HAL open science

Presentations: from Kac-Moody groups to profinite and back

Inna Capdeboscq, Alexander Lubotzky, Bertrand Rémy

To cite this version:

Inna Capdeboscq, Alexander Lubotzky, Bertrand Rémy. Presentations: from Kac-Moody groups to profinite and back. 2015. hal-01182768v4

HAL Id: hal-01182768

https://hal.science/hal-01182768v4

Preprint submitted on 29 Jul 2016 (v4), last revised 29 Aug 2016 (v5)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Presentations: from Kac-Moody groups to profinite and back

Inna Capdeboscq, Alexander Lubotzky and Bertrand Rémy

July 29, 2016

Abstract: We go back and forth between, on the one hand, presentations of arithmetic and Kac-Moody groups and, on the other hand, presentations of profinite groups, deducing along the way new results on both.

Keywords: arithmetic and profinite groups, bounded presentation, low-dimensional cohomology.

AMS classification (2000): 11F06, 17B22, 20E32, 20F20, 20G44, 20H05, 22E40, 51E24.

Introduction

In recent years several papers have been dedicated to showing that finite simple groups or arithmetic groups have presentations with bounded number of generators and relations [KL06], [GKKL07], [GKKL08], [GKKL11], [Cap13]. This paper is about such quantitative results for some classes of profinite groups.

More precisely, we will give essentially optimal bounds on the size of the presentations of maximal compact subgroups and of maximal pro-p subgroups of simple Chevalley groups over local fields. These results can be also expressed as bounds on 2-cohomology groups – see below.

Let $\mathbf{G}$ be a simple, simply connected, Chevalley group scheme of Lie rank l and let q be a power p^a for some prime p and some exponent $a \geqslant 1$. The non-Archimedean Lie group $\mathbf{G}\big(\mathbf{F}_q(\!(t)\!)\big)$ acts simplicially on its Bruhat-Tits building [Tit79]. In this action, each facet stabilizer is an extension of a finite group of Lie type by a pro-p group. Combining this with a non-positive curvature argument implies that maximal pro-p subgroups in $\mathbf{G}\big(\mathbf{F}_q(\!(t)\!)\big)$ are all conjugate to one another [Rém04, 1.C.2] (while this is not the case for maximal compact subgroups); we henceforth call *pro-p Sylow subgroup* a maximal pro-p subgroup of $\mathbf{G}\big(\mathbf{F}_q(\!(t)\!)\big)$. If P is such a subgroup then, up to conjugating it, we can assume that we have $P < \mathbf{G}(\mathbf{F}_q[[t]]) < \mathbf{G}\big(\mathbf{F}_q(\!(t)\!)\big)$. The group $\mathbf{G}(\mathbf{F}_q[[t]])$ is a *special* maximal compact subgroup.

Theorem 0.1. *There exists a constant $C > 0$ such that for any simple, simply connected, Chevalley group $\mathbf{G}$ of rank $\geqslant 2$ and for any prime power $q = p^a \geqslant 4$, the group $G = \mathbf{G}(\mathbf{F}_q[[t]])$ admits a profinite presentation $\Sigma(G)$, with $D_{\Sigma(G)}$ generators and $R_{\Sigma(G)}$ relations, satisfying*

$$D_{\Sigma(G)} + R_{\Sigma(G)} \leqslant C.$$

For a group X, let $d(X)$ (respectively $r(X)$) denote the minimal number of generators (respectively relations) of X in any of its profinite or discrete presentation (depending on whether X is a profinite or a discrete group). Then Theorem 0.1 implies that in particular

$$d(G) + r(G) \leqslant C.$$

Theorem 0.1 is proved by combining the results of [Cap13] on bounded presentations of the discrete Kay-Moody group $\mathbf{G}(\mathbf{F}_q[t, t^{-1}])$, with the fact that it has the congruence subgroup property. It is important at this point to note that the above uniformness statement is *not* true globally, that is for abstract presentations of arithmetic groups obtained by replacing the local rings $\mathbf{F}_q[[t]]$ by rings of integers of global fields (see §3 below).

Now, P as above is a subgroup of index $q^{O(l^2)}$ of $\mathbf{G}(\mathbf{F}_q[[t]])$, from which one deduces, using the Reidemeister-Schreier theorem, that P has a presentation $\Sigma(P)$ satisfying

$$D_{\Sigma(P)} + R_{\Sigma(P)} \leqslant q^{O(l^2)}.$$

By different methods, we obtain a presentation of the pro-p group P with much better bounds. A word of explanation is needed here. Let $r_p(P)$ be the minimal number of relations needed to define P as a pro-p group. In [Lub01, Corollary 5.5] it is shown that we have:

$$r(P) = \max\{d(P), r_p(P)\}.$$

Theorem 0.2. *Let $\mathbf{G}$ be a simple, simply connected, Chevalley group scheme of rank l. Let P be a Sylow pro-p-subgroup of $G = \mathbf{G}\big(\mathbf{F}_q(\!(t)\!)\big)$ where $q = p^a$. Then at least for $l \geqslant 3$ and*

$q \geqslant 16$, we obtain that $d(P) = a(l+1)$, so in particular $d(P)$ is linear in a and in l. On the other hand, $r_p(P) = r(P)$ is bounded from below and from above by polynomials of degree 2 in a and in l; these polynomials do not depend on p.

The precise formula on the number of generators is deduced from the Kac-Moody theory [CR14, Corollary 2.5]. The lower bound on the number of relations is derived from the Golod-Shafarevich inequality while the upper bound is again deduced from the theory of Kac-Moody groups. More precisely, a discrete Kac-Moody group Γ_0 is chosen carefully so that P is equal to the pro-p completion of a well-understood subgroup Γ of Γ_0. The presentation of Γ in the discrete category serves also as a presentation for P in the pro-p category.

The method of the proof enables us to go also backward and to deduce from the Golod-Shafarevich inequality that the stated presentation of Γ is essentially optimal (see Corollary 2.9).

Recall that for a profinite group the number of relations is expressed by the dimensions of the 2nd cohomology groups of various modules [Lub01, Corollary 5.5, 5.6]. It gets a particular nice form for a pro-p group P, where $r_p(P) = \dim_{\mathbf{Z}/p\mathbf{Z}} \mathrm{H}^2(P, \mathbf{Z}/p\mathbf{Z})$. Thus combining Theorems 0.1 and 0.2 we obtain

Corollary 0.3. *Let $\mathbf{G}$ be a simple, simply connected, Chevalley group scheme of rank l. Let P be a Sylow pro-p-subgroup in $G = \mathbf{G}\big(\mathbf{F}_q[[t]]\big)$ with $q = p^a$. Then the following conditions hold:*

1. *If $l \geqslant 2$ and $q \geqslant 4$, then $\dim_{\mathbf{F}_s} \mathrm{H}^2(G, M) \leqslant C \cdot \dim_{\mathbf{F}_s} M$ for every simple $\mathbf{F}_s[G]$-module M and every prime s.*

2. *If $l \geqslant 3$ and $q \geqslant 16$, then $\dim_{\mathbf{Z}/p\mathbf{Z}} \mathrm{H}^2(P, \mathbf{Z}/p\mathbf{Z})$ is bounded from below and from above by polynomials of degree 2 in a and in l; these polynomials do not depend on p.*

Theorems 0.1 and 0.2 suggest that similar results are valid also in characteristic 0, but our methods are not that efficient there (see §3). There are two main differences between the characteristic zero case and the positive characteristic case.

