$ is called **good** for $\mathfrak{g}$ if p does not divide the coefficients of the highest root of $\mathfrak{g}$. The positive characteristic p of the field $\mathbb{K}$ is called **very good** if p is good and $\mathfrak{g}$ is simple. We call the positive characteristic p **tolerable** if any proper ideal of $\mathfrak{g}$ is contained in its centre.

Let us first consider what the good characteristics are for each Chevalley Lie algebra. For a Chevalley Lie algebra of rank l, let $\alpha_1, \alpha_2, \ldots \alpha_l$ be a system of fundamental roots. We number the roots according to [Car05], and the same order appears in the Dynkin diagrams in Appendix C. We list the highest roots of each type of Lie algebra and which characteristics this correspondingly excludes from being good in Table 4.1.

Now the very good characteristics for each Chevalley Lie algebra are $p \nmid l+1$ in type A_l, $p \neq 2$ in types B_l, C_l, D_l, $p \neq 2, 3$ in types E_6, E_7, F_4, G_2, and $p \neq 2, 3, 5$ in type E_8. If p is very good, the Lie algebra $\mathfrak{g}$ behaves as in characteristic zero. In particular, $\mathfrak{g}$ is simple, its Killing form is non-degenerate, etc. Let us consider what can go wrong for the Lie algebra $\mathfrak{g}$ in small characteristics.

Suppose that p is tolerable but not very good. If p does not divide the determinant of the Cartan matrix of $\mathfrak{g}$, the Lie algebra $\mathfrak{g}$ is simple. This covers the following primes: $p = 2$ in types E_6 and G_2, $p = 3$ in types E_7 and F_4, $p = 2, 3, 5$ in type E_8. In this scenario, the $\mathfrak{g}$-modules $\mathfrak{g}$ and $\mathfrak{g}^*$ are isomorphic, which immediately gives us a non-degenerate invariant bilinear form on $\mathfrak{g}$ [H95, 0.13].

If p divides the determinant of the Cartan matrix of $\mathfrak{g}$, there is more than one Chevalley Lie algebra. We study the simply connected Lie algebra $\mathfrak{g}$, i.e., $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$ and $\mathfrak{g}/\mathfrak{z}$ is simple (where $\mathfrak{z}$ is the centre). There is a canonical map to the adjoint Lie algebra $\mathfrak{g}^\flat$:

$$\varphi : \mathfrak{g} = \mathfrak{h} \oplus \bigoplus_\alpha \mathfrak{g}_\alpha \to \mathfrak{g}^\flat = \mathfrak{h}^\flat \oplus \bigoplus_\alpha \mathfrak{g}_\alpha.$$

The map φ is the identity on the root spaces $\mathfrak{g}_\alpha$. Let us describe it on the Cartan subalgebras. The basis of the Cartan subalgebra $\mathfrak{h}$ are the simple coroots $\mathbf{h}_i = \alpha_i^\vee = [\mathbf{e}_{\alpha_i}, \mathbf{e}_{-\alpha_i}]$. The basis of the Cartan subalgebra $\mathfrak{h}^\flat$ are the fundamental coweights $\mathbf{y}_i = \varpi_i^\vee$ defined by $\alpha_i(\mathbf{y}_j) = \delta_{i,j}$. Now the map φ on the Cartan subalgebras is

Table 4.1: Good characteristics for a Chevalley Lie algebra $\mathfrak{g}$

type of $\mathfrak{g}$	highest root	good	$\det(A)$	very good
A_l	$\alpha_1 + \alpha_2 + \ldots + \alpha_l$	all	$l+1$	$p \nmid (l+1)$
B_l	$\alpha_1 + 2\alpha_2 + \ldots + 2\alpha_l$	$p \neq 2$	2	$p \neq 2$
C_l	$2\alpha_1 + 2\alpha_2 + \ldots + 2\alpha_{l-1} + \alpha_l$	$p \neq 2$	2	$p \neq 2$
D_l	$\alpha_1 + 2\alpha_2 + \ldots + 2\alpha_{l-2} + \alpha_{l-1} + \alpha_l$	$p \neq 2$	4	$p \neq 2$
E_6	$\alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + 2\alpha_5 + \alpha_6$	$p \neq 2, 3$	3	$p \neq 2, 3$
E_7	$\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 2\alpha_5 + 3\alpha_6 + 2\alpha_7$	$p \neq 2, 3$	2	$p \neq 2, 3$
E_8	$2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 5\alpha_5 + 6\alpha_5 + 3\alpha_6 + 4\alpha_7 + 2\alpha_8$	$p \neq 2, 3, 5$	1	$p \neq 2, 3, 5$
F_4	$2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4$	$p \neq 2, 3$	1	$p \neq 2, 3$
G_2	$2\alpha_1 + 3\alpha_2$	$p \neq 2, 3$	1	$p \neq 2, 3$

given by

$$\varphi(\mathbf{h}_i) = \sum_j c_{j,i}\mathbf{y}_j$$

where $c_{j,i}$ are entries of the Cartan matrix of the coroot system of $\mathfrak{g}$. The image of φ is $[\mathfrak{g}^\flat, \mathfrak{g}^\flat]$. The kernel of φ is the centre $\mathfrak{z}$. From our description $\mathfrak{z}$ is the subspace of $\mathfrak{h}$ equal to the null space of the Cartan matrix. It is equal to $\mathfrak{g}^0$, the kernel of η. The dimension of $\mathfrak{z}$ is at most 2 (see the values of r in Table A.6).

The key dichotomy now is whether the Lie algebra $\mathfrak{g}/\mathfrak{z}$ is simple or not. If $\mathfrak{g}$ is simply-laced, the algebra $\mathfrak{g}/\mathfrak{z}$ is simple. This occurs when $p \mid l+1$ in type A_l, $p = 2$ in types D_l and E_7, $p = 3$ in type E_6. Notice that A_1 in characteristic 2 needs to be excluded: $\mathfrak{g}/\mathfrak{z}$ is abelian rather than simple. In this scenario the $\mathfrak{g}$-modules $\mathfrak{g}/\mathfrak{z}$ and $(\mathfrak{g}/\mathfrak{z})^*$ are isomorphic. This gives us an invariant bilinear form with the kernel $\mathfrak{z}$ [H95, 0.13].

Let us look meticulously at $\mathfrak{g}$ of type D_l when $p = 2$. The standard representation gives a homomorphism of Lie algebras

$$\rho : \mathfrak{g} \to \mathfrak{so}_{2l}(\mathbb{K}), \quad \mathbf{x} \mapsto \rho(\mathbf{x}) = \begin{pmatrix} \rho_{11}(\mathbf{x}) & \rho_{12}(\mathbf{x}) \\ \rho_{21}(\mathbf{x}) & \rho_{22}(\mathbf{x}) \end{pmatrix},$$

where $\rho_{22}(\mathbf{x}) = \rho_{11}(\mathbf{x})^t$, while $\rho_{12}(\mathbf{x})$ and $\rho_{21}(\mathbf{x})$ are skew-symmetric $l \times l$-matrices, which for $p = 2$ is equivalent to symmetric with zeroes on the diagonal. The Lie algebra $\mathfrak{so}_{2l}(\mathbb{K})$ has a 1-dimensional centre spanned by the identity matrix. If l is odd, ρ is an isomorphism, and $\mathfrak{g}$ has a 1-dimensional centre. However, if l is even, ρ has a 1-dimensional kernel, and $\mathfrak{g}$ has a 2-dimensional centre.

It is instructive to observe how the standard representation ρ equips $\mathfrak{g}$ with an invariant form. A skew-symmetric matrix Z can be written uniquely as a sum $Z = Z^L + Z^U$, where Z^L is strictly lower triangular and Z^U is strictly upper triangular. Then the bilinear form is given by

$$\eta(\mathbf{x}, \mathbf{y}) := \langle \rho(\mathbf{x}), \rho(\mathbf{y}) \rangle := \mathrm{Tr}\,(\rho_{11}(\mathbf{x})\rho_{11}(\mathbf{y}) + \rho_{12}(\mathbf{x})^L \rho_{21}(\mathbf{y})^U + \rho_{21}(\mathbf{x})^L \rho_{12}(\mathbf{y})^U).$$

This form η is a reduction of the form $\frac{1}{2}\mathrm{Tr}\,(\varphi(\mathbf{x})\varphi(\mathbf{y}))$ on $\mathfrak{so}_{2l}(\mathbb{Z})$, hence it is invariant.

Finally we suppose that p is not tolerable. This happens when $p = 2$ in types B_l, C_l and F_4 or $p = 3$ in type G_2. In all these cases $\mathfrak{g}$ is not simply-laced and the quotient algebra $\mathfrak{g}/\mathfrak{z}$ is not simple. The short root vectors generate a proper non-central ideal I. This ideal sits in the kernel of any non-zero invariant form. Consequently, our method fails to produce any new result.

4.1.4 Dimension estimates

Here we go over some results about dimension estimates, which will be essential for proving Theorem D.

Proposition 4.17. *Let $\mathfrak{g}$ be an m-dimensional Lie algebra with an invariant bilinear form η, whose kernel $\mathfrak{g}^0$ is the centre of $\mathfrak{g}$. Suppose $r = \dim(\mathfrak{g}^0)$ and $k \geq \dim(\mathfrak{c}(\mathbf{x}))$ for any non-central element $\mathbf{x} \in \mathfrak{g}$. Finally, let U, V be subspaces of $\mathfrak{g}$ such that $\dim(U) + \dim(V) > m + k + r$. Then $[U, V] = \mathfrak{g}$.*

Proof. Suppose not, so $[U, V]$ is a subspace of $\mathfrak{g}$ of dimension strictly smaller than m. Let us consider the orthogonal complement $W = [U, V]^\perp$ under the form η. Note that $W \neq \mathfrak{g}^0$. Observe that $U \subseteq [V, W]^\perp$ since η is associative. But W admits a noncentral element $\mathbf{x} \in W$ so that $\dim(\mathfrak{c}(\mathbf{x})) \leq k$. Hence

$$\dim([V, W]) \geq \dim(V) - k \quad \text{and} \quad \dim([V, W]^\perp) \leq m + k + r - \dim(V).$$

Inevitably, $\dim(U) \leq m + k + r - \dim(V)$. □

Another basic but essential lemma is the following.

Lemma 4.18. *The inequality*

$$\dim([U, V]) \geq \dim(V) - \dim(V \cap \mathfrak{c}(\mathbf{x})) \qquad (\clubsuit)$$

holds for any $\mathbf{x} \in U$*.*
In particular, if there exists $\mathbf{x} \in U$ *such that* $\dim(U) + \dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim \mathfrak{g}$*, then the inequality*

$$\dim([U, V]) \geq \dim(U) + \dim(V) - \dim \mathfrak{g}. \tag{$\spadesuit$}$$

holds.

Proof. Let $v \in V$. The restricted map $\operatorname{ad} x : v \mapsto [x, v]$ is linear, so by the first isomorphism theorem, $[x, V]$ and $V \big/ (V \cap \mathfrak{c}(\mathbf{x}))$ are isomorphic as vector spaces. We have $[\mathbf{x}, V] \subseteq [U, V]$, so taking dimensions immediately gives ($\clubsuit$).
For the second statement, if there exists $\mathbf{x} \in U$ such that $\dim(U) + \dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim \mathfrak{g}$, then

$$\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim \mathfrak{g} - \dim(U),$$

so

$$-\dim(V \cap \mathfrak{c}(\mathbf{x})) \geq \dim(U) - \dim \mathfrak{g},$$

and inserting this in ($\clubsuit$) we get

$$\dim([U, V]) \geq \dim(U) + \dim(V) - \dim \mathfrak{g}.$$

□

We now state a theorem of [AbNS03] that was essential for their proof of Theorem 1.4, and can be viewed as the inspitation for our Theorem D.

Proposition 4.19 ([AbNS03], Theorem 3)**.** *For every pair of subspaces U and V of $\mathfrak{g}$, we have*

$$\operatorname{codim}([U, V]) \leq 2\,(\operatorname{codim}(U) + \operatorname{codim}(V)).$$

4.2 Proof of Theorem C

The proof of Theorem C relies on Theorem D that will be proved later. We follow the proof of Abért, Nikolov and Szegedy's Theorem 1.4 and Barnea, Guralnick [BG01, Theorem 1.4].

Suppose that hypotheses of Theorem C hold. We start with the following observation (cf. [AbNS03, Corollary 1 and Lemma 1] and [LSh94, Lemma 4.1]).

Lemma 4.20. *If H is an open subgroup of G_1 and $d(H)$ is the minimal number of generators of H, then*

$$d(H) \leq m + (3 + 4v(\mathfrak{g})) \log_p |G_1 : H|.$$

Moreover, if $l = 2$ and p is very good, then

$$d(H) \leq m + 3\log_p |G_1 : H|.$$

Notice that in the second case $\mathfrak{g} = A_2$, C_2 or G_2 and $m = 8$, 10 or 14 respectively.

Proof. First of all recall that $d(H) = \log_p |H : \Phi(H)| \leq \log_p |H : H'|$ where $\Phi(H)$ is the Frattini subgroup. Because of the correspondence between the open subgroups of G_1 and subalgebras of its graded Lie algebra $\mathcal{L} = L(G_1)$ (see results of Section 4.1.1), $\log_p |H : H'| \leq \dim \mathcal{H}/\mathcal{H}'$ where $\mathcal{H} = L(H)$ is the corresponding subalgebra of $\mathcal{L}$. Hence it suffices to show that

$$\dim \mathcal{H}/\mathcal{H}' \leq m + (3 + 4v(\mathfrak{g})) \dim \mathcal{L}/\mathcal{H}$$

in the general case, and that

$$\dim \mathcal{H}/\mathcal{H}' \leq m + 3 \dim \mathcal{L}/\mathcal{H}$$

in the very good rank 2 case.

Recall that the graded Lie algebra $\mathcal{L}$ is isomorphic to $\mathfrak{g} \otimes_{\mathbb{F}_p} t\mathbb{F}[t]$. Since every element $a \in \mathcal{L}$ can be uniquely written as $a = \Sigma_{i=1}^{\infty} a_i \otimes t^i$ with $a_i \in \mathfrak{g}$, one can define $l(a) := a_s$ where s is the smallest integer such that $a_s \neq 0$, and in this case $s := \deg(a)$. Now set

$$H_i := \langle l(a) \mid a \in \mathcal{H} \text{ with } \deg(a) = i \rangle.$$

Observe that $H_i = \{l(a) \mid a \in \mathcal{H} \text{ with } \deg(a) = i\} \cup \{0\}$. Then $\dim \mathcal{L}/\mathcal{H} = \Sigma_{i=1}^{\infty} \dim \mathfrak{g}/H_i$, and this sum is finite as the left hand side is finite. We define

$$\overline{H}_i := \langle l(a) \mid a \in \mathcal{H}' \text{ with } \deg(a) = i \rangle.$$

Note that $[H_i, H_j] \subseteq \overline{H}_{i+j}$. Then

$$[H_i \otimes t^i, H_j \otimes t^j] \subseteq [H_i, H_j] \otimes t^{i+j} \subseteq \overline{H}_{i+j} \otimes t^{i+j},$$

and so $\dim \mathfrak{g}/[H_i, H_j] \geq \dim \mathfrak{g}/\overline{H}_{i+j}$. Adding up these inequalities for $i = j$ and $i = j + 1$ we get

$$\dim \mathcal{L}/\mathcal{H}' = \Sigma_{i=1}^{\infty} \dim L/\overline{H}_i \leq \dim \mathfrak{g} + \Sigma_{1 \leq i \leq j \leq i+1}^{\infty} \dim \mathfrak{g}/[H_i, H_j].$$

Now we use the estimates of Theorem D:

$$\dim \mathcal{L}/\mathcal{H}' \leq m + \Sigma^{\infty}_{1\leq i\leq j\leq i+1}\alpha(\dim \mathfrak{g}/H_i + \dim \mathfrak{g}/H_j) \leq m + 4\alpha \dim \mathcal{L}/\mathcal{H},$$

where $\alpha = 1 + v(\mathfrak{g})$ or 1 depending on the rank of $\mathfrak{g}$ and p. The result follows immediately. $\square$

Now we apply an estimate from Lemma 4.13: $a_{p^k}(G_1) \leq p^{g_1+\ldots+g_{p^{k-1}}}$ where

$$g_{p^i} = g_{p^i}(G_1) = \max\{d(H) \mid H \leq_{open} G_1, |G_1 : H| = p^i\}.$$

Using Lemma 4.20, in the general case ($l \geq 2$) we have

$$a_{p^k}(G_1) \leq p^{\Sigma^{i=k-1}_{i=0} m+(3+4v(\mathfrak{g}))i} = p^{\frac{(3+4v(\mathfrak{g}))}{2}k^2+(m-\frac{3}{2}-2v(\mathfrak{g}))k}.$$

For $l = 2$ and very good p, Lemma 4.20 gives us

$$a_{p^k}(G_1) \leq p^{\Sigma^{i=k-1}_{i=0} m+3i} = p^{\frac{3}{2}k^2+(m-\frac{3}{2})k}.$$

This finishes the proof of the theorem.

4.3 Proof of Theorem D: the General Case

Let $\mathfrak{a}$ be an m-dimensional Lie algebra over a field $\mathbb{K}$ of characteristic p (prime or zero). We consider it as a topological space in the Zariski topology. We also consider a function $\dim \circ \mathfrak{c} : \mathfrak{a} \to \mathbb{R}$ that for an element $\mathbf{x} \in \mathfrak{a}$ computes the dimension of its centraliser $\mathfrak{c}(\mathbf{x})$.

Lemma 4.21. *The function* $\dim \circ \mathfrak{c}$ *is upper semicontinuous, i.e., for any number* n *the set* $\{\mathbf{x} \in \mathfrak{a} \mid \dim(\mathfrak{c}(\mathbf{x})) \leq n\}$ *is Zariski open.*

Proof. Observe that $\mathfrak{c}(\mathbf{x})$ is the kernel of the adjoint operator $\mathrm{ad}(\mathbf{x})$. Thus, $\dim(\mathfrak{c}(\mathbf{x})) \leq n$ is equivalent to $\mathrm{rank}(\mathrm{ad}(\mathbf{x})) \geq m - n$. This is clearly an open condition, given by the non-vanishing of one of the $(m - n)$-minors. $\square$

Now we move to $\overline{\mathbb{K}}$, the algebraic closure of $\mathbb{K}$. Let $\bar{\mathfrak{a}} = \mathfrak{a} \otimes_{\mathbb{K}} \overline{\mathbb{K}}$. To distinguish centralisers in $\mathfrak{a}$ and $\bar{\mathfrak{a}}$ we denote $\mathfrak{c}(\mathbf{x}) := \mathfrak{c}_{\mathfrak{a}}(\mathbf{x})$ and $\bar{\mathfrak{c}}(\mathbf{x}) := \mathfrak{c}_{\bar{\mathfrak{a}}}(\mathbf{x})$. Now we assume that $\bar{\mathfrak{a}}$ is the Lie algebra of a connected algebraic group $\mathcal{A}$. Let $\mathrm{Orb}(\mathbf{x})$ be the $\mathcal{A}$-orbit of an element $\mathbf{x} \in \bar{\mathfrak{a}}$.

Lemma 4.22. *Let* $\mathbf{x}$ *and* $\mathbf{y}$ *be elements of* $\bar{\mathfrak{a}}$ *such that* $\mathbf{x} \in \overline{\mathrm{Orb}(\mathbf{y})}$. *Then* $\dim \bar{\mathfrak{c}}(\mathbf{x}) \geq \dim \bar{\mathfrak{c}}(\mathbf{y})$.

Proof. The orbit $\mathrm{Orb}(\mathbf{y})$ intersects any open neighbourhood of $\mathbf{x}$, and, in particular, the set $X = \{\mathbf{z} \in \bar{\mathfrak{a}} \mid \dim(\bar{\mathfrak{c}}(\mathbf{z})) \leq \dim(\bar{\mathfrak{c}}(\mathbf{x}))\}$, which is open by Lemma 4.21. If $\mathbf{z} \in \mathrm{Orb}(\mathbf{y}) \cap X$, then $\dim \bar{\mathfrak{c}}(\mathbf{x}) \geq \dim \bar{\mathfrak{c}}(\mathbf{z}) = \dim \bar{\mathfrak{c}}(\mathbf{y})$. □

The stabiliser subscheme $\mathcal{A}_{\mathbf{x}}$ is, in general, non-reduced in positive characteristic. It is reduced (equivalently, smooth) if and only if the inclusion $\mathfrak{c}(\mathbf{x}) \supseteq \mathrm{Lie}(\mathcal{A}_{\mathbf{x}})$ is an equality (cf. [H95, 1.10]). If $\mathcal{A}_{\mathbf{x}}$ is smooth, the orbit-stabiliser theorem implies that

$$\dim(\mathfrak{a}) = m = \dim \mathcal{A}_{\mathbf{x}} + \dim \mathrm{Orb}(\mathbf{x}) = \dim \bar{\mathfrak{c}}(\mathbf{x}) + \dim \mathrm{Orb}(\mathbf{x}).$$

In particular, Lemma 4.22 follows from the inequality $\dim \mathrm{Orb}(\mathbf{x}) \leq \dim \mathrm{Orb}(\mathbf{y})$.

Let us further assume that $\mathcal{A} = \mathcal{G}$ is a simple connected simply connected algebraic group and $\bar{\mathfrak{a}} = \mathfrak{g}$ is a simply connected Chevalley Lie algebra. Let us fix a triangular decomposition $\mathfrak{g} = \mathfrak{n}_- \oplus \mathfrak{h} \oplus \mathfrak{n}$. An element $\mathbf{x} \in \mathfrak{g}$ is called **semisimple** if $\mathrm{Orb}(\mathbf{x}) \cap \mathfrak{h} \neq \emptyset$. An element $\mathbf{x} \in \mathfrak{g}$ is called **nilpotent** if $\mathrm{Orb}(\mathbf{x}) \cap \mathfrak{n} \neq \emptyset$. We call a representation $\mathbf{x} = \mathbf{x}_{\mathrm{s}} + \mathbf{x}_{\mathrm{n}}$ **a quasi-Jordan decomposition** if $\mathbf{x}_{\mathrm{s}} \in g(\mathfrak{h})$ (image of $\mathfrak{h}$ under g) and $\mathbf{x}_{\mathrm{n}} \in g(\mathfrak{n})$ for the same $g \in \mathcal{G}$.

Recall that **a Jordan decomposition** is a quasi-Jordan decomposition $\mathbf{x} = \mathbf{x}_{\mathrm{s}} + \mathbf{x}_{\mathrm{n}}$ such that $[\mathbf{x}_{\mathrm{s}}, \mathbf{x}_{\mathrm{n}}] = 0$. A Jordan decomposition exists and is unique if $\mathfrak{g}$ admits a non-degenerate bilinear form [KacW76, Theorem 4].

Notice that part (1) of the following lemma cannot be proved by the argument that the Lie subalgebra $\mathbb{K}\mathbf{x}$ is contained in a maximal soluble subalgebra: in characteristic 2 the Borel subalgebra $\mathfrak{b} = \mathfrak{h} \oplus \mathfrak{n}$ is not maximal soluble.

Lemma 4.23. *Assume that $p \neq 2$ or $\mathcal{G}$ is not of type C_l (in particular, this excludes $C_2 = B_2$ and $C_1 = A_1$). Then the following statements hold.*

1. *Every $\mathbf{x} \in \mathfrak{g}$ admits a (non-unique) quasi-Jordan decomposition $\mathbf{x} = \mathbf{x}_{\mathrm{s}} + \mathbf{x}_{\mathrm{n}}$.*
2. *$\mathbf{x}_{\mathrm{s}}$ belongs to the orbit closure $\overline{\mathrm{Orb}(\mathbf{x})}$.*
3. *If $\mathrm{Orb}(\mathbf{x})$ is closed, then $\mathbf{x}$ is semisimple.*
4. *$\dim \bar{\mathfrak{c}}(\mathbf{x}_s) \geq \dim \bar{\mathfrak{c}}(\mathbf{x})$.*

Proof. (cf. [KacW76, Section 3].) (1) Our assumption on $\mathfrak{g}$ assures the existence of a regular semisimple element $\mathbf{h} \in \mathfrak{h}$, i.e., an element such that $\bar{\mathfrak{c}}(\mathbf{h}) = \mathfrak{h}$. The differential $\mathrm{d}_{(e,\mathbf{h})}a : \mathfrak{g} \oplus \mathfrak{h} \to \mathfrak{g}$ of the action map $a : \mathcal{G} \times \mathfrak{h} \to \mathfrak{g}$ is given by the formula

$$\mathrm{d}_{(e,\mathbf{h})}a(\mathbf{x}, \mathbf{k}) = [\mathbf{x}, \mathbf{h}] + \mathbf{k}.$$

Since the adjoint operator $\mathrm{ad}(\mathbf{h})$ is a diagonalizable operator whose 0-eigenspace is $\mathfrak{h}$, the kernel of $\mathrm{d}_{(e,\mathbf{x})}a$ is $\mathfrak{h} \oplus 0$. Hence, the image of a contains an open subset of $\mathfrak{g}$. Since the set $\cup_{g \in \mathcal{G}} g(\mathfrak{b})$ contains the image of a, it is a dense subset of $\mathfrak{g}$.

Let $\mathcal{B}$ be the Borel subgroup of $\mathcal{G}$ whose Lie algebra is $\mathfrak{b}$. The quotient space $\mathcal{F} = \mathcal{G}/\mathcal{B}$ is a flag variety. Since $\mathcal{F}$ is projective, the projection map $\pi : \mathfrak{g} \times \mathcal{F} \to \mathfrak{g}$ is proper. The Springer variety $\mathcal{S} = \{(\mathbf{x}, g(\mathcal{B})) \,|\, \mathbf{x} \in g(\mathfrak{b})\}$ is closed in $\mathfrak{g} \times \mathcal{F}$. Hence, $\cup_{g \in \mathcal{G}} g(\mathfrak{b}) = \pi(\mathcal{S})$ is closed in $\mathfrak{g}$. Thus, $\cup_{g \in \mathcal{G}} g(\mathfrak{b}) = \mathfrak{g}$. Choosing g such that $\mathbf{x} \in g(\mathfrak{b})$ gives a decomposition.

(2) Suppose $\mathbf{x}_{\mathrm{s}} \in g(\mathfrak{h})$. Let $\mathcal{T}$ be the torus whose Lie algebra is $g(\mathfrak{h})$. We decompose $\mathbf{x}$ over the roots of $\mathcal{T}$:

$$\mathbf{x} = \mathbf{x}_{\mathrm{s}} + \mathbf{x}_{\mathrm{n}} = \mathbf{x}_0 + \sum_{\alpha \in Y(\mathcal{T})} \mathbf{x}_\alpha.$$

We can choose a basis of $Y(\mathcal{T})$ so that only positive roots appear. Hence, the action map $a : \mathcal{T} \to \mathfrak{g}$, $a(t) = t(\mathbf{x})$ extends alone the embedding $\mathcal{T} \hookrightarrow \mathbb{K}^l$ to a map $\widehat{a} : \mathbb{K}^l \to \mathfrak{g}$. Observe that $\mathbf{x}_{\mathrm{s}} = \widehat{a}(0)$.

Let $U \ni \mathbf{x}_{\mathrm{s}}$ be an open subset of $\mathfrak{g}$. Then $\widehat{a}^{-1}(U)$ is open in $\mathbb{K}^l$ and $\mathcal{T} \cap \widehat{a}^{-1}(U)$ is not empty. Pick $t \in \mathcal{T} \cap \widehat{a}^{-1}(U)$. Then $a(t) = t(\mathbf{x}) \in U$, thus, $\mathbf{x}_{\mathrm{s}} \in \overline{\mathcal{T}(\mathbf{x})} \subseteq \overline{\mathrm{Orb}(\mathbf{x})}$.

(3) This immediately follows from (1) and (2).

(4) This immediately follows from (2) and Lemma 4.22. $\square$

If α is a long simple root, its root vector $\mathbf{e}_\alpha \in \mathfrak{g} = \bar{\mathfrak{a}}$ is known as *the minimal nilpotent*. The dimension of $\mathrm{Orb}(\mathbf{e}_\alpha)$ is equal to $2(h^\vee - 1)$ (cf. [Wa99]).

Proposition 4.24. *Suppose that $l \geq 2$ and that the characteristic p of the field $\mathbb{K}$ is tolerable for $\mathfrak{g}$. Then for any noncentral $\mathbf{x} \in \mathfrak{a}$*

$$\dim \mathfrak{c}(\mathbf{x}) \leq \dim \bar{\mathfrak{c}}(\mathbf{e}_\alpha) = m - 2(h^\vee - 1).$$

Proof. Let $\mathbf{x} \in \mathfrak{a}$ ($\mathbf{y} \in \mathfrak{g}$) be a noncentral element with $\mathfrak{c}(\mathbf{x})$ ($\bar{\mathfrak{c}}(\mathbf{y})$ correspondingly) of the largest possible dimension. Observe that $\dim \mathfrak{c}(\mathbf{x}) \leq \dim \bar{\mathfrak{c}}(\mathbf{x}) \leq \dim \bar{\mathfrak{c}}(\mathbf{y})$.

Let us examine a quasi-Jordan decomposition $\mathbf{y} = \mathbf{y}_{\mathrm{s}} + \mathbf{y}_{\mathrm{n}}$. Since $\mathbf{y}_s \in \overline{\mathrm{Orb}(\mathbf{y})}$, we conclude that $\dim \bar{\mathfrak{c}}(\mathbf{y}_s) \geq \dim \bar{\mathfrak{c}}(\mathbf{y})$. But $\dim \bar{\mathfrak{c}}(\mathbf{y})$ is assumed to be maximal. There are two ways to reconcile this: either $\dim \bar{\mathfrak{c}}(\mathbf{y}_s) = \dim \bar{\mathfrak{c}}(\mathbf{y})$, or $\mathbf{y}_{\mathrm{s}}$ is central.

Suppose $\mathbf{y}_{\mathrm{s}}$ is central. Then $\mathbf{y}$ and $\mathbf{y}_{\mathrm{n}}$ have the same centralisers. We may assume that $\mathbf{y} = \mathbf{y}_{\mathrm{n}}$ is nilpotent. Lemma 4.22 allows us to assume without loss of generality that the orbit $\mathrm{Orb}(\mathbf{y})$ is minimal, that is, $\overline{\mathrm{Orb}(\mathbf{y})} = \mathrm{Orb}(\mathbf{y}) \cup \{0\}$. On the other hand, the closure $\overline{\mathrm{Orb}(\mathbf{y})}$ contains a root vector $\mathbf{e}_\beta$.

Let us prove the last statement. First, observe that $\mathbb{K}^\times \mathbf{y} \subseteq \mathrm{Orb}(\mathbf{y})$. If p is good, this immediately follows from Premet's version of Jacobson-Morozov Theorem [Pr95]. If $\mathrm{Orb}(\lambda \mathbf{y}) \neq \mathrm{Orb}(\mathbf{y})$ in an exceptional Lie algebra in a bad tolerable characteristic, then we observe two distinct nilpotent orbits with the same partition into Jordan blocks. It never occurs: all the partitions are listed in the VIGRE paper [Vi05, section 6]. The remaining case of $p = 2$ and $\mathfrak{g}$ is of type D_l is also settled in the VIGRE paper [Vi05]. Now let $\mathbf{y} \in g(\mathfrak{n})$, and $\mathcal{T}_0$ be the torus whose Lie algebra is $g(\mathfrak{h})$. Consider $\mathcal{T} := \mathcal{T}_0 \times \mathbb{K}^\times$ with the second factor acting on $\mathfrak{g}$ via the vector space structure. Write $\mathbf{y} = \sum_{\beta \in Y(\mathcal{T}_0)} \mathbf{y}_\beta$ using the roots of $\mathcal{T}_0$. The closure of the orbit $\overline{\mathcal{T}(\mathbf{y})}$ is contained in $\overline{\mathrm{Orb}(\mathbf{y})}$. Let us show that $\overline{\mathcal{T}(\mathbf{y})}$ contains one of $\mathbf{y}_\beta$. Let us write $\mathcal{T}_0 = G_\mathrm{m} \times G_\mathrm{m} \times \ldots \times G_\mathrm{m}$ and decompose $\mathbf{y} = \mathbf{y}_k + \mathbf{y}_{k+1} + \ldots + \mathbf{y}_n$ using the weights of the first factor G_m with $\mathbf{y}_k \neq 0$. Then

$$\mathcal{T}(\mathbf{y}) \supseteq \{(\lambda, 1, 1 \ldots, 1, \lambda^{-k}) \cdot \mathbf{y} | \lambda \in \mathbb{K}^\times\} = \{\mathbf{y}_k + \lambda^1 \mathbf{y}_{k+1} + \ldots + \lambda^{n-k} \mathbf{y}_n | \lambda \in \mathbb{K}^\times\}.$$

Hence, $\mathbf{y}_k \in \overline{\mathcal{T}(\mathbf{y})}$. Repeat this argument with $\mathbf{y}_k$ instead of $\mathbf{y}$ for the second factor of $\mathcal{T}_0$, and so on. At the end we arrive at nonzero $\mathbf{y}_\beta$, hence, $\mathbf{e}_\beta \in \overline{\mathrm{Orb}(\mathbf{y})}$.