The first one is that in characteristic p *all* local fields are obtained as completions of *one* global field $\mathbf{F}_p(t)$, while in characteristic 0, there is no such global field. In our method of proof, which goes from global to local, this difference is crucial: we prove a uniform result for all groups defined over a given global field k (Theorem 3.1), but there is no uniform result over all global fields (see Remark 3.4). Our uniform result for local fields in characteristic p uses substantially the fact that they all are completions of one global field.

Secondly, the pro-p Sylow subgroup of $\mathbf{G}\big(\mathbf{F}_q(\!(t)\!)\big)$ is the pro-p completion of a suitable subgroup of a Kac-Moody group (see Lemma 2.1 below for the exact result) and we are making a crucial use of this fact. No such result is known to us in characteristic 0.

Still one has good reasons to believe that results like Theorem 0.1 and Theorem 0.2 are valid also in characteristic 0. In Section 3, we sketch few partial results in this direction.

The structure of the paper is as follows. Section 1 deals with uniformly bounded profinite presentations of maximal compact subgroups of non-archimedean Chevalley groups in characteristic p. Section 2 investigates more carefully the maximal pro-p subgroups of these groups. Section 3 goes back to the questions of §1 in the characteristic 0 case. The proof for the global case is given in §4 and uses K-theory.

1 Presentations of $\mathbf{F}_q[[t]]$-points of split simple groups

Let $q = p^a$ with p a prime and $a \geqslant 1$. Let $\mathbf{G}$ be a simple, simply connected, Chevalley group. In this section we are interested in controlling presentations of the virtually pro-p groups $\mathbf{G}(\mathbf{F}_{q^e}[[t]])$ for arbitrary exponent $e \geqslant 1$. The general idea of this section is that $\mathbf{G}(\mathbf{F}_{q^e}[[t]])$ appears as a factor of the profinite completion of $\mathbf{G}(\mathbf{F}_q[t, t^{-1}])$ and that a presentation of the latter discrete group naturally gives a profinite presentation of this completion.

Therefore, in the first half of the argument we are only interested in $\mathbf{G}(\mathbf{F}_q[t, t^{-1}])$. Usually, the main viewpoint on the group $\mathbf{G}(\mathbf{F}_q[t, t^{-1}])$ is as an S-arithmetic group [Mar91]. It provides a lot of information (cf. [PR94]), but another possibility is to see it as a (split) Kac-Moody group of affine type. This gives additional information of combinatorial nature. Indeed, this group acts on a product of two twin buildings [Rém02, 12.6.3] and using the action on a single building, we can deduce from this a suitable amalgamation theorem for $\mathbf{G}(\mathbf{F}_q[t, t^{-1}])$. We use here a combination of the two viewpoints.

1.1 Bounded presentation for affine Kac-Moody groups over finite fields

To begin with, let us recall that by [Cap13, Theorem 2.1] there exists a so-called *bounded* family of presentations for affine Kac-Moody groups (with the exception of $\widetilde{A}_1$ and ${}^*\widetilde{A}_1$). In particular, we have:

Theorem 1.1 ([Cap13])**.** *There exists a constant $C > 0$ such that for any simple, simply connected, Chevalley group scheme $\mathbf{G}$ of rank $\geqslant 2$ and for any prime power $q \geqslant 4$, the group $G = \mathbf{G}(\mathbf{F}_q[t, t^{-1}])$ admits a presentation $\Sigma(G)$ with $D_{\Sigma(G)}$ generators and $R_{\Sigma(G)}$ relations satisfying*

$$D_{\Sigma(G)} + R_{\Sigma(G)} \leqslant C.$$

1.2 Bounded presentation for profinite Chevalley groups in characteristic p

We can now turn to completion processes. The following proposition provides a relationship between presentations of $\mathbf{G}(\mathbf{F}_q[t, t^{-1}])$ and of $\mathbf{G}(\mathbf{F}_q[[t]])$; it is a quantitative version of a method already used in [Lub05].

Proposition 1.2. *Assume that the rank of the simple, simply connected, Chevalley group $\mathbf{G}$ is $\geqslant 2$ and that the arithmetic group $\mathbf{G}(\mathbf{F}_q[t, t^{-1}])$ has a presentation with d generators and r relations. Then for any $e \geqslant 1$, the group $\mathbf{G}(\mathbf{F}_{q^e}[[t]])$ has a profinite presentation with d generators and $r + 1$ relations.*

Proof. Set $A = \mathbf{F}_q[t, t^{-1}]$ and denote by $\widehat{A}$ the profinite completion of this ring. Let $\mathcal{P}$ be the set of monic irreducible polynomials in $\mathbf{F}_q[t]$ and $\mathcal{P}_e$ those of degree e. The prime ideals in $A = \mathbf{F}_q[t][\frac{1}{t}]$ are parametrized by $\mathcal{P} \setminus \{t\}$, so by the Chinese remainder theorem, we have

$$\widehat{A} \cong \prod_{f \in \mathcal{P} \setminus \{t\}} \widehat{A}^f$$

where $\widehat{A}^f = \varprojlim_{n \geqslant 1} A/(f^n)$ is isomorphic to $\mathbf{F}_{q^{\deg(f)}}[[x]]$. Using $\mathcal{P} = \bigsqcup_{e \geqslant 1} \mathcal{P}_e$, we see therefore that

$$\widehat{A} \cong (\mathbf{F}_q[[t]])^{q-1} \times \prod_{e \geqslant 2} (\mathbf{F}_{q^e}[[t]])^{\#\mathcal{P}_e}.$$

We set $S = \{0; \infty\}$. The group $\mathbf{G}(A)$ is thus an S-arithmetic group. We denote by $\widehat{\mathbf{G}(A)}$ its profinite completion and by $\overline{\mathbf{G}(A)}$ its S-congruence completion. The canonical map

$\pi : \widehat{\mathbf{G}(A)} \to \overline{\mathbf{G}(A)}$ is a continuous group homomorphism restricting to the identity map of the dense subgroup $\mathbf{G}(A)$; as a consequence, π is surjective. Since there is no place of $\mathbf{F}_q(t)$ at which $\mathbf{G}$ is anisotropic and since $\mathbf{G}$ is simply connected, strong approximation [Pra77] implies that the S-congruence completion $\overline{\mathbf{G}(A)}$ is described by means of the S-adèles $\mathbf{A}_S$ of $\mathbf{F}_q(t)$. One therefore deduces:

$$\overline{\mathbf{G}(A)} \cong \mathbf{G}(\widehat{A}) \cong \mathbf{G}(\mathbf{F}_q[[t]])^{q-1} \times \prod_{e \geqslant 2} \mathbf{G}(\mathbf{F}_{q^e}[[t]])^{\#\mathcal{P}_e}.$$

For further use in the paper, let us quote a precise statement on the solution to the congruence subgroup problem (see [Rag76], [PR83] and [Mar91, VIII.2.16 Theorem]).