Without loss of generality we now assume that $\mathbf{y} = \mathbf{e}_\beta$ for a simple root β. If p is good, then $\dim(\bar{\mathfrak{c}}(\mathbf{e}_\beta))$ does not depend on the field:

$$\bar{\mathfrak{c}}(\mathbf{e}_\beta) = \ker(d\beta : \mathfrak{h} \to \mathbb{K}) \oplus \bigoplus_{\gamma+\beta \text{ is not a root}} \mathfrak{g}_\gamma.$$

In particular, it is as in characteristic zero: the long root vector has a larger centraliser than the short root vector and $\dim \bar{\mathfrak{c}}(\mathbf{y}) = \dim \bar{\mathfrak{c}}(\mathbf{e}_\alpha) = m - 2(h^\vee - 1)$ [Wa99]. If $p = 2$ and $\mathfrak{g}$ is of type D_l, then a direct calculation gives the same formula for $\dim \bar{\mathfrak{c}}(\mathbf{e}_\alpha)$. In the exceptional cases in bad characteristics the orbits and their centralisers are computed in the VIGRE paper [Vi05]. One goes through their tables and establishes the formula for $\dim \bar{\mathfrak{c}}(\mathbf{y})$ in all the cases.

Now suppose $\dim \bar{\mathfrak{c}}(\mathbf{y}_s) = \dim \bar{\mathfrak{c}}(\mathbf{y})$. We may assume that $\mathbf{y} = \mathbf{y}_\mathrm{s}$ is semisimple. Then $\mathbf{y}$ is in some Cartan subalgebra $g^{-1}(\mathfrak{h})$ and $\dim \bar{\mathfrak{c}}(g(\mathbf{y})) = \dim \bar{\mathfrak{c}}(\mathbf{y})$. Moreover,

$$\bar{\mathfrak{c}}(g(\mathbf{y})) = \mathfrak{h} \oplus \bigoplus_{\{\alpha | \alpha(g(\mathbf{y}))=0\}} \mathfrak{g}_\alpha$$

is a reductive subalgebra. If $\varphi : \mathfrak{g} \to \mathfrak{g}^\flat$ is the canonical map (see Section 4.1.3), then $\dim \bar{\mathfrak{c}}(g(\mathbf{y})) = \dim \mathfrak{c}_{\mathfrak{g}^\flat}(\varphi(g(\mathbf{y})))$. It remains to examine the Lie algebras case by case and exhibit a non-zero element in $\mathfrak{h}^\flat$ with the maximal dimension of centraliser. This is done in Appendices A.6 and B. □

We may now prove the first part of Theorem D. We use m, l, r and s as in Definition 4.15. If $\dim(U) + \dim(V) > m + s + r$, we are done by Proposition 4.17:

$$\mathrm{codim}([U, V]) = 0 \leq (1 + v(\mathfrak{g}))(\mathrm{codim}(U) + \mathrm{codim}(V)).$$

Now we assume that $\dim(U) + \dim(V) \leq m + s + r$. It is known, see Proposition 4.19, that

$$\operatorname{codim}([U,V]) \leq l + \operatorname{codim}(U) + \operatorname{codim}(V).$$

It remains to notice that $l = v(\mathfrak{g})(m-s-r) \leq v(\mathfrak{g})(\operatorname{codim}(U) + \operatorname{codim}(V))$. The theorem is proved.

4.4 Proof of Theorem D: Rank 2

In this section $\mathbf{G}$ is a Chevalley group scheme of rank 2. The characteristic p of the field $\mathbb{K}$ is zero or very good for $\mathfrak{g}$. Let $\{\alpha, \beta\}$ be the set of simple roots of $\mathfrak{g}$ with $|\beta| \leq |\alpha|$. If $\mathfrak{g}$ is of type A_2 then α and β have the same length. The group $\mathcal{G} = \mathbf{G}(\overline{\mathbb{K}})$ acts on on $\mathfrak{g}$ via the adjoint action. By $\mathfrak{c}(\mathbf{x})$ we denote the centraliser $\mathfrak{c}_{\mathfrak{g}}(\mathbf{x})$ in this section. Let us summarise some standard facts about this adjoint action (cf. [H95]).

1. If $\mathbf{x} \in \mathfrak{g}$, the stabiliser $\mathcal{G}_{\mathbf{x}}$ is smooth, i.e., its Lie algebra is the centraliser $\mathfrak{c}(\mathbf{x})$.
2. The dimensions $\dim(\operatorname{Orb}(\mathbf{x})) = \dim(\mathcal{G}) - \dim(\mathfrak{c}(\mathbf{x}))$ and $\dim(\mathfrak{c}(\mathbf{x}))$ are even.
3. If $\mathbf{x} \neq 0$ is semisimple, $\dim(\mathfrak{c}(\mathbf{x})) \in \{2, 4\}$. Hence, $\dim(\operatorname{Orb}(\mathbf{x})) \in \{m-2, m-4\}$.
4. A truly mixed element $\mathbf{x} = \mathbf{x}_{\mathrm{s}} + \mathbf{x}_{\mathrm{n}}$ (with non-zero semisimple and nilpotent parts) is regular, i.e., $\dim(\mathfrak{c}(\mathbf{x})) = 2$ (cf. Lemma 4.23).
5. $\mathbf{x}$ is nilpotent if and only if $\overline{\operatorname{Orb}(\mathbf{x})}$ contains 0.
6. There is a unique orbit of regular nilpotent elements $\operatorname{Orb}(\mathbf{e}_r)$ where $\mathbf{e}_r = \mathbf{e}_\alpha + \mathbf{e}_\beta$. In particular, $\dim(\mathfrak{c}(\mathbf{e}_r)) = 2$ and $\dim(\operatorname{Orb}(\mathbf{e}_r)) = m-2$.
7. For two nilpotent elements $\mathbf{x}$ and $\mathbf{y}$ we write $\mathbf{x} \succeq \mathbf{y}$ if $\overline{\operatorname{Orb}(\mathbf{x})} \supseteq \operatorname{Orb}(\mathbf{y})$. The following are representatives of all the nilpotent orbits in $\mathfrak{g}$ (in brackets we report $[\dim(\operatorname{Orb}(\mathbf{x})), \dim(\mathfrak{c}(\mathbf{x}))]$):

   (a) If $\mathbf{G}$ is of type A_2, then

   $$\mathbf{e}_r\,[6,2] \succeq \mathbf{e}_\alpha\,[4,4] \succeq 0\,[0,8]\,.$$

   (b) If $\mathbf{G}$ is of type C_2, then $\mathbf{e}_\alpha$ and $\mathbf{e}_\beta$ are no longer in the same orbit and so we have

   $$\mathbf{e}_r\,[8,2] \succeq \mathbf{e}_\beta\,[6,4] \succeq \mathbf{e}_\alpha\,[4,6] \succeq 0\,[0,10]\,.$$

(c) If $\mathbf{G}$ is of type G_2, there is an additional subregular nilpotent orbit of an element $\mathbf{e}_{sr} = \mathbf{e}_{2\alpha+3\beta} + \mathbf{e}_\beta$. In this case we have

$$\mathbf{e}_r\,[12,2] \succeq \mathbf{e}_{sr}\,[10,4] \succeq \mathbf{e}_\beta\,[8,6] \succeq \mathbf{e}_\alpha\,[6,8] \succeq 0\,[0,14]\,.$$

We will now prove Theorem D for groups of type A_2, C_2 and G_2. We need to show that if U and V are subspaces of $\mathfrak{g}$, then inequality (♠) holds, i.e.

$$\dim([U,V]) \geq \dim(U) + \dim(V) - \dim\mathfrak{g}.$$

This is proved by repeated use of Lemma 4.18.

Now we give a case-by-case proof of inequality (♠). Without loss of generality we assume that $1 \leq \dim(U) \leq \dim(V)$ and that the field $\mathbb{K}$ is algebraically closed.

4.4.1 $\mathbf{G} = A_2$

Using the standard facts, observe that if $\mathbf{x} \in \mathfrak{g} \setminus \{0\}$, then $\dim(\mathfrak{c}(\mathbf{x})) \leq 4$. Moreover, if $\dim(\mathfrak{c}(\mathbf{x})) = 4$, then either $\mathbf{x} \in \mathrm{Orb}(\mathbf{e}_\alpha)$, or $\mathbf{x}$ is semisimple. Since $\dim\mathfrak{g} = 8$, we need to establish that

$$\dim([U,V]) \geq \dim(U) + \dim(V) - 8.$$

Now we consider various possibilities.

Case 1: If $\dim(U) \leq 4$, then $\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim(\mathfrak{c}(\mathbf{x})) \leq 4 \leq 8 - \dim(U)$ for any nonzero $\mathbf{x} \in U$. We are done by Lemma 4.18.

Case 2: If $\dim(U) + \dim(V) > 12$, then the hypotheses of Proposition 4.17 hold. Hence, $[U,V] = \mathfrak{g}$ that obviously implies the desired conclusion.

Therefore we may suppose that $\dim(U) + \dim(V) \leq 12$ and $\dim U \geq 5$. This leaves us with the following two cases.

Case 3: $\dim(U) = 5$ and $\dim(V) \leq 7$. We need to show that

$$\dim([U,V]) \geq \dim(U) + \dim(V) - 8 = \dim(V) - 3.$$

As $\dim(\overline{\mathrm{Orb}(\mathbf{e}_\alpha)}) = 4$, we may pick $\mathbf{x} \in U$ with $\mathbf{x} \notin \overline{\mathrm{Orb}(\mathbf{e}_\alpha)}$. If $\mathbf{x}$ is regular, we are done by Lemma 4.18 since $\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim(\mathfrak{c}(\mathbf{x})) = 2$. If $\mathbf{x}$ is not regular, then $\dim(\mathfrak{c}(\mathbf{x})) = 4$ and $\mathbf{x}$ is semisimple. In particular, its centraliser $\mathfrak{c}(\mathbf{x})$ contains a Cartan subalgebra $g(\mathfrak{h})$ of $\mathfrak{g}$.

Let us consider the intersection $V \cap \mathfrak{c}(\mathbf{x})$. If $\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq 3$, we are done by Lemma 4.18. Otherwise, $V \supseteq \mathfrak{c}(\mathbf{x})$ and V contains a regular semisimple element $\mathbf{y} \in g(\mathfrak{h}) \subseteq V$. If $U \supseteq \mathfrak{c}(\mathbf{y}) = g(\mathfrak{h})$, then $U \ni \mathbf{y}$ and we are done by Lemma 4.18 as in the previous paragraph. Otherwise, $\dim(U \cap \mathfrak{c}(\mathbf{y})) \leq 1$ and we finish the proof using Lemma 4.18:

$$\dim([U, V]) \geq \dim(U) - \dim(U \cap \mathfrak{c}(\mathbf{y})) \geq 5 - 1 = 4 \geq \dim(V) - 3.$$

Case 4: $\dim(U) = \dim(V) = 6$. This time we must show that

$$\dim([U, V]) \geq 4 = \dim(V) - 2.$$

By Lemma 4.18 it suffices to find a regular element in $\mathbf{x} \in U$ (or in V) since $\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim(\mathfrak{c}(\mathbf{x})) = 2$. Observe that

$$\dim(U \cap V) \geq \dim(U) + \dim(V) - 8 = 4 = \dim(\overline{\mathrm{Orb}(\mathbf{e}_\alpha)}).$$

Since $\overline{\mathrm{Orb}(\mathbf{e}_\alpha)}$ is an irreducible algebraic variety and not an affine space, there exists $\mathbf{x} \in U \cap V$ such that $\mathbf{x} \notin \overline{\mathrm{Orb}(\mathbf{e}_\alpha)}$. If $\mathbf{x}$ is regular, we are done. If $\mathbf{x}$ is not regular, $\mathbf{x}$ is semisimple and its centraliser $\mathfrak{c}(\mathbf{x}) = \mathbb{K}\mathbf{x} \oplus \mathfrak{l}$, a direct sum of Lie algebras $\mathbb{K}\mathbf{x} \cong \mathbb{K}$ and $\mathfrak{l} \cong \mathfrak{sl}_2(\mathbb{K})$.

Consider the intersection $V \cap \mathfrak{c}(\mathbf{x})$. If $\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq 2$, we are done by Lemma 4.18 as before. Assume that $\dim(V \cap \mathfrak{c}(\mathbf{x})) \geq 3$. If $\dim(V \cap \mathfrak{c}(\mathbf{x})) = 4$, V contains $\mathfrak{c}(\mathbf{x})$ and consequently a regular semisimple element $\mathbf{y}$.

Finally, consider the case $\dim(V \cap \mathfrak{c}(\mathbf{x})) = 3$. Let π_2 be the natural projection $\pi_2 : \mathfrak{c}(\mathbf{x}) \to \mathfrak{l}$ and set $W := \pi_2(V \cap \mathfrak{c}(\mathbf{x}))$. Since $\mathbb{K}\mathbf{x} \subseteq V \cap \mathfrak{c}(\mathbf{x})$, the subspace W of $\mathfrak{sl}_2(\mathbb{K})$ is 2-dimensional. Clearly, $V \cap \mathfrak{c}(\mathbf{x}) \subseteq \mathbb{K}\mathbf{x} \oplus W$. Since both spaces have dimension 3, $V \cap \mathfrak{c}(\mathbf{x}) = \mathbb{K}\mathbf{x} \oplus W$. Then $W = \mathbf{a}^\perp$ (with respect to the Killing form), where $0 \neq \mathbf{a} \in \mathfrak{sl}_2(\mathbb{K})$ is either semisimple or nilpotent. In both cases W contains a nonzero nilpotent element $\mathbf{z}$. Thus, we have found a regular element $\mathbf{x}+\mathbf{z} \in V \cap \mathfrak{c}(\mathbf{x})$. This finishes the proof for A_2.

4.4.2 $\mathbf{G} = C_2$

Notice that this time $\dim(\mathfrak{c}(\mathbf{x})) \leq 6$ for all $0 \neq \mathbf{x} \in \mathfrak{g}$. Moreover, if $\dim(\mathfrak{c}(\mathbf{x})) = 6$, $\mathbf{x} \in \mathrm{Orb}(\mathbf{e}_\alpha)$. Finally, the set $\overline{\mathrm{Orb}(\mathbf{e}_\alpha)} = \mathrm{Orb}(\mathbf{e}_\alpha) \cup \{0\}$ is a 4-dimensional cone, and the set $\overline{\mathrm{Orb}(\mathbf{e}_\beta)} = \mathrm{Orb}(\mathbf{e}_\beta) \cup \mathrm{Orb}(\mathbf{e}_\alpha) \cup \{0\}$ is a 6-dimensional cone.

As $\dim \mathfrak{g} = 10$, this time we need to show that

$$\dim([U, V]) \geq \dim(U) + \dim(V) - 10 = \dim(V) - (10 - \dim(U)).$$

Case 1: $\dim(U) \leq 4$. We are done by Lemma 4.18 since for any $0 \neq \mathbf{x} \in U$,

$$\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim(\mathfrak{c}(\mathbf{x})) \leq 6 \leq 10 - \dim(U).$$

Case 2: $5 \leq \dim(U) \leq 6$. Hence, we may choose $\mathbf{x} \in U$ such that $\mathbf{x} \notin \overline{\mathrm{Orb}(\mathbf{e}_\alpha)}$. We are done by Lemma 4.18 since

$$\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim(\mathfrak{c}(\mathbf{x})) \leq 4 \leq 10 - \dim(U).$$

Case 3: If $\dim(U) + \dim(V) > 16$, then then the hypotheses of Proposition 4.17 hold. Hence, $[U, V] = \mathfrak{g}$, which implies the desired conclusion.

Therefore, we may assume that $\dim(U) + \dim(V) \leq 16$ and $\dim(U) \geq 7$. This leaves us with the remaining two cases.

Case 4: $\dim(U) = 7$, $\dim(V) \leq 9$. Now we must show that $\dim([U, V]) \geq \dim(V) - 3$. By Lemma 4.18 it suffices to pick $\mathbf{x} \in U$ with $\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq 3$. In particular, a regular element will do.