Theorem 1.3. *Let $\mathbf{G}$ be a simply connected Chevalley group, let k be a global field and let S be a finite set of places of k. Let A denote the ring of S-integers in k and for each $v \in S$, let k_v be the corresponding completion of k. We set $\mathrm{rk}_S(\mathbf{G}) = \sum_{v \in S} \mathrm{rk}_{k_v}(\mathbf{G})$ and assume that $\mathrm{rk}_S(\mathbf{G}) \geqslant 2$. Then the kernel of the map $\pi : \widehat{\mathbf{G}(A)} \to \overline{\mathbf{G}(A)}$ is cyclic; it is even trivial whenever S contains a non-Archimedean place.*

In our case, where G has rank $\geqslant 2$ and all places are non-Archimedean, the map π is an isomorphism : $\widehat{\mathbf{G}(A)} \cong \mathbf{G}(\widehat{A})$. This implies that for any fixed $e \geqslant 1$, one can write $\widehat{\mathbf{G}(A)}$ as a product:

$$\widehat{\mathbf{G}(A)} = \mathbf{G}(\mathbf{F}_{q^e}[[t]]) \times M$$

where M is a product of infinitely many groups of the form $\mathbf{G}(\mathbf{F}_{q^s}[[t]])$ with finite multiplicity for each exponent $s \geqslant 1$.

By our group-theoretic hypothesis, the abstract group $\mathbf{G}(A)$ has a presentation with d generators and r relations, therefore so does $\widehat{\mathbf{G}(A)}$ as a profinite group. Now, notice that M, as a normal subgroup of $\widehat{\mathbf{G}(A)}$, is generated by one element! Indeed, every factor of the direct product M, say $\mathbf{G}(\mathbf{F}_{q^s}[[t]])$, has no non-trivial abelian quotient; moreover it admits a semi-direct product decomposition $\mathbf{G}(\mathbf{F}_{q^s}) \ltimes Q$ where Q is a pro-p group [RR06, 1.C]. The semi-direct product decomposition implies that $\mathbf{G}(\mathbf{F}_{q^s}[[t]])$ has a unique maximal normal subgroup. Indeed, let $\pi : \mathbf{G}(\mathbf{F}_{q^s}[[t]]) \to S$ be a quotient map to a simple (necessarily non-abelian) group. The group Q is normal in $\mathbf{G}(\mathbf{F}_{q^s}[[t]])$, therefore $\pi(Q)$ is a normal p-group in S, hence is trivial. This implies that π factorizes through the homomorphism $\mathbf{G}(\mathbf{F}_{q^s}[[t]]) \to \mathbf{G}(\mathbf{F}_{q^s})$, whose target group has a unique simple quotient.

Pick then $g \in M$ such that each one of its coordinates is outside that maximal normal subgroup; it is not difficult to see that the normal closure $\langle\langle g \rangle\rangle_M$ of g in M is M itself. Thus we get a profinite presentation for $\mathbf{G}(\mathbf{F}_{q^e}[[t]]) = \dfrac{\widehat{\mathbf{G}(A)}}{\{1\} \times \langle\langle g \rangle\rangle_M}$ which has d generators and $r+1$ relations. □

Proof of Theorem 0.1. This statement is now a consequence of the combination of Theorem 1.1 and Proposition 1.2. □

Remark 1.4. *In Theorem 0.1 we assume that $l \geqslant 2$. We believe it is also true for $l = 1$, i.e., for $\mathrm{SL}_2(\mathbf{F}_q[[t]])$.*

2 Sylow pro-p-subgroups of Chevalley groups over $\mathbf{F}_q(\!(t)\!)$

The other type of compact subgroups we consider in this paper is given by the maximal pro-p subgroups of $\mathbf{G}\big(\mathbf{F}_q(\!(t)\!)\big)$. To prove Theorem 0.2 we will use again Kac-Moody theory, but in a different way than in Theorem 0.1.

The idea is to see the pro-p group we are interested in as the full pro-p completion of a suitable arithmetic group, which can itself be seen as a subgroup of a Kac-Moody group over a finite field. Again we use the fact that a presentation for a discrete group naturally leads to a profinite or pro-p presentation of the corresponding completion.

2.1 The pro-p completions

Let $q = p^a$ ($a \geqslant 1$) and $\mathbf{G}$ be a simple simply connected Chevalley group scheme of rank $l \geqslant 3$. Take $A = \mathbf{F}_q[t]$ and consider $\Gamma_0 := \mathbf{G}(A)$. Suppose further that $I = (f(t))$ is an ideal of A generated by an irreducible polynomial $f(t)$ and B is the completion of A with respect to I. Let P be a pro-p-Sylow subgroup of $\mathbf{G}(B)$. Then P is an open maximal pro-p subgroup of $\mathbf{G}(B)$. Now consider a very special case: $f(t) = t$, so $B \cong \mathbf{F}_q[[t]]$. Set $\Gamma = \Gamma_0 \cap P = \mathbf{G}(A) \cap P$.

Lemma 2.1. *The group P is the pro-p completion of Γ.*

Proof. By the affirmative solution of the CSP (the congruence subgroup problem) for Γ_0 (see Theorem 1.3), its profinite completion $\widehat{\mathbf{G}(A)}$ is equal to $\prod_Y \mathbf{G}(Y)$, where Y runs over all the completions of A (one of which is B). As Γ is of finite index in Γ_0, the profinite completion of Γ can be easily read from that of Γ_0: $\widehat{\Gamma} = \prod_{Y \neq B} \mathbf{G}(Y) \times P$ when this time Y runs over all of the completions of A except for B. The completion B contributes the factor P. Now, the pro-p completion of a group is equal (by abstract nonsense) to the maximal pro-p quotient of its profinite completion. But for $Y \neq B$, the group $\mathbf{G}(Y)$ has no non-trivial p-quotients and so the maximal pro-p quotient of $\widehat{\Gamma}$ is only P. This finishes the proof. $\square$

In what follows, we sum up the lemma by writing $P = \Gamma_{\hat{p}}$ (i.e. $\Gamma_{\hat{p}}$ henceforth denotes the pro-p completion of a discrete group Γ).

2.2 Presentations of Sylow p-subgroups of $\mathrm{SL}_3(\mathbf{F}_q)$ and $\mathrm{Sp}_4(\mathbf{F}_q)$

As a preparation for proving Theorem 0.2, we will now produce presentations of Sylow p-subgroups of $\mathrm{SL}_3(\mathbf{F}_q)$ (i.e., $A_2(q)$) and $\mathrm{Sp}_4(\mathbf{F}_q)$ (i.e., $C_2(q)$), with $q = p^a$. We single out these p-groups because, as we will see in the next section, they will turn out to be building blocks of Γ from Lemma 2.1.

Notation : For a group H and any $a, b \in H$, denote $[a, b] := aba^{-1}b^{-1}$ and $a^b := bab^{-1}$.

In what follows we will need the following well known result attributed to P. Hall.

Lemma 2.2. *Let G be a group that is an extension of H by N*

$$1 \to N \to G \to H \to 1.$$

Suppose that N has a finite presentation $N = \langle n_1, ..., n_r \mid R_1(n_1, ..., n_r), ..., R_k(n_1, ..., n_r)\rangle$ and H has a finite presentation $H = \langle h_1, ..., h_s \mid W_1(h_1, ..., h_s), ..., W_l(h_1, ..., h_s)\rangle$. Then G

has the following finite presentation

$$G = \langle n_1, ..., n_r, g_1, ..., g_s \mid R_1(n_1, ...n_r), ..., R_k(n_1, ..., n_r), g_i n_j g_i^{-1} = V_{ij}(n_1, ..., n_r),$$

$$g_i^{-1} n_j g_i = U_{ij}(n_1, ..., n_r), 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant r, W_i(g_1, ..., g_s) = \widetilde{W}_i(n_1, ..., n_r), 1 \leqslant i \leqslant l\rangle$$

where $\pi(g_i) = h_i$, $1 \leqslant i \leqslant s$, *for the natural projection* $\pi : G \to H$ *and relations* U_{ij}, V_{ij} *and* $\widetilde{W}_i$ *are the obvious suspects.*

The next statement is Theorem 2 of [BD01].

Lemma 2.3. *Let* S *be a Sylow* p*-subgroup of the finite group* $\mathrm{SL}_3(\mathbf{F}_q)$ *where* $q = p^a$ *for* $a \geqslant 1$. *Then* $|S| = q^3 = p^{3a}$, *the minimal number of generators of* S *is* $2a$, *and* S *has the following presentation on* $2a$ *generators and with* $2a(a+1)$ *relations.*

There are elements $s_1(v_k), s_2(v_k) \in S$, $1 \leqslant k \leqslant a$, *that generate* S *and are subject to the following relations:*

(A1) $(s_i(v_k))^p = 1$ *for* $i = 1, 2$ *and* $1 \leqslant k \leqslant a$,

(A2) $[s_i(v_k), s_i(v_{k'})] = 1$ *for* $i = 1, 2$ *and* $1 \leqslant k < k' \leqslant a$,

(A3) $[s_1(v_1), [s_1(v_k), s_2(v_1)]] = [s_2(v_1), [s_1(v_k), s_2(v_1)]] = 1$ *for* $1 \leqslant k \leqslant a$,

(A4) $[s_1(v_k)^{-1}, s_2(v_{k'})^{-1}] = \prod_{1 \leqslant r \leqslant a} [s_1(v_r), s_2(v_1)]^{c(k,k',r)}$ *with some fixed* $c(k, k', 1), \ldots, c(k, k', a) \in \mathbf{Z}$, *for* $1 \leqslant k \leqslant a$ *and* $2 \leqslant k' \leqslant a$.

Proof. This is the proof of Theorem 2 of [BD01]. □

Remark that for odd p, the presentation of S given above has not only minimal number of generators, but also minimal number of relations [BD01, Theorem 3].

Notice that under a natural identification of S with the unipotent radical of the standard Borel subgroup of $\mathrm{SL}_3(\mathbf{F}_q)$ (where the simple roots of A_2 are denoted by α_1 and α_2), we may choose $s_1(v_k)$ and $s_2(v_k)$ to correspond to $x_{\alpha_1}(v_k)$ and $x_{\alpha_2}(v_k)$, $1 \leqslant k \leqslant a$, where $v_1, \ldots, v_a$ are chosen to be some generators of $\mathbf{F}_q$, with $v_1 = 1$.

2.2.1 Sylow p-subgroup of $\mathrm{Sp}_4(\mathbf{F}_q)$

We will now discuss presentations of Sylow p-subgroup of $\mathrm{Sp}_4(\mathbf{F}_q)$, $q = p^a$, $a \geq 1$. For our purposes either p is odd, or $p = 2$ and $q \geq 16$. Let S be a Sylow p-subgroup of $\mathrm{Sp}_4(\mathbf{F}_q)$.

On the one hand, as $\mathrm{Sp}_4(\mathbf{F}_q)$ is identified with the universal version of the group $C_2(q)$, it has a natural Steinberg presentation [GLS98, Theorem 1.12.1] and thus so does S. Unfortunately, this presentation of S has $4(q-1)$ generators and $16(q-1)^2$ relations.

On the other hand, as either $p \geqslant 3$, or $p = 2$ and $q \geq 16$, [GLS98, Th. 3.3.1] (together with some additional calculations in the case when $p = 2$) implies that in fact S has a minimal set of generators $\{x_\alpha(v_i), x_\beta(v_i) \mid 1 \leqslant i \leqslant a\}$ where $v_1 = 1$ and v_i $(2 \leqslant i \leqslant a)$ generate $\mathbf{F}_q$ (here α and β are simple roots of C_2, with α being a short root and β a long one). In particular, S is a group of order $q^4 = p^{4a}$ with $d(S) = 2a$. We may now apply [LSe03, Prop. 3.4.1] to conclude that S has a presentation with $2a$ generators and $8a^2$ relations.

However shorter presentations of S exist and would give more precise estimates for us. The reader who is not concerned with this difference is welcome to skip the rest of this subsection. We will now produce a presentation of S (in the case when p is odd) on $2a$ generators and

with $\frac{7a^2+13a}{2}$ relations. Using this technique, one can also produce a shorter presentation in the case when $p = 2$. However, the calculation is lengthy, and we decided to demonstrate how it can be done (and get a good estimate) only for $p \geq 3$. The difference in those two cases happens because of the redundancies in the commutator relations for $p = 2$.

Lemma 2.4. *Let S be a Sylow p-subgroup of the finite group $\mathrm{Sp}_4(\mathbf{F}_q)$ where $q = p^a$ for $a \geqslant 1$ and p is odd. Then $|S| = q^4 = p^{4a}$, the minimal number of generators of S is $2a$, and S has the following presentation on $2a$ generators and with $\frac{7a^2+13a}{2}$ relations.*

There are elements $x_\alpha(v_k), x_\beta(v_k) \in S$, $1 \leqslant k \leqslant a$, that generate S. For $1 \leq i \leq a$, set

$$x_{\alpha+\beta}(v_i) = [x_\beta(v_1), x_\alpha(v_i)] \prod_{k=1}^{a} [x_\alpha(\frac{1}{2}v_k), [x_\beta(v_1), x_\alpha(v_1)]]^{r_k}$$

$$\text{and} \quad x_{2\alpha+\beta}(v_i) = [x_\alpha(\frac{1}{2}v_i), x_{\alpha+\beta}(v_1)]$$

where for each i, the element $x_\alpha(\frac{1}{2}v_i) = \Pi_{j=1}^{a} x_\alpha(v_j)^{m(j,i)}$ with some $m(j,i) \in \mathbf{Z}$, $1 \leqslant j \leqslant a$.

Then S has a presentation with the generators $x_\alpha(v_k), x_\beta(v_k) \in S$, $1 \leqslant k \leqslant a$, and the following relations:

(C1) $(x_\alpha(v_k))^p = 1$, $(x_\beta(v_k))^p = 1$ *and* $(x_{\alpha+\beta}(v_k))^p = 1$ *for* $1 \leqslant k \leqslant a$,

(C2) $[x_\alpha(v_k), x_\alpha(v_{k'})] = 1$ *for* $1 \leqslant k < k' \leqslant a$,

(C3) $[x_\beta(v_k), x_\beta(v_{k'})] = 1$ *for* $1 \leqslant k < k' \leqslant a$,

(C4) $[x_{\alpha+\beta}(v_k), x_{\alpha+\beta}(v_{k'})] = 1$ *for* $1 \leqslant k < k' \leqslant a$,

(C5) $[x_\alpha(v_1), [x_\alpha(v_k), x_{\alpha+\beta}(v_1)]] = [x_{\alpha+\beta}(v_1), [x_\alpha(v_k), x_{\alpha+\beta}(v_1)]] = 1$ *for* $1 \leqslant k \leqslant a$,

(C6) $[x_\alpha(v_k)^{-1}, x_{\alpha+\beta}(v_{k'})^{-1}] = \prod_{1 \leqslant r \leqslant a} [x_\alpha(v_r), x_{\alpha+\beta}(v_1)]^{c(k,k',r)}$ *with some fixed* $c(k,k',1), \ldots, c(k,k',a) \in \mathbf{Z}$, *for* $1 \leqslant k \leqslant a$ *and* $2 \leqslant k' \leqslant a$.