Let us choose $\mathbf{x} \in U$ such that $\mathbf{x} \notin \overline{\mathrm{Orb}(\mathbf{e}_\beta)}$. If $\mathbf{x}$ is regular, we are done. If $\mathbf{x}$ is not regular, $\mathbf{x}$ is semisimple. Hence, its centraliser $\mathfrak{c}(\mathbf{x})$ contains a Cartan subalgebra $g(\mathfrak{h})$. Let us consider the intersection $V \cap \mathfrak{c}(\mathbf{x})$. If $\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq 3$, we are done again. Assume that $\dim(V \cap \mathfrak{c}(\mathbf{x})) = 4$. Consequently, $V \supseteq \mathfrak{c}(\mathbf{x})$ and V contains a regular semisimple element $\mathbf{y} \in g(\mathfrak{h}) \subseteq V$. Now if $U \supseteq \mathfrak{c}(\mathbf{y}) = g(\mathfrak{h})$, then we have found a regular element $\mathbf{y} \in U$. Otherwise, $\dim(U \cap \mathfrak{c}(\mathbf{y})) \leq 1$, and so, as $\mathbf{y} \in V$, we finish using inequality ($\clubsuit$) of Lemma 4.18:

$$\dim([U, V]) \geq \dim(U) - \dim(U \cap \mathfrak{c}(\mathbf{y})) \geq 7 - 1 = 6 \geq \dim(V) - 3.$$

Case 5: $\dim(U) = \dim(V) = 8$. Let us observe that

$$\dim(U \cap V) \geq \dim(U) + \dim(V) - 10 = 6 = \dim(\overline{\mathrm{Orb}(\mathbf{e}_\beta)}).$$

Since $\overline{\mathrm{Orb}(\mathbf{e}_\beta)}$ is an irreducible algebraic variety and not an affine space, there exists $\mathbf{x} \in U \cap V$ such that $\mathbf{x} \notin \overline{\mathrm{Orb}(\mathbf{e}_\beta)}$. If $\mathbf{x}$ is regular, we are done by Lemma 4.18:

$$\dim([U, V]) \geq \dim(V) - \dim(V \cap \mathfrak{c}(\mathbf{x})) \geq 8 - 2 = 6 = \dim(U) + \dim(V) - 10.$$

If $\mathbf{x}$ is not regular, then $\mathbf{x}$ is semisimple and its centraliser $\mathfrak{c}(\mathbf{x}) = \mathbb{K}\mathbf{x} \oplus \mathfrak{l}$, a direct sum of Lie algebras $\mathbb{K}$ and $\mathfrak{l} \cong \mathfrak{sl}_2(\mathbb{K})$. If $\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq 2$, then by Lemma 4.18

$$\dim([U, V]) \geq \dim(V) - \dim(V \cap \mathfrak{c}(\mathbf{x})) \geq 8 - 2 = 6.$$

Thus we may assume that $\dim(V \cap \mathfrak{c}(\mathbf{x})) \geq 3$. We now repeat the argument from the last paragraph of Section 4.4.1. This concludes the proof for C_2.

4.4.3 $\mathbf{G} = G_2$

In this case $\dim(\mathfrak{c}(\mathbf{x})) \leq 8$ for all $0 \neq \mathbf{x} \in \mathfrak{g}$. Moreover, if $\dim(\mathfrak{c}(\mathbf{x})) = 8$, then $\mathbf{x} \in \mathrm{Orb}(\mathbf{e}_\alpha)$. The centre of $\mathfrak{c}(\mathbf{e}_\alpha)$ is $\overline{\mathbb{K}}\mathbf{e}_\alpha$. Finally, the set $\overline{\mathrm{Orb}(\mathbf{e}_\alpha)} = \mathrm{Orb}(\mathbf{e}_\alpha) \cup \{0\}$ is a 6-dimensional cone, the set $\overline{\mathrm{Orb}(\mathbf{e}_\beta)} = \mathrm{Orb}(\mathbf{e}_\beta) \cup \mathrm{Orb}(\mathbf{e}_\alpha) \cup \{0\}$ is an 8-dimensional cone and the set $\overline{\mathrm{Orb}(\mathbf{e}_{sr})} = \mathrm{Orb}(\mathbf{e}_{sr}) \cup \mathrm{Orb}(\mathbf{e}_\beta) \cup \mathrm{Orb}(\mathbf{e}_\alpha) \cup \{0\}$ is a 10-dimensional cone.

As $\dim \mathfrak{g} = 14$, our goal now is to show that

$$\dim([U, V]) \geq \dim(U) + \dim(V) - 14.$$

In order to do so, as before, we are going to consider several mutually exclusive cases.

Case 1: $\dim(U) \leq 6$. We are done by Lemma 4.18 since for any $0 \neq \mathbf{x} \in U$,

$$\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim(\mathfrak{c}(\mathbf{x})) \leq 8 \leq 14 - \dim(U).$$

Case 2: $7 \leq \dim(U) \leq 8$. In this case we may choose $\mathbf{x} \in U$ such that $\mathbf{x} \notin \overline{\mathrm{Orb}(\mathbf{e}_\alpha)}$. We are done by Lemma 4.18 since

$$\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim(\mathfrak{c}(\mathbf{x})) \leq 6 \leq 14 - \dim(U).$$

Case 3: $9 \leq \dim(U) \leq 10$. Now we may pick $\mathbf{x} \in U$ such that $\mathbf{x} \notin \overline{\mathrm{Orb}(\mathbf{e}_\beta)}$. Again we are done by Lemma 4.18 since

$$\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq \dim(\mathfrak{c}(\mathbf{x})) \leq 4 \leq 14 - \dim(U).$$

Case 4: If $\dim(U) + \dim(V) > 22$, then $[U, V] = \mathfrak{g}$ by Proposition 4.17. This leaves us with a single last possibility.

Case 5: $\dim(U) = \dim(V) = 11$. It remains to show that

$$\dim([U, V]) \geq 8 = \dim(V) - 3.$$

By dimension considerations we can choose $\mathbf{x} \in U$ such that $\mathbf{x} \notin \overline{\mathrm{Orb}(\mathbf{e}_{sr})}$. Then $\dim(\mathfrak{c}(\mathbf{x})) \leq 4$. If $\dim(V \cap \mathfrak{c}(\mathbf{x})) \leq 3$, we are done by by Lemma 4.18. Thus we may assume that $\dim(\mathfrak{c}(\mathbf{x})) = 4$ and $\mathfrak{c}(\mathbf{x}) \subseteq V$. Since $\mathbf{x}$ is not nilpotent, $\mathbf{x}$ must be semisimple. Hence, $\mathfrak{c}(\mathbf{x}) \subseteq V$ contains a Cartan subalgebra $g(\mathfrak{h})$ and, therefore, a regular semisimple element $\mathbf{y} \in g(\mathfrak{h})$. We are done by Lemma 4.18:

$$\dim(U \cap \mathfrak{c}(\mathbf{y})) \leq \dim(\mathfrak{c}(\mathbf{y})) \leq 2.$$

We have finished the proof of Theorem D.

Chapter 5

Subgroup growth of twisted Chevalley groups over $\mathbb{F}_p([[t]])$

5.1 Twisted Chevalley groups

Here we include a partial solution to the problem of determining the subgroup growth of the twisted counterparts of the groups from Chapter 4.

In the previous chapter we examined the subgroup growth of the congruence subgroups of Chevalley groups over $\mathbb{F}_p([[t]])$. These are the groups related to the Kac-Moody groups corresponding to extended Cartan matrices, i.e. the so-called untwisted types of affine Kac-Moody groups. Now we would like to look at the remainder of affine Kac-Moody groups over $\mathbb{F}_p$, namely the twisted groups

$$\mathbf{G}_{sc}^{\widetilde{A}'_1}(\mathbb{F}_p), \mathbf{G}_{sc}^{\widetilde{B}^t_n}(\mathbb{F}_p), \mathbf{G}_{sc}^{\widetilde{C}'_n}(\mathbb{F}_p), \mathbf{G}_{sc}^{\widetilde{C}^t_n}(\mathbb{F}_p), \mathbf{G}_{sc}^{\widetilde{F}^t_4}(\mathbb{F}_p), \mathbf{G}_{sc}^{\widetilde{G}^t_2}(\mathbb{F}_p),$$

whose bounded presentations we calculated in Section 3.4.

It is possible to realise the Kac-Moody algebras associated to the twisted GCMs as fixed point subalgebras of Kac-Moody algebras associated to extended Cartan matrices under certain automorphisms (cf. [Car05] section 18.4), and similarly it is possible to realise the twisted groups above as fixed point subgroups of the untwisted affine Kac-Moody groups under certain automorphisms (cf. [Ra92] chapter 4).
Now let $\mathbf{G}$ be a simple simply connected Chevalley group scheme and $G = \mathbf{G}(\mathbb{F}_p[[t]])$ a Chevalley group with G_1 its first congruence subgroup. Let σ be a group automorphism of an untwisted affine Kac-Moody group corresponding to G of the type just described. The automorphism σ induces an automorphism of G, which we by abuse of notation also call σ. Let G^σ be the fixed points of G under this automorphism

and let

$$G_1^\sigma := G^\sigma \cap G_1.$$

In this chapter we postulate the following provisional result on the subgroup growth of G_1^σ.

Conjecture 5.1. *Let p be a very good prime for $\mathbf{G}$. If σ has order 2 and G^σ is not of type $\widetilde{C}_n^t$ then we have*

$$a_{p^k}(G_1^\sigma) \leq p^{\frac{D-1}{2}k^2+(\dim \mathfrak{m}-1)k}.$$

If G^σ is of type $\widetilde{G}_2^t$ then we have

$$a_{p^k}(G_1^\sigma) \leq p^{\frac{(3+\lceil\varepsilon\rceil)}{2}k^2+6k}.$$

Here $\mathfrak{m}$ is a known finite dimensional Lie algebra module associated with $\mathbf{G}$ and D and ε are positive constants that need to be determined. This result is unproven since it relies on some other conjectures that we will state below.

In order to establish this result, we need to know what happens to the graded Lie algebra under these automorphisms. Recall that for the first congruence subgroup G_1 of the Chevalley group $\mathbf{G}(\mathbb{F}_p[[t]])$ the graded Lie algebra $\mathcal{L}$ was isomorphic to $\mathfrak{g} \otimes_{\mathbb{F}_p} t\mathbb{F}_p[t]$, where $\mathfrak{g}$ was the simple finite dimensional Lie algebra over $\mathbb{F}_p$ corresponding to $\mathbf{G}$. So first we need to know what happens to $\mathfrak{g}$ under such an automorphism. On the level of this finite dimensional Lie algebra, this automorphism is a graph automorphism. We again call this graph automorphism σ. Let $\mathfrak{g}^\sigma$ denote the fixed point subalgebra (or eigenspace with eigenvalue 1) of $\mathfrak{g}$ under this map. Over the complex numbers $\mathfrak{g}$ splits into the eigenspaces of σ as follows.

Proposition 5.2 ([Car05], Prop. 18.8, 18.13)**.** *(i) Let $\mathfrak{g}$ be a simple Lie algebra of type A_l, D_{l+1} or E_6 and σ be a graph automorphism of order 2. Let $\mathfrak{g}_{-1}$ be the eigenspace of σ on $\mathfrak{g}$ with eigenvalue -1. Then we have the vector space decomposition*

$$\mathfrak{g} = \mathfrak{g}^\sigma \oplus \mathfrak{g}_{-1}$$

and $\mathfrak{g}_{-1}$ is an irreducible $\mathfrak{g}^\sigma$-module.

(ii) Let $\mathfrak{g}$ have type D_4 and σ be a graph automorphism of $\mathfrak{g}$ of order 3. Let $\mathfrak{g}_\omega$, $\mathfrak{g}_{\omega^2}$ be the eigenspaces of σ with eigenvalues ω, ω^2 where $\omega = e^{2\pi i/3}$. Then we have the vector space decomposition

$$\mathfrak{g} = \mathfrak{g}^\sigma \oplus \mathfrak{g}_\omega \oplus \mathfrak{g}_{\omega^2}$$

and $\mathfrak{g}_\omega$, $\mathfrak{g}_{\omega^2}$ are both irreducible $\mathfrak{g}^\sigma$-modules.

In very good characteristic the Lie algebra $\mathfrak{g}$ behaves as it does over $\mathbb{C}$, so the above still holds. We now go over the different cases of this decomposition more carefully - this is largely taken from the proof of the above proposition. We let $L(A)$ denote the simple Lie algebra with Cartan matrix of type A over a field $\mathbb{K}$ of very good characteristic.

$\widetilde{A}_1'$: We have $\mathfrak{g} = L(A_2) \cong \mathfrak{sl}_3$ of dimension 8, $\mathfrak{g}^\sigma = L(A_1) \cong \mathfrak{sl}_2$ of dimension 3, and the decomposition is

$$L(A_2) = L(A_1) \oplus \mathfrak{g}_{-1},$$

where $\mathfrak{g}_{-1}$ is the irreducible $L(A_1)$-module of highest weight $4\omega_1$ and dimension 5.

$\widetilde{C}_l'$: We have $\mathfrak{g} = L(A_{2l}) \cong \mathfrak{sl}_{2l+1}$ of dimension $2l(2l+2)$, $\mathfrak{g}^\sigma = L(B_l)$ of dimension $l(2l+1)$, and the decomposition is

$$L(A_{2l}) = L(B_l) \oplus \mathfrak{g}_{-1},$$

where $\mathfrak{g}_{-1}$ is the irreducible $L(B_l)$-module of highest weight $2\omega_1$ and dimension $l(2l+3)$.

$\widetilde{C}_l^t$: We have $\mathfrak{g} = L(D_{l+1})$ of dimension $(l+1)(2l+1)$, $\mathfrak{g}^\sigma = L(B_l)$ of dimension $l(2l+1)$, and the decomposition is

$$L(D_{l+1}) = L(B_l) \oplus \mathfrak{g}_{-1},$$

where $\mathfrak{g}_{-1}$ is the irreducible $L(B_l)$-module of highest weight ω_1 and dimension $2l+1$.

$\widetilde{B}_l^t$: We have $\mathfrak{g} = L(A_{2l-1})$ of dimension $(2l-1)(2l+1)$, $\mathfrak{g}^\sigma = L(C_l)$ of dimension $l(2l+1)$, and the decomposition is

$$L(A_{2l-1}) = L(C_l) \oplus \mathfrak{g}_{-1},$$

where $\mathfrak{g}_{-1}$ is the irreducible $L(C_l)$-module of highest weight ω_2 and dimension $(l-1)(2l+1)$.

$\widetilde{F}_4^t$: We have $\mathfrak{g} = L(E_6)$ of dimension 78, $\mathfrak{g}^\sigma = L(F_4)$ of dimension 52, and the decomposition is

$$L(E_6) = L(F_4) \oplus \mathfrak{g}_{-1},$$

where $\mathfrak{g}_{-1}$ is the irreducible $L(F_4)$-module of highest weight ω_4 and dimension 26.

$\widetilde{G}_2^t$**:** We have $\mathfrak{g} = L(D_4)$ of dimension 28, $\mathfrak{g}^\sigma = L(G_2)$ of dimension 14, and the decomposition is

$$L(D_4) = L(G_2) \oplus \mathfrak{g}_\omega \oplus \mathfrak{g}_{\omega^2},$$

where $\mathfrak{g}_\omega$, $\mathfrak{g}_{\omega^2}$ are both irreducible $L(G_2)$-modules of highest weight ω_2 and dimension 7.

Now we can proceed to looking at what happens to $\mathcal{L}$ under the suitable automorphism. We do this separately for the cases of order 2 and order 3.

5.2 General methods when σ has order 2

Let $\mathfrak{g}$ be the finite dimensional Lie algebra appearing in the realisation of the affine Kac-Moody algebra we are twisting. As above we write $\mathfrak{g}^\sigma$ for the fixed point Lie subalgebra of $\mathfrak{g}$ under the automorphism σ of order 2. We have the vector space decomposition $\mathfrak{g} = \mathfrak{g}^\sigma \oplus \mathfrak{g}_{-1}$, where $\mathfrak{g}_{-1}$ is the -1-eigenspace of σ. We know that this eigenspace is a $\mathfrak{g}^\sigma$-module, and we denote this module by $\mathfrak{m}$.
By considering eigenvalues, note that inside $\mathfrak{g}$ we have $[\mathfrak{m}, \mathfrak{m}] \subseteq \mathfrak{g}^\sigma$.
The graded Lie algebra $\mathcal{L}$ of the untwisted Chevalley group is isomorphic to $\mathfrak{g} \otimes_{\mathbb{F}_p} t\mathbb{F}_p[t]$. By abuse of notation we also call this $\mathcal{L}$, so we have

$$\mathcal{L} = (\mathfrak{g} \otimes t) \oplus (\mathfrak{g} \otimes t^2) \oplus (\mathfrak{g} \otimes t^3) \oplus (\mathfrak{g} \otimes t^4) \otimes \dots,$$

where we write $\otimes$ for $\otimes_{\mathbb{F}_p}$.
The automorphism we need to define on $\mathcal{L}$ comes from a suitable automorphism of the associated affine Kac-Moody group. See Chapter 4 of [Ra92] for details of how such an automorphism is constructed. For our purposes it is enough to know what it does on $\mathcal{L}$. It turns out that here it is a variant of the **twisted graph automorphisms** that occur for the loop realisations of the affine Kac-Moody algebras of untwisted type, see Section 18.4 of [Car05] for details of this.
We proceed to define a map $\sigma : \mathcal{L} \to \mathcal{L}$ (by abuse of notation we again use the same notation for the automorphism). Each element a of $\mathcal{L}$ is of the form $a = \Sigma_{k=1}^{\infty} a_i \otimes t^k$ with $a_k \in \mathfrak{g}$, where only finitely many non-zero summands are allowed. We can define σ by specifying what it does on homogeneous components of form $a_k \otimes t^k$. Let r be the order of σ. Then in analogy with the twisted graph automorphisms of affine Kac-Moody algebras, we define $\delta = e^{2\pi i/r}$. In this section we have $r = 2$, so $\delta = -1$. Then we define

$$\sigma(a_k \otimes t^k) := \sigma(a_k) \otimes \delta^{-k} t^k$$

and extend this by linearity to all of $\mathcal{L}$. If k is odd, say $k = 2k' + 1$, we see that we have

$$\sigma(a_k \otimes t^k) = \sigma(a_k) \otimes (-1)^{-2k'-1} t^k = -\sigma(a_k) \otimes t^k,$$

and if k is even, say $k = 2k'$, we have

$$\sigma(a_k \otimes t^k) = \sigma(a_k) \otimes (-1)^{-2k'} t^k = \sigma(a_k) \otimes t^k.$$

The elements in $\mathfrak{g}$ for which $\sigma(a) = a$ are precisely the ones in the fixed point subalgebra $\mathfrak{g}^\sigma$, and the elements in $\mathfrak{g}$ for which $\sigma(a) = -a$ are precisely the ones in the -1-eigenspace $\mathfrak{m}$.
Let $\mathcal{L}^\sigma$ be the fixed point subalgebra of $\mathcal{L}$ under this automorphism. Then we see that we have:

$$\mathcal{L}^\sigma = (\mathfrak{m} \otimes t) \oplus (\mathfrak{g}^\sigma \otimes t^2) \oplus (\mathfrak{m} \otimes t^3) \oplus (\mathfrak{g}^\sigma \otimes t^4) \oplus \dots$$

To proceed like we did in the previous chapter we will need a result analogous to Theorem D. Recall that for subspaces U and V of a Lie algebra $\mathfrak{g}$ this result placed an upper bound on the codimension of $[U, V]$ in terms of a multiple of $\operatorname{codim}(U) + \operatorname{codim}(V)$. MAGMA computations indicate that similar results hold for the twisted cases, but we are currently unable to prove them. Instead we make the following conjectures.