(C7) $[x_{\alpha+\beta}(v_1), x_\beta(v_i)] = 1$ *for* $1 \leqslant i \leqslant a$,

(C8) $[x_{\alpha+\beta}(v_i), x_\beta(v_1)] = 1$ *for* $1 \leqslant i \leqslant a$,

(C9) $x_{2\alpha+\beta}(v_i^2)^{-1} = \Pi_{k=1}^{a} x_{2\alpha+\beta}(v_k)^{r_k}$ *for all* $1 \leqslant i \leqslant a$ *where* $r_k \in \mathbf{Z}$,

(C10) $[x_\beta(v_1), x_\alpha(v_i)] = x_{\alpha+\beta}(v_i) x_{2\alpha+\beta}(v_i^2)$ *for* $1 \leqslant i \leqslant a$.

(C11) $[x_\alpha(v_j)^{-1}, x_\beta(v_i)^{-1}] = x_{\alpha+\beta}(v_i v_j) x_{2\alpha+\beta}(v_i v_j^2)^{-1}$ *for* $1 \leqslant i, j \leqslant a$, *where* $x_{\alpha+\beta}(v_i v_j) = \Pi_{k=1}^{a} x_{\alpha+\beta}(v_k)^{d(i,j,k)}$ *and* $x_{2\alpha+\beta}(v_i v_j^2) = \Pi_{k=1}^{a} x_{2\alpha+\beta}(v_k)^{f(i,j,k)}$ *with some* $d(i,j,k), f(i,j,k) \in \mathbf{Z}$.

The rest of the section deals with the proof of Lemma 2.4.

Proof. Let S be a Sylow p-subgroup of $\mathrm{Sp}_4(\mathbf{F}_q)$, $q = p^a$, $a \geq 1$ and p odd. Recall that $|S| = q^4 = p^{4a}$ and in the Lie theoretic notation, S is a product of four root subgroups X_α, X_β, $X_{\alpha+\beta}$ and $X_{2\alpha+\beta}$. Each root subgroup $X_\gamma \cong (\mathbf{F}_q, +)$ and is generated by root elements $x_\gamma(v_i)$ for some v_i's , $1 \leq i \leq a$.

First of all notice that S is a semidirect product of its normal subgroup $S_0 = X_\alpha X_{\alpha+\beta} X_{2\alpha+\beta}$ of order q^3 and a subgroup $S_1 = X_\beta$ of order q. The former one is generated by $x_\alpha(v_i)$ and $x_{\alpha+\beta}(v_i)$ (for $1 \leqslant i \leqslant a$) and is isomorphic to a Sylow p-subgroup of $\mathrm{SL}_3(\mathbf{F}_q)$. The latter one is a root subgroup of S generated by $x_\beta(v_i)$ (for $1 \leqslant i \leqslant a$). To present S, we are going to use the presentation of S_0 from Lemma 2.3, then take an obvious presentation of S_1 and finally use P. Hall's lemma (Lemma 2.2 above) to "glue" those two presentations together in order to obtain a presentation of S. We will then add few relations (that hold in S) and show that some of the relations (in this newly obtained presentation) are redundant and can be obtained as a consequence of other relations.

We begin by recording a combined list of generators and relations for a presentation of S_0 (given in Lemma 2.3) and for a presentation of $S_1 \cong (\mathbf{F}_q, +)$:

Generators: $x_\alpha(v_k)$, $x_{\alpha+\beta}(v_k)$ and $x_\beta(v_k)$ with $1 \leqslant k \leqslant a$.

Relations:

1. For $1 \leqslant k \leqslant a$,
   (a) $(x_\alpha(v_k))^p = 1$, $(x_\beta(v_k))^p = 1$, and
   (b) $(x_{\alpha+\beta}(v_k))^p = 1$,
2. $[x_\alpha(v_k), x_\alpha(v_{k'})] = 1$ for $1 \leqslant k < k' \leqslant a$,
3. $[x_\beta(v_k), x_\beta(v_{k'})] = 1$ for $1 \leqslant k < k' \leqslant a$,
4. $[x_{\alpha+\beta}(v_k), x_{\alpha+\beta}(v_{k'})] = 1$ for $1 \leqslant k < k' \leqslant a$,
5. $[x_\alpha(v_1), [x_\alpha(v_k), x_{\alpha+\beta}(v_1)]] = [x_{\alpha+\beta}(v_1), [x_\alpha(v_k), x_{\alpha+\beta}(v_1)]] = 1$ for $1 \leqslant k \leqslant a$,
6. $[x_\alpha(v_k)^{-1}, x_{\alpha+\beta}(v_{k'})^{-1}] = \prod_{1 \leqslant r \leqslant a} [x_\alpha(v_r), x_{\alpha+\beta}(v_1)]^{c(k,k',r)}$ with some fixed $c(k,k',1), \ldots, c(k,k',a) \in \mathbf{Z}$, for $1 \leqslant k \leqslant a$ and $2 \leqslant k' \leqslant a$.

Let us now introduce the following notation that will make the next step more comfortable. It comes from the Steinberg notation. Let

$$x_{2\alpha+\beta}(v_i) = [x_\alpha(\frac{1}{2}v_i), x_{\alpha+\beta}(v_1)] \quad \text{for} \quad 1 \leqslant i \leqslant a$$

where $x_\alpha(\frac{1}{2}v_i) = \Pi_{j=1}^a x_\alpha(v_j)^{m(j,i)}$ for all $1 \leqslant i \leqslant a$ with some $m(j,i) \in \mathbf{Z}$, $1 \leqslant j \leqslant a$.

To use P. Hall's lemma, we need the following additional relations to hold:

(A) $x_\beta(v_i)^{-1} x_\alpha(v_j) x_\beta(v_i) = R'_{ij}$ which is equivalent to $[x_\alpha(v_j)^{-1}, x_\beta(v_i)^{-1}] = x_{\alpha+\beta}(v_i v_j) x_{2\alpha+\beta}(v_i v_j^2)^{-1}$ for $1 \leqslant i, j \leqslant a$,

(B) $x_\beta(v_i) x_\alpha(v_j) x_\beta(v_i)^{-1} = R_{ij}$ which is equivalent to $[x_\alpha(v_j)^{-1}, x_\beta(v_i)] = x_{\alpha+\beta}(v_i v_j)^{-1} x_{2\alpha+\beta}(v_i v_j^2)$ for $1 \leqslant i, j \leqslant a$,

(C) $x_\beta(v_i) x_{\alpha+\beta}(v_j) x_\beta(v_i)^{-1} = x_{\alpha+\beta}(v_j)$ for $1 \leqslant i, j \leqslant a$,

(D) $x_\beta(v_i)^{-1} x_{\alpha+\beta}(v_j) x_\beta(v_i) = x_{\alpha+\beta}(v_j)$ for $1 \leqslant i, j \leqslant a$.

In (A) and (B) above, $x_{\alpha+\beta}(v_i v_j) = \Pi_{k=1}^a x_{\alpha+\beta}(v_k)^{d(i,j,k)}$ and $x_{2\alpha+\beta}(v_i v_j^2) = \Pi_{k=1}^a x_{2\alpha+\beta}(v_k)^{f(i,j,k)}$ for all $1 \leqslant i, j \leqslant a$ with some $d(i,j,k), f(i,j,k) \in \mathbf{Z}$.

By Lemma 2.2, the group S has a presentation with $3a$ generators (listed above) and in which the relations are given by (1)–(6) and (A)–(D).

Let us now observe that the following relations also hold in S. They are the consequences of relations (C) and (D) and the Steinberg relations in $\mathrm{Sp}_4(\mathbf{F}_q)$ (cf. [GLS98, Th 1.12.1]).

7. $[x_{\alpha+\beta}(v_1), x_\beta(v_i)] = 1$ for $1 \leqslant i \leqslant a$,

8. $[x_{\alpha+\beta}(v_i), x_\beta(v_1)] = 1$ for $1 \leqslant i \leqslant a$,

9. $x_{2\alpha+\beta}(v_i^2)^{-1} = \Pi_{k=1}^a x_{2\alpha+\beta}(v_k)^{r(k,i)}$ for all $1 \leqslant i \leqslant a$ where $r(k,i) \in \mathbf{Z}$,

10. $[x_\beta(v_1), x_\alpha(v_i)] = x_{\alpha+\beta}(v_i) x_{2\alpha+\beta}(v_i^2)$ for $1 \leqslant i \leqslant a$.

Consider the combined list of relations (1)–(10) and (A), (B), (C), (D). They all hold in S and give a presentation of S on the set of $3a$ generators given above. We will now show that in fact we may reduce the list of generators and that relations (B), (C) and (D) follow from (1)–(10) and (A).

In what will follow the following commutator identity will be very useful:

$$[a, bc] = [a, b][a, c]^b \quad (*)$$

First of all, notice that (9) and (10) together with the identity $(*)$ imply that for $1 \leqslant j \leqslant a$, we have:

$$x_{\alpha+\beta}(v_i) = [x_\beta(v_1), x_\alpha(v_i)] \prod_{k=1}^a [x_\alpha(\tfrac{1}{2}v_k), [x_\beta(v_1), x_\alpha(v_1)]]^{r(k,i)}$$

where for each k, the element $x_\alpha(\frac{1}{2}v_k)$ is expressed in terms of $x_\alpha(v_i)$'s and $x_\beta(v_i)$'s, $1 \leqslant i \leqslant a$, as above. In particular, we may remove $x_{\alpha+\beta}(v_i)$, $1 \leqslant i \leqslant a$, from the list of generators.

Now, let us prove the following statement.

Claim 2.5. *The following relations follow from the relations (1)–(10) and (A):*

1. $[x_\beta(v_j), x_{2\alpha+\beta}(v_i)] = 1$ *for all* $1 \leqslant i, j \leqslant a$.

2. $[[x_\alpha(v_i), x_\beta(v_1)], x_\beta(v_j)] = 1$ *for* $1 \leqslant i, j \leqslant a$.

3. $[x_{\alpha+\beta}(v_i), x_\beta(v_j)] = 1$ *for* $1 \leqslant i, j \leqslant a$, *i.e., relations* (C) *and* (D).

4. *relations* (B).

Proof. 1.Observe that $[x_{2\alpha+\beta}(v_i), x_\beta(v_j)] = [[x_\alpha(\frac{1}{2}v_i), x_{\alpha+\beta}(v_1)], x_\beta(v_j)]$ for $1 \leqslant i, j, \leqslant a$. Recall now the Hall-Witt identity formulated for our definition of the commutators:

$$[[y, x^{-1}], z^{-1}]^{y^{-1}} [[z, y^{-1}], x^{-1}]^{z^{-1}} [[x, z^{-1}], y^{-1}]^{x^{-1}} = 1$$

Let us apply it with $y = x_\alpha(\frac{1}{2}v_i)$, $x = x_{\alpha+\beta}(v_1)^{-1}$ and $z = x_\beta(v_j)^{-1}$. First notice that $[[x, z^{-1}], y^{-1}] = [[x_{\alpha+\beta}(v_1)^{-1}, x_\beta(v_j)], x_\alpha(\frac{1}{2}v_i)^{-1}] = [1, x_\alpha(\frac{1}{2}v_i)^{-1}] = 1$ because of (7). Now, $[[z, y^{-1}], x^{-1}] = [[x_\beta(v_j)^{-1}, x_\alpha(\frac{1}{2}v_i)^{-1}], x_{\alpha+\beta}(v_1)] = [[x_\beta(v_j)^{-1}, \Pi_{k=1}^a x_\alpha(v_k)^{-m(i,k)}], x_{\alpha+\beta}(v_1)]$ by (2). Let us look more closely at $[x_\beta(v_j)^{-1}, \Pi_{k=1}^a x_\alpha(v_k)^{-m(i,k)}]$. Using repeatedly the commutator identity $(*)$ together with relation (A) and the fact that the subgroup $H_0 := \langle x_{\alpha+\beta}(v_i), x_{2\alpha+\beta}(v_i), 1 \leqslant i \leqslant a\rangle$ of S_0 is normal in S_0, we see that $[x_\beta(v_j)^{-1}, x_\alpha(\frac{1}{2}v_i)^{-1}] \in H_0$ for all $1 \leqslant i, j \leqslant a$. Now the structure of S_0 tells us that H_0 is abelian and as $x_{\alpha+\beta}(v_1) \in H_0$, we conclude that $[[x_\beta(v_j)^{-1}, x_\alpha(\frac{1}{2}v_i)^{-1}], x_{\alpha+\beta}(v_1)] = 1$. [1] At last the Hall-Witt identity gives us that $[[x_\alpha(\frac{1}{2}v_i), x_{\alpha+\beta}(v_1)], x_\beta(v_j)] = 1$ for $1 \leqslant i, j \leqslant a$, which implies the desired result.

[1] We may use the facts about the structure of S_0 since S_0 is given by relations (1), (2), (4), (5) and (6), and (9) holds in S_0.

2. Our proof follows a similar one in [BD01]. We have that
$x_\beta(v_j)[x_\alpha(v_i), x_\beta(v_1)] = x_\alpha(v_i)x_\beta(v_j)x_\beta(v_j)^{-1}x_\alpha(v_i)^{-1}x_\beta(v_j)x_\alpha(v_i)x_\beta(v_1)x_\alpha(v_i)^{-1}x_\beta(v_1)^{-1} =$
$= x_\alpha(v_i)x_\beta(v_j)[x_\beta(v_j)^{-1}, x_\alpha(v_i)^{-1}]x_\beta(v_1)x_\alpha(v_i)^{-1}x_\beta(v_1)^{-1}$.

Since $[x_\beta(v_j)^{-1}, x_\alpha(v_i)^{-1}] = [x_\alpha(v_i)^{-1}, x_\beta(v_j)^{-1}]^{-1}$, using relations (A) together with part 1 and relations (8), we observe that $[x_\beta(v_j)^{-1}, x_\alpha(v_i)^{-1}]x_\beta(v_1) = x_\beta(v_1)[x_\beta(v_j)^{-1}, x_\alpha(v_i)^{-1}]$. As furthermore, $x_\beta(v_1)$ commutes with $x_\beta(v_j)$, we have that
$x_\beta(v_j)[x_\alpha(v_i), x_\beta(v_1)] = x_\alpha(v_i)x_\beta(v_1)x_\beta(v_j)x_\beta(v_j)^{-1}x_\alpha(v_i)^{-1}x_\beta(v_j)x_\alpha(v_i)x_\alpha(v_i)^{-1}x_\beta(v_1)^{-1} =$
$x_\alpha(v_i)x_\beta(v_1)x_\alpha(v_i)^{-1}x_\beta(v_j)x_\beta(v_1)^{-1} = x_\alpha(v_i)x_\beta(v_1)x_\alpha(v_i)^{-1}x_\beta(v_1)^{-1}x_\beta(v_j) = [x_\alpha(v_i), x_\beta(v_1)]x_\beta(v_j)$.