Conjecture 5.3. *Let $[\ ,\ ]_1 : \mathfrak{g}^\sigma \times \mathfrak{g}^\sigma \to \mathfrak{g}^\sigma$ be the ordinary Lie bracket in $\mathfrak{g}^\sigma$. Let U and V be two subspaces of $\mathfrak{g}^\sigma$. Then we have*

$$\operatorname{codim}([U, V]_1) \leq A\,(\operatorname{codim}(U) + \operatorname{codim}(V))$$

for some constant $A \geq 1$.

Conjecture 5.4. *Let $[\ ,\ ]_2 : \mathfrak{g}^\sigma \times \mathfrak{m} \to \mathfrak{m}$ be the action of $\mathfrak{g}^\sigma$ on its module $\mathfrak{m}$. Let U be a subspace of $\mathfrak{g}^\sigma$ and V be a subspace of $\mathfrak{m}$. Then we have*

$$\operatorname{codim}([U, V]_2) \leq B\,(\operatorname{codim}(U) + \operatorname{codim}(V))$$

for some constant $B \geq 1$.

Conjecture 5.5. *Let $[\ ,\ ]_3 : \mathfrak{m} \times \mathfrak{m} \to \mathfrak{g}^\sigma$ be the Lie bracket in $\mathfrak{g}$ restricted to $\mathfrak{m}$. Let U and V be two subspaces of $\mathfrak{m}$. Then we have*

$$\operatorname{codim}([U, V]_3) \leq C\,(\operatorname{codim}(U) + \operatorname{codim}(V))$$

for some constant $C \geq 1$.

Assuming these results we can proceed to prove an analogue of Theorem C.

We let $\mathcal{H}$ be a graded subalgebra of finite codimension in $\mathcal{L}^\sigma$. Since every element $a \in \mathcal{L}$ can be uniquely written as $a = \Sigma_{i=1}^{\infty} a_i \otimes t^i$ with $a_i \in \mathfrak{g}$, we can define $l(a) := a_s$ where s is the smallest integer such that $a_s \neq 0$, and in this case $s := \deg(a)$. Now set

$$H_i := \langle l(a) \mid a \in \mathcal{H} \text{ with } \deg(a) = i \rangle.$$

Note that $H_i = \{l(a) \mid a \in \mathcal{H} \text{ with } \deg(a) = i\} \cup \{0\}$. Similarly we define

$$L_i := \langle l(a) \mid a \in \mathcal{L}^\sigma \text{ with } \deg(a) = i \rangle.$$

Then

$$\dim \frac{\mathcal{L}^\sigma}{\mathcal{H}} = \sum_{i=1}^{\infty} \dim \frac{L_i}{H_i}.$$

and since the codimension of $\mathcal{H}$ is finite, this sum has finitely many non-zero terms. We have

$$L_i = \begin{cases} \mathfrak{g}^\sigma & \text{for i even} \\ \mathfrak{m} & \text{for i odd} \end{cases}.$$

Next we note that

$$[H_i \otimes t^i, H_j \otimes t^j] \subseteq [H_i, H_j] \otimes t^{i+j} \subseteq \overline{H}_{i+j} \otimes t^{i+j},$$

where $\overline{H}_{i+j}$ is the Lie algebra part of the $i+j$-th term of $\mathcal{H}' = [\mathcal{H}, \mathcal{H}]$. So $\dim \overline{H}_{i+j} \geq \dim [H_i, H_j]$ and so

$$\dim \frac{L_{i+j}}{[H_i, H_j]} \geq \dim \frac{L_{i+j}}{\overline{H}_{i+j}}.$$

Now we consider these inequalities for $i = j$ and $i = j + 1$:

$$j=1 \quad i=1 : \quad \dim \frac{L_2}{[H_1, H_1]_3} \geq \dim \frac{L_2}{\overline{H}_2} \qquad \text{where } L_2 = \mathfrak{g}^\sigma \text{ and } H_1 \subseteq \mathfrak{m}$$

$$j=1 \quad i=2 : \quad \dim \frac{L_3}{[H_2, H_1]_2} \geq \dim \frac{L_3}{\overline{H}_3} \qquad \text{where } L_2 = \mathfrak{m} \text{ and } H_2 \subseteq \mathfrak{g}^\sigma, H_1 \subseteq \mathfrak{m}$$

$$j=2 \quad i=2 : \quad \dim \frac{L_4}{[H_2, H_2]_1} \geq \dim \frac{L_4}{\overline{H}_4} \qquad \text{where } L_4 = \mathfrak{g}^\sigma \text{ and } H_2 \subseteq \mathfrak{g}^\sigma$$

$$j=2 \quad i=3 : \quad \dim \frac{L_5}{[H_3, H_2]_2} \geq \dim \frac{L_5}{\overline{H}_5} \qquad \text{where } L_5 = \mathfrak{m} \text{ and } H_3 \subseteq \mathfrak{m}, H_2 \subseteq \mathfrak{g}$$

$$j=3 \quad i=3 : \quad \dim \frac{L_6}{[H_3, H_3]_3} \geq \dim \frac{L_6}{\overline{H}_6} \qquad \text{where } L_6 = \mathfrak{g}^\sigma \text{ and } H_3 \subseteq \mathfrak{m}$$

$$j=3 \quad i=4 : \quad \dim \frac{L_7}{[H_4, H_3]_2} \geq \dim \frac{L_7}{\overline{H}_7} \qquad \text{where } L_7 = \mathfrak{m} \text{ and } H_4 \subseteq \mathfrak{g}^\sigma, H_3 \subseteq \mathfrak{m}$$

$$j = 4 \quad i = 4 \ : \quad \dim \frac{L_8}{[H_4, H_4]_1} \geq \dim \frac{L_8}{\overline{H}_8} \qquad \text{where } L_8 = \mathfrak{g}^\sigma \text{ and } H_4 \subseteq \mathfrak{g}^\sigma$$

$$j = 4 \quad i = 5 \ : \quad \dim \frac{L_9}{[H_5, H_4]_2} \geq \dim \frac{L_9}{\overline{H}_9} \qquad \text{where } L_9 = \mathfrak{m} \text{ and } H_5 \subseteq \mathfrak{m}, H_4 \subseteq \mathfrak{g}^\sigma$$

and so on. Adding these together we get

$$\begin{aligned}
\dim \frac{\mathcal{L}^\sigma}{\mathcal{H}'} &= \sum_{i=1}^{\infty} \dim \frac{L_i}{\overline{H}_i} \\
&\leq \dim \frac{L_1}{\overline{H}_1} + \sum_{1 \geq i \geq j \geq i+1}^{\infty} \dim \frac{L_{i+j}}{[H_i, H_j]} \\
&\leq \dim L_1 + \sum_{1 \geq i \geq j \geq i+1}^{\infty} \dim \frac{L_{i+j}}{[H_i, H_j]} \\
&= \dim \mathfrak{m} + (\dim \frac{L_2}{[H_1, H_1]_3} + \dim \frac{L_6}{[H_3, H_3]_3} + \ldots) \\
&\quad + (\dim \frac{L_4}{[H_2, H_2]_1} + \dim \frac{L_8}{[H_4, H_4]_1} + \ldots) \\
&\quad + (\dim \frac{L_3}{[H_2, H_1]_2} + \dim \frac{L_5}{[H_3, H_2]_2} + \ldots) \\
&\leq \dim \mathfrak{m} + C\, (\dim \frac{L_1}{H_1} + \dim \frac{L_1}{H_1} + \dim \frac{L_3}{H_3} + \dim \frac{L_3}{H_3} + \ldots) \\
&\quad + A\, (\dim \frac{L_2}{H_2} + \dim \frac{L_2}{H_2} + \dim \frac{L_4}{H_4} + \dim \frac{L_4}{H_4} + \ldots) \\
&\quad + B\, (\dim \frac{L_1}{H_1} + \dim \frac{L_2}{H_2} + \dim \frac{L_2}{H_2} + \dim \frac{L_3}{H_3} + + \dim \frac{L_3}{H_3} \ldots) \\
&= \dim \mathfrak{m} + (2C + B) \dim \frac{L_1}{H_1} + (2A + 2B) \dim \frac{L_2}{H_2} + (2C + 2B) \dim \frac{L_3}{H_3} \\
&\quad + (2A + 2B) \dim \frac{L_4}{H_4} + (2C + 2B) \dim \frac{L_5}{H_5} + (2A + 2B) \dim \frac{L_6}{H_6} + \ldots
\end{aligned}$$

We now set $D \coloneqq \max\{2A + 2B\,,\, 2C + 2B\}$. Then the whole sum above is less than or equal to $\dim \mathfrak{m} + D \dim \frac{\mathcal{L}}{\mathcal{H}}$.
So we have $\dim \frac{\mathcal{L}^\sigma}{\mathcal{H}'} \leq \dim \mathfrak{m} + D \dim \frac{\mathcal{L}^\sigma}{\mathcal{H}}$. And since we also have $\dim \frac{\mathcal{L}^\sigma}{\mathcal{H}'} = \dim \frac{\mathcal{L}^\sigma}{\mathcal{H}} + \dim \frac{\mathcal{H}}{\mathcal{H}'}$, this gives us

$$\dim \frac{\mathcal{H}}{\mathcal{H}'} \leq \dim \mathfrak{m} + (D - 1) \dim \frac{\mathcal{L}^\sigma}{\mathcal{H}}.$$

Following the method described in the proof of Theorem C we can use this estimate to give us the following estimate on the subgroup growth of the corresponding first congruence subgroup G_1^σ:

$$
\begin{aligned}
a_{p^k}(G_1^\sigma) &\leq p^{\sum_{i=0}^{i=k-1} \dim \mathfrak{m} + (D-1)i} \\
&= p^{\frac{D-1}{2}k^2 + (\dim \mathfrak{m} - \frac{D}{2} + \frac{1}{2})k} \\
&\leq p^{\frac{D-1}{2}k^2 + (\dim \mathfrak{m} - 1)k}.
\end{aligned}
$$

We would now need to look at these three products in more detail to establish precise values for the constants A, B and C in the above conjectures.
Note that in the case ${}^t\widetilde{C}_l$, $\mathfrak{m} \wedge \mathfrak{m} \cong \mathfrak{g}$, so the product $[\ ,\ ]_3$ is the wedge product. We state a lemma about the dimension of the wedge product of two subspaces of a vector space.

Lemma 5.6. *Let V be a finite dimensional vector space of dimension n and let U and W be subspaces of V of dimensions k and l, respectively. Then $U \bigwedge W$ is a subspace of $\bigwedge^2 V = V \bigwedge V$. Assume furthermore that* $\dim U \cap W = m$. *Then we have*

$$\dim(U \bigwedge W) = \binom{m}{2} + kl - m^2.$$

Proof. For any basis $y_1, \ldots, y_n$ of V, $\{y_i \wedge y_j \mid 1 \leq i < j \leq n\}$ is a basis of $\bigwedge^2 V$. We can pick a basis

$$u_1, \ldots, u_{k-m}, \quad x_1, \ldots, x_m, \quad w_1, \ldots, w_{l-m}, \quad v_1, \ldots, v_{n-(k+l-m)}$$

for V such that the x_i form a basis for $U \cap W$, the u_i form a basis for a complement of $U \cap W$ in U, the w_i form a basis for a complement of $U \cap W$ in W, and the v_i form a basis for a complement of $U + W$ in V. If we take the wedge products of this basis to get a basis of $\bigwedge^2 V$, then the elements in this basis of form $y_i \wedge y_j$ where $y_i \in U$ and $y_j \in V$ will form a basis of $U \bigwedge V$. Hence we proceed to count the number of elements of this form.
One option of getting elements of this form is if the first component is of form u_i and the second component is of form x_j or w_j. There are $(k-m)\cdot(m+l-m) = (k-m)\cdot l$ elements like this.
Another option is that both the first and second component are of the form x_i. These elements form a basis of $\bigwedge^2(U \cap W)$, so there are $\binom{m}{2}$ of them.
The last option is that the first component is of form x_i and the second is of form w_j. There are $m \cdot (l-m)$ elements like this.
Adding these together we get

$$
\begin{aligned}
\dim(U \bigwedge W) &= \dim\left(\frac{U}{U \cap W}\right) \cdot \dim W + \dim \bigwedge^2 (U \cap W) + \dim\left(\frac{W}{U \cap W}\right) \cdot \dim(U \cap W) \\
&= (k-m) \cdot l + \binom{m}{2} + (l-m) \cdot m
\end{aligned}
$$

$$= \binom{m}{2} + kl - m^2.$$

□

We see that in the ${}^t\widetilde{C}_l$ case Conjecture 5.5 cannot be uniformly true, i.e. it is impossible to find a constant C that will work for all l. Indeed, in that case $\mathfrak{m}$ has dimension $2l+1$ and $\mathfrak{g}^\sigma = \mathfrak{m} \wedge \mathfrak{m}$ has dimension $\binom{2l+1}{2} = l(2l+1)$. If we pick U and V to to be subspaces of codimension 1 in $\mathfrak{m}$ such that $U = V$, then we have $C(\mathrm{codim}(U) + \mathrm{codim}(V)) = 2C$ but $\mathrm{codim}(U \bigwedge V) = \dim \mathfrak{g}^\sigma - (\binom{2l}{2} + 2l \cdot 2l - (2l)^2) = 2l$. So it is impossible to pick a constant C that will make Conjecture 5.5 true for all l, the best we can do is a constant depending on l.
In the other cases the product maps through the wedge but has a kernel so we expect the conjectures to hold.

5.3 $\widetilde{G}_2^t(\mathbb{F}_p)$

Here we do as in the previous section, now for groups where the twisting automorphism has order 3. There is only one type of these: $\widetilde{G}_2^t$. As we saw above, the finite Lie algebra $\mathfrak{g}$ of type D_4 has an eigenspace decomposition

$$\mathfrak{g} = \mathfrak{g}^\sigma \oplus \mathfrak{g}_\omega \oplus \mathfrak{g}_{\omega^2},$$

where $\mathfrak{g}^\sigma$ is a finite Lie algebra of type G_2 and dimension 14, $\omega = e^{2\pi i/3}$ and $\mathfrak{g}_\omega$, $\mathfrak{g}_{\omega^2}$ are both irreducible $\mathfrak{g}^\sigma$-modules of dimension 7. We call these modules $\mathfrak{m}_1$ and $\mathfrak{m}_2$.

As before, the graded Lie algebra $\mathcal{L}$ has form

$$\mathcal{L} = (\mathfrak{g} \otimes t) \oplus (\mathfrak{g} \otimes t^2) \oplus (\mathfrak{g} \otimes t^3) \oplus (\mathfrak{g} \otimes t^4) \oplus \dots.$$

Again we define $\delta = e^{2\pi i/r}$, where r is the order of σ. So here $\delta = \omega$. We again define the map $\sigma : \mathcal{L} \to \mathcal{L}$ by

$$\sigma(a_k \otimes t^k) := \sigma(a_k) \otimes \delta^{-k} t^k$$

and extend this by linearity to all of $\mathcal{L}$. By similar reasoning to the precious case we get that the fixed point subalgebra $\mathcal{L}^\sigma$ of $\mathcal{L}$ under this map is

$$\mathcal{L}^\sigma = (\mathfrak{m}_1 \otimes t) \oplus (\mathfrak{m}_2 \otimes t^2) \oplus (\mathfrak{g}^\sigma \otimes t^3) \oplus (\mathfrak{m}_1 \otimes t^4) \oplus (\mathfrak{m}_2 \otimes t^5) \oplus (\mathfrak{g}^\sigma \otimes t^6) \oplus \dots$$

Let us denote by L_i each term in the expression for $\mathcal{L}^\sigma$, so that we get $\mathcal{L}^\sigma = \bigoplus_{i=1}^\infty L_i$.
Now let $\mathcal{H}$ be a graded Lie subalgebra of $\mathcal{L}^\sigma$ of finite codimension.