3. From (10) and (9) we have

$$x_{\alpha+\beta}(v_i) = [x_\beta(v_1), x_\alpha(v_i)]x_{2\alpha+\beta}(v_i^2)^{-1} = [x_\beta(v_1), x_\alpha(v_i)]\Pi_{k=1}^a x_{2\alpha+\beta}(v_k)^{r(k,i)}$$

As $[a, bc] = [a, b][a, c]^b$, $[x_\beta(v_j), x_{\alpha+\beta}(v_i)] = [x_\beta(v_j), [x_\beta(v_1), x_\alpha(v_i)]\Pi_{k=1}^a x_{2\alpha+\beta}(v_k)^{r(k,i)}] =$
$= [x_\beta(v_j), [x_\beta(v_1), x_\alpha(v_i)]][x_\beta(v_j), \Pi_{k=1}^a x_{2\alpha+\beta}(v_k)^{r(k,i)}]^{[x_\beta(v_1), x_\alpha(v_i)]}$.

Using part 2, we see that $[x_\beta(v_j), [x_\beta(v_1), x_\alpha(v_i)]] = 1$, and from part 1 it follows that the commutator $[x_\beta(v_j), \Pi_{k=1}^a x_{2\alpha+\beta}(v_k)^{r(k,i)}] = 1$. This gives (C). Now notice that (D) is an immediate consequence of (C).

4. Finally we observe that relations (A) together with parts 1 and 3 imply that $x_\beta(v_i)^{-1}$ commutes with $[x_\alpha(v_j)^{-1}, x_\beta(v_i)^{-1}]$. Therefore by [BD01, Lemma 2] we have:

$$[x_\alpha(v_j)^{-1}, x_\beta(v_i)] = [x_\alpha(v_j)^{-1}, x_\beta(v_i)^{-1}]^{-1},$$

which in turn (using the relations in S_0) implies relations (B). □

Thus we have shown that S has a presentation with the generators $x_\alpha(v_k)$ and $x_\beta(v_k)$, $1 \leqslant k \leqslant a$, subject to the relations (1)–(10) and (A). Rename the relations (1)–(10) into (C1)–(C10) and relations (A) into (C11). Finally, counting the number of those relations, we obtain a presentation of S on $2a$ generators and the promised number of relations. □

2.3 Kac-Moody groups: presentation of $\Gamma = U_+$

Recall that $\overline{G} = \mathbf{G}\big(\mathbf{F}_q(\!(t)\!)\big)$ can be thought of as a topological Kac-Moody group. Since the rank of it as a Chevalley group is l, its Kac-Moody rank is $l+1$. Then $\mathbf{G}(\mathbf{F}_q[[t]])$ can be naturally identified with a maximal parahoric subgroup and P with the pro-unipotent radical $\overline{U}_+$ of the standard Iwahori subgroup $\overline{B}_+$. Thus $P = \overline{U}_+$ is the closure of U_+ in $\overline{G}$ where U_+ is the subgroup of the corresponding minimal Kac-Moody group $\widetilde{G} = \mathbf{G}(\mathbf{F}_q[t, t^{-1}])$ generated by the positive real root subgroups of $\widetilde{G}$ [RR06, Theorem 1.C].

In the notation of §2.1, we apply Lemma 2.1 with $\Gamma = U_+$: this tells us that P is the pro-p completion of the group U_+ which, in what follows, is better understood than P thanks to a combination of §2.2 and of Kac-Moody arguments which we explain in the rest of the subsection. We will then deduce a presentation of P from a presentation of $\Gamma = U_+$ because $P = \Gamma_{\hat{p}}$.

Let us go first a bit deeper into Kac-Moody theory. Let A be the generalized Cartan matrix of $\widetilde{G}$ and $\pi = \{\alpha_0, \alpha_1, \ldots, \alpha_l\}$ be the set of its fundamental roots. Corollary 1.2 of [DM07] implies that if A is 3-spherical and $q \geqslant 16$, then U_+ is an amalgamated product of the system $\{X_{\alpha_i}\} \cup \{X_{\alpha_i,\alpha_j}\}$, $0 \leqslant i, j \leqslant l$, where each $X_{\alpha_i} = \langle x_{\alpha_i}(c) \mid c \in \mathbf{F}_q\rangle \cong (\mathbf{F}_q, +)$ is a fundamental root subgroup of $\widetilde{G}$ and $X_{\alpha_i,\alpha_j} = \langle X_{\alpha_i}, X_{\alpha_j} \mid R_{i,j}\rangle$ where $R_{i,j}$ comes from the rank 2 subsystem with fundamental roots α_i and α_j. To simplify things, let us denote

$X_i := X_{\alpha_i}$ and $X_{i,j} := X_{\alpha_i,\alpha_j}$ (in particular, remark that $X_{i,j} = X_{j,i}$ for all $0 \leqslant i, j \leqslant l$). Thus in fact, U_+ is a group generated by the elements of the root subgroups X_i's for $i = 0, 1, ..., l$ and presented by the relations between those generators that hold in $X_{i,j}$ for $0 \leqslant i, j \leqslant l$ (we may let $X_{i,i} := X_i$).

Recall that the 3-spherical condition is relevant to generalized Dynkin diagrams as obtained for instance in Kac-Moody theory. In our situation the Dynkin diagram of the (untwisted) affine Kac-Moody group $\widetilde{G} = \mathbf{G}(\mathbf{F}_q[t, t^{-1}])$ obtained from $\mathbf{G}$, is the diagram obtained by adding suitably a single vertex to the (classical, i.e. spherical) Dynkin diagram of $\mathbf{G}$. The resulting Dynkin diagram is called the completed Dynkin diagram of $\mathbf{G}$; the vertex and the edges emanating from it are added in such a way that any subdiagram obtained by removing an arbitrary vertex (and the edges emanating from it) is of finite type. Geometrically, this corresponds to the fact that we pass from a finite Weyl group to an affine one acting on a Euclidean tiling so that any vertex stabilizer is a finite Weyl group. In other words, if $\mathbf{G}$ is a Chevalley group of rank l, then the Kac-Moody group $\widetilde{G}$ is l-spherical.

Let us now discuss the tools we will need to obtain an explicit presentation of U_+. Let $v_1, \ldots, v_a$ be generators of $\mathbf{F}_q$ with $v_1 = 1$. It is obvious that for each i,

$$\langle \{x_{\alpha_i}(v_k)\}_{1 \leqslant k \leqslant a} \mid x_{\alpha_i}(v_k)^p = 1, [x_{\alpha_i}(v_k), x_{\alpha_i}(v_{k'})] = 1 \text{ for } 1 \leqslant k < k' \leqslant a \rangle$$

is a presentation of X_i. Therefore U_+ is generated by elements $\{x_{\alpha_i}(v_k)\}_{1 \leqslant k \leqslant a, 0 \leqslant i \leqslant l}$ and the following $a(l+1) + \frac{1}{2}a(a-1)(l+1) = \frac{a(a+1)(l+1)}{2}$ relations must hold:

1. $x_{\alpha_i}(v_k)^p = 1$ for $1 \leqslant k \leqslant a$ and $0 \leqslant i \leqslant l$.
2. $[x_{\alpha_i}(v_k), x_{\alpha_i}(v_{k'})] = 1$ for $1 \leqslant k < k' \leqslant a$ and $0 \leqslant i \leqslant l$.