To proceed further, we again make the following conjectures, which can be seen as twisted analogues of Theorem D.

Conjecture 5.7.

Let U and V be subspaces of $\mathfrak{g}^\sigma$. Then we have

$$\dim \frac{\mathfrak{g}^\sigma}{[U,V]} \leq \dim \frac{\mathfrak{g}^\sigma}{U} + \dim \frac{\mathfrak{g}^\sigma}{V}.$$

Conjecture 5.8.

Let U and V be subspaces of $\mathfrak{m}_1$. Then we have

$$\dim \frac{\mathfrak{m}_2}{[U,V]} \leq \dim \frac{\mathfrak{m}_1}{U} + \dim \frac{\mathfrak{m}_1}{V}.$$

Similarly, if U and V are subspaces of $\mathfrak{m}_2$, we have $\dim \frac{\mathfrak{m}_1}{[U,V]} \leq \dim \frac{\mathfrak{m}_2}{U} + \dim \frac{\mathfrak{v}_2}{V}$.

Conjecture 5.9.

Let U be a subspace of $\mathfrak{g}^\sigma$ and let V be a subspace of $\mathfrak{m}_2$. Then we have

$$\dim \frac{\mathfrak{m}_2}{[U,V]} \leq \dim \frac{\mathfrak{g}^\sigma}{U} + \dim \frac{\mathfrak{m}_2}{V}.$$

Similarly, if U is a subspace of $\mathfrak{m}_1$ and V is a subspace of $\mathfrak{g}^\sigma$, we have $\dim \frac{\mathfrak{m}_1}{[U,V]} \leq \dim \frac{\mathfrak{m}_1}{U} + \dim \frac{\mathfrak{g}^\sigma}{V}$.

Conjecture 5.10.

Let U be a subspace of $\mathfrak{m}_2$ and let V be a subspace of $\mathfrak{m}_1$. Then we have

$$\dim \frac{\mathfrak{g}^\sigma}{[U,V]} \leq (1+\varepsilon)(\dim \frac{\mathfrak{m}_2}{U} + \dim \frac{\mathfrak{m}_1}{V}),$$

where $\varepsilon > 0$.

We then get the following conditional result.

Lemma 5.11. *Let $\mathcal{H}$ be a graded Lie subalgebra of finite codimension in $\mathcal{L}^\sigma$. Then*

$$\dim \mathcal{H}/\mathcal{H}' \leq 7 + (3 + \lceil \varepsilon \rceil) \dim \mathcal{L}^\sigma/\mathcal{H},$$

where $\mathcal{H}' = [\mathcal{H}, \mathcal{H}]$ and $\lceil \varepsilon \rceil$ is the smallest integer which is greater than or equal to ε.

Proof. We follow the proof of Theorem C, which closely follows the proof of Lemma 1 from [AbNS03]. Every $a \in \mathcal{L}^\sigma$ can be written uniquely in the form

$$a = \sum_{s=1}^{\infty} a_s \otimes t^s,$$

where $a_s \in L_s$, where L_s is given by

$$L_s = \begin{cases} \mathfrak{m}_1, & \text{if } s \equiv 1 \mod 3 \\ \mathfrak{m}_2, & \text{if } s \equiv 2 \mod 3 \\ \mathfrak{g}^\sigma, & \text{if } s \equiv 0 \mod 3. \end{cases}$$

We define the leading term of a by $l(a) := a_s$, where s is the least integer such that $a_s \neq 0$, and we call this s the degree $\deg(a)$ of a. We put

$$H_i := \langle l(a) \mid a \in \mathcal{H} \text{ with } \deg(a) = i \rangle.$$

So H_i is the i-th homogeneous component of $\mathcal{H}$. We therefore have

$$\dim \mathcal{L}^\sigma / \mathcal{H} = \sum_{i=1}^{\infty} \dim L_i / H_i, \tag{5.1}$$

and since we assume $\dim \mathcal{L}^\sigma / \mathcal{H}$ is finite, this sum has finitely many non-zero summands. We have

$$[H_i \otimes t^i, H_j \otimes t^j] = [H_i, H_j] \otimes t^{i+j} \subseteq \overline{H}_{i+j} \otimes t^{i+j}, \tag{5.2}$$

where

$$\overline{H}_i := \langle l(a) \mid a \in \mathcal{H}' \text{ with } \deg(a) = i \rangle$$

(so $\overline{H}_i$ is the i-th homogeneous component of $\mathcal{H}'$, which is a graded Lie subalgebra of $\mathcal{H}$). So the inclusion in equation (5.2) implies

$$\dim L_{i+j} / [H_i, H_j] \geq \dim L_{i+j} / \overline{H}_{i+j}. \tag{5.3}$$

We now expand the following sum and bound each term from above using (5.3) (and the fact that $\dim \frac{L_1}{H_1} \leq \dim L_1 = 7$):

$$\begin{aligned} \dim \mathcal{L}^\sigma / \mathcal{H}' = \sum_{i=1}^{\infty} \dim L_i / \overline{H}_i &= \dim \frac{L_1}{\overline{H}_1} + \dim \frac{L_2}{\overline{H}_2} + \dim \frac{L_3}{\overline{H}_3} + \dim \frac{L_4}{\overline{H}_4} + \dim \frac{L_5}{\overline{H}_5} + \dim \frac{L_6}{\overline{H}_6} \\ &+ \dim \frac{L_7}{\overline{H}_7} + \dim \frac{L_8}{\overline{H}_8} + \dim \frac{L_9}{\overline{H}_9} \dim \frac{L_{10}}{\overline{H}_{10}} + \dim \frac{L_{11}}{\overline{H}_{11}} \\ &+ \dim \frac{L_{12}}{\overline{H}_{12}} + \dim \frac{L_{13}}{\overline{H}_{13}} + \dim \frac{L_{14}}{\overline{H}_{14}} + \dim \frac{L_{15}}{\overline{H}_{15}} + \dim \frac{L_{16}}{\overline{H}_{16}} + \dots \\ &\leq 7 + \dim \frac{L_2}{[H_1, H_1]} \dim \frac{L_3}{[H_2, H_1]} + \dim \frac{L_4}{[H_2, H_2]} + \dim \frac{L_5}{[H_3, H_2]} \\ &+ \dim \frac{L_6}{[H_3, H_3]} + \dim \frac{L_7}{[H_4, H_3]} + \dim \frac{L_8}{[H_4, H_4]} + \dim \frac{L_9}{[H_5, H_4]} \end{aligned}$$

$$+\dim\frac{L_{10}}{[H_5,H_5]}+\dim\frac{L_{11}}{[H_6,H_5]}+\dim\frac{L_{12}}{[H_6,H_6]}+\dim\frac{L_{13}}{[H_7,H_6]}$$
$$+\dim\frac{L_{14}}{[H_7,H_7]}++\dim\frac{L_{15}}{[H_8,H_7]}++\dim\frac{L_{16}}{[H_8,H_8]}\dots$$

Now we use our four conjectures to bound each term in this sum:

$$\begin{aligned}
&\le 7+(\dim\frac{L_1}{H_1}+\dim\frac{L_1}{H_1})+(1+\varepsilon)(\dim\frac{L_2}{H_2}+\dim\frac{L_1}{H_1})+(\dim\frac{L_2}{H_2}+\dim\frac{L_2}{H_2})\\
&\quad+(\dim\frac{L_3}{H_3}+\dim\frac{L_2}{H_2})+(\dim\frac{L_3}{H_3}+\dim\frac{L_3}{H_3})+(\dim\frac{L_4}{H_4}+\dim\frac{L_3}{H_3})\\
&\quad+(\dim\frac{L_4}{H_4}+\dim\frac{L_4}{H_4})+(1+\varepsilon)(\dim\frac{L_5}{H_5}+\dim\frac{L_4}{H_4})+(\dim\frac{L_5}{H_5}+\dim\frac{L_5}{H_5})\\
&\quad+(\dim\frac{L_6}{H_6}+\dim\frac{L_5}{H_5})+(\dim\frac{L_6}{H_6}+\dim\frac{L_6}{H_6})+(\dim\frac{L_7}{H_7}+\dim\frac{L_6}{H_6})\\
&\quad+(\dim\frac{L_7}{H_7}+\dim\frac{L_7}{H_7})+(1+\varepsilon)(\dim\frac{L_8}{H_8}+\dim\frac{L_7}{H_7})+(\dim\frac{L_8}{H_8}+\dim\frac{L_8}{H_8})+\dots
\end{aligned}$$

And rearranging this we get

$$\begin{aligned}
&=7+(4+\varepsilon)\dim\frac{L_1}{H_1}+(4+\varepsilon)\dim\frac{L_2}{H_2}+4\dim\frac{L_3}{H_3}+(4+\varepsilon)\dim\frac{L_4}{H_4}+(4+\varepsilon)\dim\frac{L_5}{H_5}\\
&\quad+4\dim\frac{L_6}{H_6}+(4+\varepsilon)\dim\frac{L_7}{H_7}+(4+\varepsilon)\dim\frac{L_8}{H_8}+\dots\\
&\le 7+(4+\lceil\varepsilon\rceil)\sum_{i=1}^{\infty}\dim\frac{L_i}{H_i}\\
&=7+(4+\lceil\varepsilon\rceil)\dim\mathcal{L}^\sigma/\mathcal{H}.
\end{aligned}$$

And since we have $\dim\mathcal{L}^\sigma/\mathcal{H}'=\dim\mathcal{L}^\sigma/\mathcal{H}+\dim\mathcal{H}/\mathcal{H}'$, by substracting $\dim\mathcal{L}^\sigma/\mathcal{H}$ from each side we get the desired

$$\dim\mathcal{H}/\mathcal{H}'\le 7+(3+\lceil\varepsilon\rceil)\dim\mathcal{L}^\sigma/\mathcal{H}.$$

□

Now let G_1^σ denote the intersection of the first congruence subgroup of $D_4(\mathbb{F}_p[[t]])$ with the subgroup consisting of fixed points G^σ of $G=D_4(\mathbb{F}_p[[t]])$ under the automorphism σ of order 3. Following the method described in the proof of Theorem C, the above estimate on the dimension of $\dim\mathcal{H}/\mathcal{H}'$ can give us the following estimate on the subgroup growth of G_1^σ:

$$\begin{aligned}
a_{p^k}(G_1^\sigma)&\le p^{\sum_{i=0}^{i=k-1}7+(3+\lceil\varepsilon\rceil)i}\\
&=p^{\frac{(3+\lceil\varepsilon\rceil)}{2}k^2+(7-\frac{3}{2}-\frac{\lceil\varepsilon\rceil}{2})k}\\
&\le p^{\frac{(3+\lceil\varepsilon\rceil)}{2}k^2+6k}.
\end{aligned}$$

Appendix A

Tables

A.1 Presentations of $\mathbf{G}(\mathbb{F}_q)$

Table A.1: Presentations of $\mathbf{G}(\mathbb{F}_q)$ [GKaKasL11]

Group	q odd				q even			
	$\lvert D_\sigma\rvert$	$\lvert R_\sigma\rvert$	label	contains	$\lvert D_\sigma\rvert$	$\lvert R_\sigma\rvert$	label	contains
$\mathrm{SL}(2,q)$	3	9	σ_1		3	5	ρ_1	
$\mathrm{SL}(3,q)$	4	14	σ_2	σ_1	4	10	ρ_2	ρ_1
$\mathrm{SL}(4,q)$	5	20	σ_3	σ_1	5	16	ρ_3	ρ_1
$\mathrm{SL}(4,q)$	6	21	σ_4	σ_1, σ_2	6	17	ρ_4	ρ_1, ρ_2
$\mathrm{SL}(n,q)$, $5 \leq n \leq 8$	5	21	σ_5	σ_1	5	17	ρ_5	ρ_1
$\mathrm{SL}(n,q)$, $5 \leq n \leq 8$	6	22	σ_6	σ_1, σ_2	6	18	ρ_6	ρ_1, ρ_2
$\mathrm{SL}(n,q)$, $n \geq 9$	6	25	σ_7	σ_1	6	21	ρ_7	ρ_1
$\mathrm{SL}(n,q)$, $n \geq 9$	7	26	σ_8	σ_1, σ_2	7	22	ρ_8	ρ_1, ρ_2
$\mathrm{Sp}(4,q)$	5	27	σ_9	σ_1 (short)				
$\mathrm{Sp}(4,q)$	6	28	σ_{10}	σ_1 (twice)	6	20	ρ_{10}	ρ_1 (twice)
$\mathrm{Sp}(2n,q)$, $n \geq 3$	8	47	σ_{11}		9	40	ρ_{11}	
$\mathrm{Spin}(2n+1,q)$, $n \geq 3$	9	48	σ_{12}					
$\mathrm{Spin}(8,q)$	6	29	σ_{13}	σ_1	6	25	ρ_{13}	ρ_1
$\mathrm{Spin}(2n,q)$, $5 \leq n \leq 8$	6	30	σ_{14}	σ_1	6	26	ρ_{14}	ρ_1
$\mathrm{Spin}(2n,q)$, $n \geq 9$	7	34	σ_{15}	σ_1	7	30	ρ_{15}	ρ_1
$\mathrm{G}_2(q)$	6	31	σ_{16}	σ_1 (twice)	6	23	ρ_{16}	ρ_1 (twice)

A.2 Generators and Relations of $\widetilde{X}(q)$

Table A.2: Generators and Relations of $\widetilde{X}(q)$

Group	q odd		q even	
	generators	relations	generators	relations
$\widetilde{A}_2(q)$	5	26	5	22
$\widetilde{A}_3(q)$	7	34	7	30
$\widetilde{A}_n(q)$, $4 \leq n \leq 7$	7	35	7	31
$\widetilde{A}_n(q)$, $n \geq 8$	9	43	9	39
$\widetilde{B}_3(q)$	8	43	8	35
$\widetilde{B}^t_3(q)$	7	42	8	35
$\widetilde{B}_4(q)$, $\widetilde{B}^t_4(q)$	8	51	9	44
$\widetilde{B}_n(q)$, $\widetilde{B}^t_n(q)$, $5 \leq n \leq 8$	8	52	9	45
$\widetilde{B}_n(q)$, $\widetilde{B}^t_n(q)$, $n \geq 9$	9	56	10	49
$\widetilde{C}_2(q)$, $\widetilde{C}'_2(q)$	7	49	9	39
$\widetilde{C}_n(q)$, $n \geq 3$	10	69	12	59
$\widetilde{C}'_n(q)$, $n \geq 3$	11	70	12	59
$\widetilde{C}^t_2(q)$	8	50	9	39
$\widetilde{C}^t_n(q)$	12	71	12	59
$\widetilde{D}_4(q)$	7	38	7	34
$\widetilde{D}_5(q)$	7	39	7	35
$\widetilde{D}_n(q)$, $6 \leq n \leq 8$	7	38	7	34
$\widetilde{D}_n(q)$, $n \geq 9$	8	42	8	38
$\widetilde{E}_6(q)$	7	36	7	32
$\widetilde{E}_7(q)$	6	30	6	26
$\widetilde{E}_8(q)$	7	34	7	30
$\widetilde{F}_4(q)$, $\widetilde{F}^t_4(q)$	8	50	9	43
$\widetilde{G}_2(q)$, $\widetilde{G}^t_2(q)$	7	40	7	32

A.3 Relations of $\mathbf{G}(\mathbb{F}_q[t, t^{-1}])$ with 2 generators

Table A.3: Relations of $\mathbf{G}(\mathbb{F}_q[t, t^{-1}])$ with 2 generators

type	$\mathbf{G}$	$\lvert R_\sigma \rvert$	$\lvert R_\sigma \rvert$	type	$\mathbf{G}$	$\lvert R_\sigma \rvert$	$\lvert R_\sigma \rvert$
		q odd	q even			q odd	q even
	SL_3	29	25		Spin_7	45	38
	SL_4	37	33		Spin_9	54	47
A_{n-1}	SL_n, $4 \leq n \leq 8$	38	34	B_n	Spin_{2n+1}, $5 \leq n \leq 8$	55	48
	SL_n, $n \geq 9$	46	42		Spin_{2n+1}, $n \geq 9$	59	52
	Spin_8	41	37		Sp_4	52	42
	Spin_{10}	42	38		Sp_6	61	51
D_n	Spin_{2n}, $6 \leq n \leq 8$	41	37	C_n	Sp_8	67	57
	Spin_{2n}, $n \geq 9$	45	41		Sp_{2n}, $5 \leq n \leq 8$	68	58
	E_6	39	35		Sp_{2n}, $n \geq 9$	72	62
E_n	E_7	33	29	F_4	F_4	53	46
	E_8	37	33	G_2	G_2	43	35

A.4 Extra Generators and Relations for $\widetilde{X}(q)_{ad}$ and $\widetilde{X}_{ad}(q)$

The columns of Table A.4 are organised as follows. We list Dynkin's labels for affine groups and Cartan labels for finite groups in Column 1. Column 2 contains the group $\mathcal{P}/\mathcal{Q}$: by $(a_1, \ldots, a_k)$ we mean the group $\mathbb{Z}/a_1 \times \ldots \times \mathbb{Z}/a_k$.

The next two columns are related to $X(q)_{ad}$. Column 3 lists the minimal number of generators for $Z(q)$. We get a generator if there is a non-trivial homomorphism from a cyclic direct summand $\mathbb{Z}/k$ of $\mathcal{P}/\mathcal{Q}$ to $\mathbb{F}_q^\times$. We introduce a symbol $\mathfrak{A}(k)$, equal to 1, if $gcd(k, q-1) > 1$ and 0 if $gcd(k, q-1) = 1$. Column 4 is a maximal possible value of $\mathfrak{A}(k)$ taken over all q: this is the number of extra relations to describe $X(q)_{ad}$ for generic q.

The right three columns are related to $X_{ad}(q)$. Column 3 lists the minimal number of generators for $H(q)$. We get a generator if there is a non-trivial quotient by the k-th powers, where $\mathbb{Z}/k$ is a direct summand of $\mathcal{P}/\mathcal{Q}$: $\mathrm{Ext}^1(\mathbb{Z}/k, \mathbb{F}_q^\times) \cong \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^k$. This is controlled by the symbol $\mathfrak{A}(k)$. No generator arises from the infinite cyclic group: $\mathrm{Ext}^1(\mathbb{Z}, \mathbb{F}_q^\times) = 0$, yet the infinite cyclic group appears only in the affine types where $H(q)$ has an extra generator. Hence, $|D_1| = |D_2|$. Column 4 uses a maximal possible value of $\mathfrak{A}(k)$: this is a number of extra generators needed to describe $X_{ad}(q)$ for generic q. The last column is the maximal cardinality of $D_1^\sharp \cup R_2^\sharp \cup D_2^{act}$, the number of extra relations needed to describe $X_{ad}(q)$. In our computation we use the estimates $|D_1^\sharp| = |D_1| = |D_2|$, $|R_2^\sharp| = |R_2| = |D_2|$ and $|D_2^{act}| = 2|D_2|$. The latter holds because $X(q)$ is generated by 2 elements (with few exceptions, see Theorem 3.12). Hence, $|D_1^\sharp \cup R_2^\sharp \cup D_2^{act}| = 4|D_1|$.

Table A.4: Extra Generators and Relations for $\widetilde{X}(q)_{ad}$ and $\widetilde{X}_{ad}(q)$

X_n	$\mathcal{P}/\mathcal{Q}$	$\lvert D_1\rvert = \lvert D_2\rvert$	max $(\lvert D_1\rvert = \lvert D_2\rvert)$	max $\lvert D_1^\sharp \cup R_2^\sharp \cup D_2^{act}\rvert$
A_n	$(n+1)$	$\mathfrak{A}(n+1)$	1	4
B_n, C_n, E_7	(2)	$\mathfrak{A}(2)$	1	4
D_{2n}	$(2,2)$	$2\mathfrak{A}(2)$	2	8
D_{2n+1}	(4)	$\mathfrak{A}(2)$	1	4
G_2, F_4, E_8	$()$	0	0	0
E_6	(3)	$\mathfrak{A}(3)$	1	4
$\widetilde{A}_{n-1}$	$(0,n)$	$1+\mathfrak{A}(n)$	2	8
$\widetilde{B}_n, \widetilde{C}_n, \widetilde{E}_7, \widetilde{B}_n^t, \widetilde{C}_n^t$	$(0,2)$	$1+\mathfrak{A}(2)$	2	8
$\widetilde{D}_{2n}$	$(0,2,2)$	$1+2\mathfrak{A}(2)$	3	12
$\widetilde{D}_{2n+1}$	$(0,4)$	$1+\mathfrak{A}(2)$	2	8
$\widetilde{G}_2, \widetilde{F}_4, \widetilde{E}_8, \widetilde{C}_n', \widetilde{F}_4^t, \widetilde{G}_2^t$	(0)	1	1	4
$\widetilde{E}_6$	$(0,3)$	$1+\mathfrak{A}(3)$	2	8

A.5 Generators and Relations of Classical $\mathbf{G}(\mathbb{F}_q[t, t^{-1}])$

Table A.5: Generators and Relations of Classical $\mathbf{G}(\mathbb{F}_q[t, t^{-1}])$

$\mathbf{G}$	D_σ	R_σ, q odd	R_σ, q even	$\mathbf{G}$	D_σ	R_σ	D_σ	R_σ
					q odd		q even	
PSL_3	5	28	24	SO_7	9	48	8	36
PSL_n, $4 \leq n \leq 8$	7	37	33	SO_9	9	56	9	45
PSL_n, $n \geq 9$	9	45	41	SO_{2n+1}, $5 \leq n \leq 8$	9	57	9	46
PGL_3	6	31	27	SO_{2n+1}, $n \geq 9$	10	61	10	50
PGL_n, $4 \leq n \leq 8$	8	40	36	SO_8 or SO_{2n}, $6 \leq n \leq 8$	8	43	7	35
PGL_n, $n \geq 9$	10	48	44	SO_{10}	8	44	7	36
				SO_{2n}, $n \geq 9$	9	47	8	39

A.6 Ridgeline numbers and maximal dimensions of centralisers

The columns of Table A.6 are organised as follows. Column 3 contains the nullity r of an invariant form. It is equal to $\dim \mathfrak{z}$. Column 4 contains the dual Coxeter number. Column 5 contains the ridgeline number. Column 6 contains dimension of the centraliser of the minimal nilpotent. Column 7 contains a minimal non-central semisimple element in $\mathfrak{g}^\flat$, using simple coweights $\mathbf{y}_i$ and the enumeration of roots in Bourbaki [Bo68]. Column 8 contains the dimension of the centraliser of the minimal semisimple element in $\mathfrak{g}^\flat$.

Table A.6: Ridgeline numbers and maximal dimensions of centralisers

type of $\mathfrak{g}$	p	r	$h^\vee$	$v(\mathfrak{g})$	$m-2(h^\vee-1)$	$\mathbf{y}$	$\dim \mathfrak{c}(\mathbf{y})$
$A_l, l \geq 2$	$(p, l+1) = 1$	0	$l+1$	$\frac{1}{2}$	l^2	$\mathbf{y}_1$	l^2
$A_l, l \geq 2$	$p \mid (l+1)$	1	$l+1$	$\frac{l}{2l-1}$	l^2	$\mathbf{y}_1$	l^2
$B_l,\ l \geqslant 3$	$p \neq 2$	0	$2l-1$	$\frac{1}{4}(1+\frac{1}{l-1})$	$2l^2-3l+4$	$\mathbf{y}_1$	$2l^2-3l+2$
$C_l,\ l \geq 2$	$p \neq 2$	0	$l+1$	$\frac{1}{2}$	$2l^2-l$	$\mathbf{y}_1$	$2l^2-3l+2$
$D_l,\ l \geq 4$	$p \neq 2$	0	$2l-2$	$\frac{1}{4}(1+\frac{3}{2l-3})$	$2l^2-5l+6$	$\mathbf{y}_1$	$2l^2-5l+4$
$D_l,\ l = 2l_0 \geq 4$	2	2	$2l-2$	$\frac{1}{4}(1+\frac{2}{l-2})$	$2l^2-5l+6$	$\mathbf{y}_1$	$2l^2-5l+4$
$D_l,\ l = 2l_0+1 \geq 4$	2	1	$2l-2$	$\frac{1}{4}(1+\frac{7}{4l-7})$	$2l^2-5l+6$	$\mathbf{y}_1$	$2l^2-5l+4$
G_2	$p > 3$	0	4	$\frac{1}{3}$	8	$\mathbf{y}_1$	4
G_2	$p = 2$	0	4	$\frac{1}{3}$	8	$\mathbf{y}_1$	6
F_4	$p \neq 2$	0	9	$\frac{1}{4}$	36	$\mathbf{y}_1$	22
E_6	$p \neq 3$	0	12	$\frac{3}{11}$	56	$\mathbf{y}_1$	46
E_6	3	1	12	$\frac{2}{7}$	56	$\mathbf{y}_1$	46
E_7	$p \neq 2$	0	18	$\frac{7}{34}$	99	$\mathbf{y}_7$	79
E_7	$p = 2$	1	18	$\frac{7}{33}$	99	$\mathbf{y}_7$	79
E_8	$p \neq 2$	0	30	$\frac{4}{29}$	190	$\mathbf{y}_8$	134
E_8	$p = 2$	0	30	$\frac{4}{29}$	190	$\mathbf{y}_3$	136

Appendix B

MAGMA example

Here we show how to use MAGMA for one of the tasks needed in the proof of Proposition 4.24. Recall that this involved a finite dimensional Chevalley-type Lie algebra in positive characteristic. It was known that the dimension of the centraliser of a minimal nilpotent element was given by $m-2(h^\vee-1)$ (where m was the dimension of the Lie algebra and $h^\vee$ was the dual Coxeter number) and it was necessary to show that the maximal dimension of the centraliser of a non-zero semisimple element was not greater than this. This was checked manually by working out the maximal dimension of the centraliser of a semisimple element in all bad characteristics, over the corresponding prime field. We illustrate this on the example of E_6 in characteristic 3.
In this case we have $m = 78$ and $h^\vee = 12$, so $m - 2(h^\vee - 1) = 78 - 2 \cdot 11 = 56$.
We begin by defining the root datum and printing the Dynkin diagram and number of positive roots.

```
> R := RootDatum("E6");
> DynkinDiagram(R);

E6    1 - 3 - 4 - 5 - 6
              |
              2

> NumberOfPositiveRoots(R);

36
```

MAGMA has these 36 positive roots ordered, with the roots `Root(R, i)` for $i = 1 \ldots 6$ referring to the 6 fundamental roots. Note that MAGMA uses a different ordering to the one we choose in Appendix C. Next we define the fundamental coweights:

```
> L:= FundamentalCoweights(R);

[1 0 0 0 0 0]
[0 1 0 0 0 0]
[0 0 1 0 0 0]
[0 0 0 1 0 0]
[0 0 0 0 1 0]
[0 0 0 0 0 1]
```

This lists the fundamental coweights $\mathbf{y}_1, \ldots, \mathbf{y}_6$ as rows of a matrix. If we want to apply a particular coweight to a particular root we do the following:

```
> (Root(R, 36) ,  L[1] + L[3]);

3
```

This applies the coweight $\mathbf{y}_1 + \mathbf{y}_3$ to the 36th root in MAGMA's numbering, which corresponds to $\alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6$. The result is 3 and this number is viewed as a rational number, so to reduce it modulo 3 we need to coerce it into the field of 3 elements like so:

```
GF(3) ! (Root(R, 36) ,  L[1] + L[3]);

0
```

The fundamental coweights form a basis for the Cartan subalgebra, so a semisimple element is a linear combination of fundamental coweights. Now we can do the main loop of applying this to every positive root and every linear combination of fundamental coweights:

```
for a:= -1 to 1 do
  for b:= -1 to 1 do
   for c:= -1 to 1 do
    for d:= -1 to 1 do
     for e:= -1 to 1 do
      for f:= -1 to 1 do
       y:= 0;
        for i:= 1 to 36 do
        x:= GF(3) ! (Root(R, i) , a*L[1] + b*L[2] + c*L[3] + d*L[4] + e*L[5] +
f*L[6]); x;
         if x eq 0 then y:= y+1;
         else y:= y;
```

```
         end if;
        end for;
        y;
      end for;
     end for;
    end for;
   end for;
  end for;
 end for;
```

This produces a list of all the results of this calculation, each stored under the variable `x`. Removing the `x;` from the code, the only displayed value becomes `y`, which counts the number of 0's, i.e. for each mod-3-linear combination of fundamental coweights it counts the number of roots that annihilate it. The `for i:= 1 to 36 do` command by default assumes steps of size 1, so it produces 36 iterations.
The result of the code above with the `x;` produces a list with 3^6 entries. We would like to quickly find the maximal one. There is one entry of 36 (obtained by setting all the coefficients of the coweights to 0) so we would like to ignore this entry. The correct modification is:

```
z:= 0;
for a:= -1 to 1 do
  for b:= -1 to 1 do
   for c:= -1 to 1 do
    for d:= -1 to 1 do
     for e:= -1 to 1 do
      for f:= -1 to 1 do
       y:= 0;
        for i:= 1 to 36 do
        x:= GF(3) ! (Root(R, i) , a*L[1] + b*L[2] + c*L[3] + d*L[4] + e*L[5] +
f*L[6]);
         if x eq 0 then y:= y+1;
         else y:= y;
         end if;
        end for;
        y;
        if y ge z and y lt 36 then z:= y;
        else z:= z;
        end if;
      end for;
     end for;
```

```
    end for;
   end for;
  end for;
 end for;
z;
```

which displays the same long list plus `20` at the bottom. Removing the `y;` in each iteration displays only the final result, 20.

We would also like to find a specific instance of a semisimple element whose centraliser has this dimension. Trial and error shows that often at least one of the fundamental coweights has a centraliser of maximal dimension, so we attempt now with the fundamental coweight $\mathbf{y}_1$:

```
y:= 0;
for i:= 1 to 36 do
 x:= GF(3) ! (Root(R, i) , L[1]);
         if x eq 0 then y:= y+1;
         else y:= y;
         end if;
        end for;
        y;

20
```

This shows that $\mathbf{y}_1$ does indeed get annihilated by the maximum number of positive roots, 20, so it is a semisimple element whose centaliser has maximal dimension.

The element $\mathbf{y}_1$ gets annihilated by the corresponding negative roots as well, and by the elements in the Cartan subalgebra, so its centraliser has dimension $20+20+6 = 46 < 56$, which we record in Table A.6.

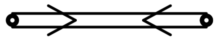
Appendix C

Affine Dynkin diagrams and GCMs

Here we include a list of the generalised Cartan matrices and Dynkin diagrams that we use. We include here only the ones of affine type. To obtain the ones of finite type, recall that for an extended generalised Cartan matrix $\widetilde{A}$ we can obtain the corresponding Cartan matrix A by deleting the 0-th row and column of $\widetilde{A}$, and we can obtain the Dynkin diagram of type X from the one of type $\widetilde{X}$ by deleting the vertex a_0 (and all edges connected to it).

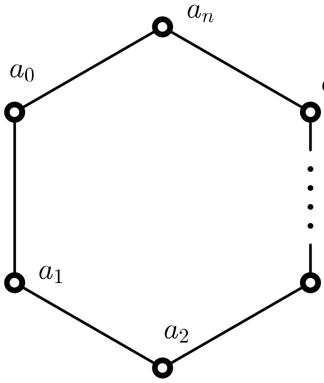
Untwisted types

$\widetilde{A}_1$



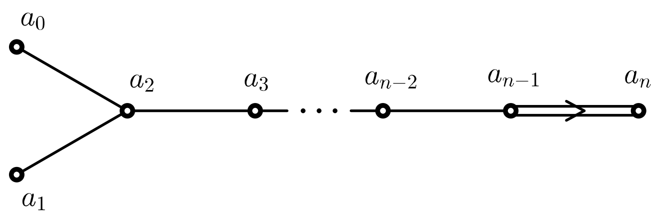
$$\begin{array}{c} 0 \\ 1 \end{array} \begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}$$

$\widetilde{A}_n, \quad n \geq 2$



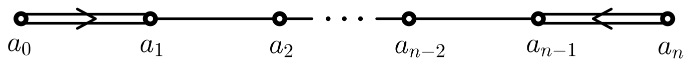
$$\begin{array}{r} 0 \\ 1 \\ 2 \\ . \\ . \\ . \\ n-2 \\ n-1 \\ n \end{array} \begin{pmatrix} 2 & -1 & & & & & & & -1 \\ -1 & 2 & -1 & & & & & & \\ & -1 & 2 & \cdot & & & & & \\ & & \cdot & \cdot & \cdot & & & & \\ & & & \cdot & \cdot & \cdot & & & \\ & & & & \cdot & \cdot & \cdot & & \\ & & & & & \cdot & 2 & -1 & \\ & & & & & & -1 & 2 & -1 \\ -1 & & & & & & & -1 & 2 \end{pmatrix}$$

$\widetilde{B}_n, \quad n \geq 3$



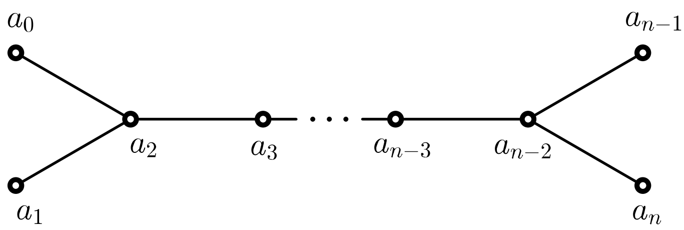
$$\begin{array}{r} 0 \\ 1 \\ 2 \\ 3 \\ \cdot \\ \cdot \\ n-2 \\ n-1 \\ n \end{array} \begin{pmatrix} 2 & & -1 & & & & & & \\ & 2 & -1 & & & & & & \\ -1 & -1 & 2 & -1 & & & & & \\ & & -1 & 2 & \cdot & & & & \\ & & & \cdot & \cdot & \cdot & & & \\ & & & & \cdot & \cdot & \cdot & & \\ & & & & & \cdot & 2 & -1 & \\ & & & & & & -1 & 2 & -1 \\ & & & & & & & -2 & 2 \end{pmatrix}$$

$\widetilde{C}_n, \quad n \geq 2$



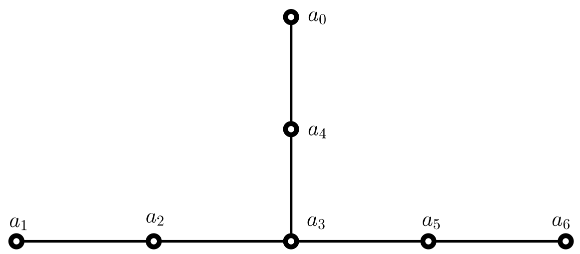
$$\begin{array}{r} 0 \\ 1 \\ 2 \\ \cdot \\ \cdot \\ \cdot \\ n-2 \\ n-1 \\ n \end{array} \begin{pmatrix} 2 & -1 & & & & & & & \\ -2 & 2 & -1 & & & & & & \\ & -1 & 2 & \cdot & & & & & \\ & & \cdot & \cdot & \cdot & & & & \\ & & & \cdot & \cdot & \cdot & & & \\ & & & & \cdot & \cdot & \cdot & & \\ & & & & & \cdot & 2 & -1 & \\ & & & & & & -1 & 2 & -2 \\ & & & & & & & -1 & 2 \end{pmatrix}$$

$\widetilde{D}_n, \quad n \geq 4$



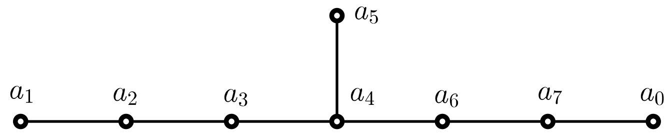
$$\begin{array}{r} 0 \\ 1 \\ 2 \\ 3 \\ \cdot \\ \cdot \\ \cdot \\ n-3 \\ n-2 \\ n-1 \\ n \end{array} \begin{pmatrix} 2 & & -1 & & & & & & & & \\ & 2 & -1 & & & & & & & & \\ -1 & -1 & 2 & -1 & & & & & & & \\ & & -1 & 2 & \cdot & & & & & & \\ & & & \cdot & \cdot & \cdot & & & & & \\ & & & & \cdot & \cdot & \cdot & & & & \\ & & & & & \cdot & \cdot & \cdot & & & \\ & & & & & & \cdot & 2 & -1 & & \\ & & & & & & & -1 & 2 & -1 & -1 \\ & & & & & & & & -1 & 2 & \\ & & & & & & & & -1 & & 2 \end{pmatrix}$$

$\widetilde{E}_6$



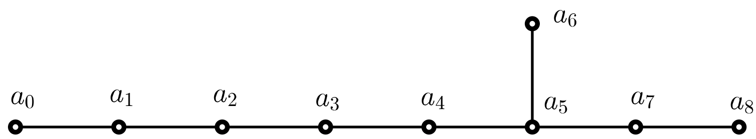
$$\begin{array}{r} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{pmatrix} 2 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & -1 & 0 \\ -1 & 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

$\widetilde{E}_7$



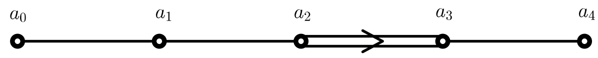
$$
\begin{array}{c}
0\\1\\2\\3\\4\\5\\6\\7
\end{array}
\begin{pmatrix}
2 & 0 & 0 & 0 & 0 & 0 & 0 & -1\\
0 & 2 & -1 & 0 & 0 & 0 & 0 & 0\\
0 & -1 & 2 & -1 & 0 & 0 & 0 & 0\\
0 & 0 & -1 & 2 & -1 & 0 & 0 & 0\\
0 & 0 & 0 & -1 & 2 & -1 & -1 & 0\\
0 & 0 & 0 & 0 & -1 & 2 & 0 & 0\\
0 & 0 & 0 & 0 & -1 & 0 & 2 & -1\\
-1 & 0 & 0 & 0 & 0 & 0 & -1 & 2
\end{pmatrix}
$$

$\widetilde{E}_8$



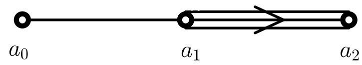
$$
\begin{array}{c}
0\\1\\2\\3\\4\\5\\6\\7\\8
\end{array}
\begin{pmatrix}
2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
-1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & -1 & 2 & -1 & -1 & 0\\
0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 2 & -1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2
\end{pmatrix}
$$

$\widetilde{F}_4$



$$\begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \quad \begin{pmatrix} 2 & -1 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & -2 & 2 & -1 \\ 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

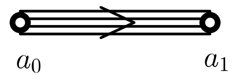
$\widetilde{G}_2$



$$\begin{array}{c} 0 \\ 1 \\ 2 \end{array} \quad \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -3 & 2 \end{pmatrix}$$

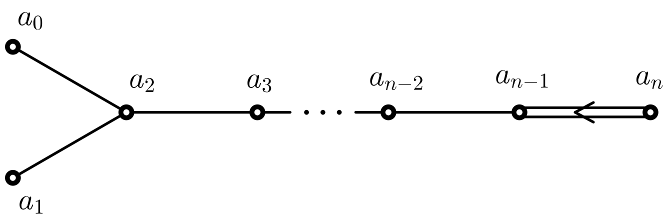
Twisted types

$\widetilde{A}_1'$



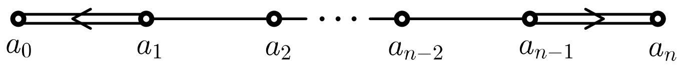
$$\begin{array}{c} 0 \\ 1 \end{array} \begin{pmatrix} 2 & -1 \\ -4 & 2 \end{pmatrix}$$

$\widetilde{B}_n^t, \quad n \geq 3$



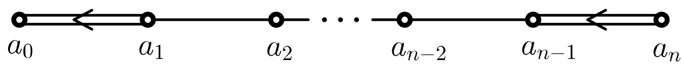
$$\begin{array}{r} 0 \\ 1 \\ 2 \\ 3 \\ \cdot \\ \cdot \\ n-2 \\ n-1 \\ n \end{array} \begin{pmatrix} 2 & & -1 & & & & & \\ & 2 & -1 & & & & & \\ -1 & -1 & 2 & -1 & & & & \\ & & -1 & 2 & \cdot & & & \\ & & & \cdot & \cdot\ \cdot & & & \\ & & & & \cdot\ \cdot & \cdot & & \\ & & & & \cdot & 2 & -1 & \\ & & & & & -1 & 2 & -2 \\ & & & & & & -1 & 2 \end{pmatrix}$$

$\widetilde{C}_n^t, \quad n \geq 2$



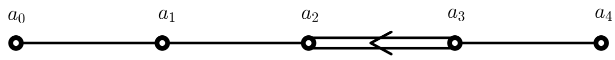
$$\begin{array}{r} 0 \\ 1 \\ 2 \\ \cdot \\ \cdot \\ \cdot \\ n-2 \\ n-1 \\ n \end{array} \begin{pmatrix} 2 & -2 & & & & & & & \\ -1 & 2 & -1 & & & & & & \\ & -1 & 2 & \cdot & & & & & \\ & & \cdot & \cdot & \cdot & & & & \\ & & & \cdot & \cdot & \cdot & & & \\ & & & & \cdot & \cdot & \cdot & & \\ & & & & & \cdot & 2 & -1 & \\ & & & & & & -1 & 2 & -1 \\ & & & & & & & -2 & 2 \end{pmatrix}$$

$\widetilde{C}_n', \quad n \geq 2$



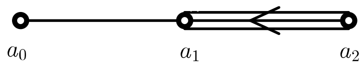
$$\begin{array}{r} 0 \\ 1 \\ 2 \\ \cdot \\ \cdot \\ \cdot \\ n-2 \\ n-1 \\ n \end{array} \begin{pmatrix} 2 & -2 & & & & & & & \\ -1 & 2 & -1 & & & & & & \\ & -1 & 2 & \cdot & & & & & \\ & & \cdot & \cdot & \cdot & & & & \\ & & & \cdot & \cdot & \cdot & & & \\ & & & & \cdot & \cdot & \cdot & & \\ & & & & & \cdot & 2 & -1 & \\ & & & & & & -1 & 2 & -2 \\ & & & & & & & -1 & 2 \end{pmatrix}$$

$\widetilde{F}_4^t$



$$\begin{array}{c c}
0 & \\
1 & \\
2 & \\
3 & \\
4 &
\end{array}
\begin{pmatrix}
2 & -1 & 0 & 0 & 0 \\
-1 & 2 & -1 & 0 & 0 \\
0 & -1 & 2 & -2 & 0 \\
0 & 0 & -1 & 2 & -1 \\
0 & 0 & 0 & -1 & 2
\end{pmatrix}$$

$\widetilde{G}_2^t$



$$\begin{array}{c c}
0 & \\
1 & \\
2 &
\end{array}
\begin{pmatrix}
2 & -1 & 0 \\
-1 & 2 & -3 \\
0 & -1 & 2
\end{pmatrix}$$

Bibliography

[A69] E. Abe, *Chevalley groups over local rings*, Tôhoku Math. J. **21** (1969), 474–494.

[AbNS03] M. Abért, N. Nikolov, B. Szegedy, *Congruence subgroup growth of arithmetic groups in positive characteristic*, Duke Math. J., **117** (2003), no. 2, 367–383.

[AbrM97] P. Abramenko, B. Mühlherr, *Presentations de certaines BN-paires jumelées comme sommes amalgamée*, C. R. Acad. Sci. Paris Ser. I Math. **325** (1997), 701–706.

[AsG84] M. Aschbacher, R. Guralnick. *Some applications of the first cohomology group*, J. Algebra, **90** (1984), 446–460.

[BG01] Y. Barnea, R. Guralnick, *Subgroup growth in some pro-p groups*, Proc. Amer. Math. Soc., **130** (2001), no. 3, 653–659.

[Bo68] N. Bourbaki, *Groupes et algèbres de Lie, Ch. IV–VI*, Hermann, Paris, 1968.

[C13] I. Capdeboscq, *Bounded presentations of Kac-Moody groups*, J. Group Theory, **16** (2013), 899–905.

[C15] I. Capdeboscq, *On the generation of discrete and topological Kac-Moody groups*, C. R. Math. Acad. Sci. Paris, **353** (2015), 695–699.

[CKR17] I. Capdeboscq, K. Kirkina, D. Rumynin, *Subgroup growth in some profinite Chevalley groups*, Proc. Amer. Math. Soc., **145** (2017), no. 10, 4187 – 4200.

[CKR17a] I. Capdeboscq, K. Kirkina, D. Rumynin, *Presentations of affine Kac-Moody groups*, preprint (2016), arXiv:1609.02464.

[CLRe16] I. Capdeboscq, A. Lubotzky, B. Rémy, *Presentations: from Kac-Moody groups to profinite and back*, Transformation Groups, **21** (2016), issue 4, 929 – 951.

[CRe] I. Capdeboscq, B. Rémy, *Generation of non-Archimedean reductive groups*, preprint.

[Ca07] P.-E. Caprace, *On 2-spherical Kac-Moody groups and their central extensions*, Forum Math., **19** (2007), 763–781.

[Car72] R. Carter, *Simple groups of Lie type*, John Wiley & Sons Ltd, London, 1972.

[Car92] R. Carter, *Kac-Moody groups and their automorphisms*, Groups, combinatorics and geometry (Durham, 1990), 218–228, LMS Lecture Note Ser., **165**, Cambridge Univ. Press, Cambridge, 1992.

[Car05] R. Carter, *Lie algebras of finite and affine type*, Cambridge Studies in Advanced Mathematics, **96**, Cambridge Univ. Press, Cambridge, 2005.

[CarCh93] R. Carter, Y. Chen, *Automorphisms of affine Kac-Moody groups and related Chevalley groups over rings*, J. Algebra **155** (1993), 44-94.

[Che55] C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. **7** (1) (1955), 14–66.

[D65] M. Demazure, *Schémes en groupes réductifs*, Bull. Soc. Math. France **93** (1965), 369–413.

[GKa00] R. Guralnick, W. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra **234** (2000), 743–792.

[GKaKasL07] R. Guralnick, W. Kantor, M. Kassabov and A. Lubotzky, *Presentations of finite simple groups: profinite and cohomological approaches*, Groups Geom. Dyn. **1** (2007), 469–523.

[GKaKasL08] R. Guralnick, W. Kantor, M. Kassabov and A. Lubotzky, *Presentations of finite simple groups: A quantitative approach*, J. Amer. Math. Soc. **21** (2008), 711–774.

[GKaKasL11] R. Guralnick, W. Kantor, M. Kassabov and A. Lubotzky, *Presentations of finite simple groups: A computational approach*, J. Eur. Math. Soc., **13** (2011), 391–458.

[H95] J. Humphreys, *Conjugacy Classes in Semisimple Algebraic Groups*, Math. Surveys and Monographs, v.43, Amer. Math. Soc., Providence, 1995.

[J97] D.L. Johnson, *Presentations of Groups*, 2nd ed., LMS Student Texts 15, Cambridge University Press, 1997.

[KaL90] W. Kantor, A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata, **36** (1990), 67–87.

[Kac83] V. Kac, *Infinite-Dimensional Lie-Algebras*, Progress in Mathematics v. 44, Birkhäuser, 1983.

[KacW76] V. Kac, B. Weisfeiler, *Coadjoint action of a semi-simple algebraic group and the center of the enveloping algebra in characteristic p*, Indag. Math., **38** (1976), no. 2, 136–151.

[Kl07] B. Klopsch, *Five lectures on analytic pro-p groups: a meeting-ground between finite p-groups and Lie theory*, Lecture notes, 2007/2008, available at time of writing at `http://reh.math.uni-duesseldorf.de/~klopsch/mathematics/Manuskripte/analytic_groups.pdf`.

[LMa91] A. Lubotzky, A. Mann, *On groups of polynomial subgroup growth*, Invent. Math, **104** (1991), no. 3, 521–533 .

[LSh94] A. Lubotzky, A. Shalev, *On some Λ-analytic pro-p groups*, Israel J. Math., **85** (1994), no. 1–3, 307–337.

[LSe03] A. Lubotzky, D. Segal, *Subgroup growth*, Progress in Mathematics, vol. 212, Birkhäuser, Basel, 2003.

[MarT13] A. Maróti, M. Tamburini Bellani, *A solution to a problem of Wiegold*, Comm. Algebra, **41** (2013), 34–49.

[MoReh91] J. Morita, U. Rehmann, *Symplectic K2 of Laurent polynomials, associated Kac-Moody groups and Witt rings*, Math. Z. **206** (1991), 57–66.

[PVa96] E. Plotkin, N. Vavilov, *Chevalley groups over commutative rings: I. Elementary calculations*, Acta Applicandae Math, **45** (1996) 73–113, Kluwer Academic Publishers.

[Pr95] A. Premet, *An analogue of the Jacobson-Morozov theorem for Lie algebras of reductive groups of good characteristic*, Trans. Amer. Math. Soc., **347** (1995), no. 8, 29612988.

[Ra92] J. Rammage, *On Some Twisted Kac-Moody Groups*, doctoral thesis, University of Warwick, 1992.

[Sh92] A. Shalev, *Growth functions, p-adic analytic groups, and groups of finite coclass*, J. London Math. Soc., **46** (1992), no. 1, 111–122.

[St62] R. Steinberg, *Generators for simple groups*, Canad. J. Math, **14** (1962), 277–283.

[St68] R. Steinberg, *Lectures on Chevalley groups*, mimeographed lecture notes, Yale Univ. Math. Dept. 1968.

[Ti87] J. Tits, *Uniqueness and presentation of Kac-Moody groups over fields*, Journal of Algebra **105** (1987), 542–573.

[Vi05] University of Georgia VIGRE Algebra Group, *Varieties of nilpotent elements for simple Lie algebras II: Bad primes*, J. Algebra, **292** (2005), no. 1, 65–99.

[Wa99] W. Wang, *Dimension of a minimal nilpotent orbit*, Proc. Amer. Math. Soc., **127** (1999), no. 3, 935–936.