   The remaining relations will come from the subsystems $X_{i,j}$ for $0 \leqslant i \neq j \leqslant l$. Clearly, those depend on the type of $X_{i,j}$ which is determined by the type of root system generated by α_i and α_j. Let us discuss those case-by-case.

   Suppose first that $X_{i,j}$ is of type $A_1 \times A_1$. Then $X_{i,j} \cong X_i \times X_j$ and we would need the following additional relations to describe $X_{i,j}$ in this case:

3. $[x_i(v_k), x_j(v_{k'})] = 1$ for $1 \leqslant k, k' \leqslant a$. Thus for every subsystem $X_{i,j}$ of type $A_1 \times A_1$, we will have a^2 additional relations.

4. If $X_{i,j}$ is of type A_2, then $X_{i,j}$ is isomorphic to a Sylow p-subgroup of $\mathrm{SL}_3(\mathbf{F}_q)$, and so using Lemma 2.3, we notice that we need relations (A3) and (A4) with $s_i(v_k) = x_i(v_k)$, $1 \leq k \leq a$. Thus for every subsystem $X_{i,j}$ of type A_2, we will have $2a + a(a-1) = a(a+1)$ additional relations.

5. Finally, if $X_{i,j}$ is of type C_2, then $X_{i,j}$ is isomorphic to a Sylow p-subgroup of $\mathrm{Sp}_4(\mathbf{F}_q)$. If p is odd, we may use the results of §2.2.1 telling us that we need

   $$\frac{7a^2 + 13a}{2} - 2a - a(a-1) = \frac{5a^2 + 11a}{2}$$

   additional relations. These are relations (C4)–(C11) and some of relations (C1). If $p = 2$, we use the result of [LSe03, Prop. 3.4.1] to say that $X_{i,j}$ requires $8a^2$ additional relations.

Finally, notice that all of the above relations are products of p-powers and commutators. Therefore, $U_+/([U_+,U_+]U_+^p)$ is an elementary abelian p-group of order at most $p^{a(l+1)}$. To see that the exact order of this quotient is $p^{a(l+1)}$, it is enough to exhibit a quotient of U_+ which is an elementary abelian p-group whose order is equal to this upper bound. This can be seen by considering the action of U_+ on the set of alcoves sharing a codimension 1 face with the alcove c stabilized by U_+. These alcoves are in one-to-one correspondence with the set of simple roots of the Kac-Moody group $\widetilde{G}$ defined by c. Moreover, by the commutation relations between root groups in $\widetilde{G}$, each given simple root group acts simply transitively on the alcoves sharing a given panel with c (but $\neq c$) and acts trivially on the remaining alcoves of the finite set under consideration. The image of U_+ for this action is the desired quotient. Therefore we obtain that

$$U_+/([U_+,U_+]U_+^p) \cong \mathbf{F}_p^{a(l+1)}$$

(see also Corollary 2.5 of [CR14]).

We can now summarise:

Proposition 2.6. *Let $\widetilde{G} = \mathbf{G}(\mathbf{F}_q[t,t^{-1}])$ be a minimal affine untwisted Kac-Moody group of rank $l+1 \geq 4$ defined over a field $\mathbf{F}_q$ where $q = p^a$, $a \in \mathbf{N}$, $q \geqslant 16$. Let U_+ be the subgroup of $\widetilde{G}$ generated by the positive real root subgroups. Then the the following conditions hold:*

1. *$U_+/([U_+,U_+]U_+^p) \cong \mathbf{F}_p^{a(l+1)}$, and so $d(U_+) = a(l+1)$.*
2. *The group U_+ has a presentation $\langle \{x_i(v_k)\}_{0\leqslant i\leqslant l, 1\leqslant k\leqslant a} \mid R\rangle$ such that R are as described in (1)–(5) above.*
3. $$r(U_+) \leqslant \frac{a(a+1)(l+1)}{2} + |\{X_{i,j} \mid X_{i,j} \text{ is of type } A_1\times A_1\}|\cdot a^2$$
$$+ |\{X_{i,j} \mid X_{i,j} \text{ is of type } A_2\}|\cdot a(a+1) + |\{X_{i,j} \mid X_{i,j} \text{ is of type } C_2\}|\cdot |R_{C_2}|$$
where $|R_{C_2}| = \frac{5a^2+11a}{2}$ if q is odd, and $|R_{C_2}| = 8a^2$ if q is even.

We may now evaluate $r(U_+)$ in each case using Proposition 2.6. We then record the datum and the outcomes of the calculations in Table 1. For groups of type B_n, C_n and F_4, we only record the estimates for p odd (though all the estimates appear in the next section). We do it because the bound for $p=2$ is quite far away from being sharp.

2.4 Conclusion

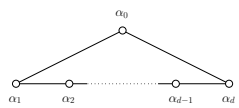
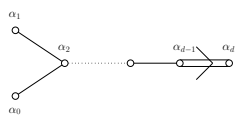
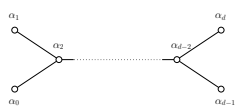
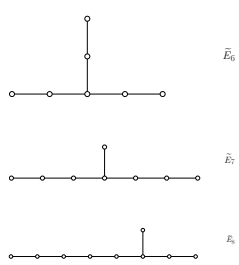
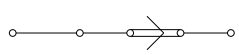
The number of generators of $P = \Gamma_{\hat{p}}$ in its presentation coming from Γ is $a(l+1)$. This is in fact a presentation with a minimal number of generators (by Proposition 2.6 – see also [CR14, Cor. 2.5]). Moreover the generators can be chosen to be $x_0(v_k), ..., x_l(v_k)$, $1 \leqslant k \leqslant a$. Our discussion gives us that P has a presentation $\langle x_0(v_k), ..., x_l(v_k), 1 \leqslant k \leqslant a \mid R\rangle$ with $|R| \leqslant Ca^2(l+1)^2$ (with C an appropriate constant as calculated in the previous section). More precisely, this proves the upper bound in the next theorem:

Theorem 2.7. *Let $\mathbf{G}\big(\mathbf{F}_q(\!(t)\!)\big)$ be a simple, simply connected, Chevalley group of rank l over a field $\mathbf{F}_q(\!(t)\!)$ with $q = p^a \geqslant 16$, and let P be its Sylow pro-p-subgroup. Then*

$$\frac{a^2(l+1)^2}{4} \leqslant r(P)$$

and the following upper bounds hold:

Table 1:

Type of $\mathbf{G}$	Kac-Moody diagram of $\widetilde{\mathbf{G}}$	$\lvert\{X_{i,j}\}\rvert$ for $X_{i,j} = A_1 \times A_1$	$\lvert\{X_{i,j}\}\rvert$ for $X_{i.j} = A_2$	$\lvert\{X_{i,j}\}\rvert$ for $X_{i,j} = C_2$	$r(U_+) \leqslant$ (* - is given only for $p \geq 3$)
A_l		$\frac{(l+1)(l-2)}{2}$	$l+1$	0	$\frac{a^2(l+1)^2+3a(l+1)}{2}$
B_l		$\frac{l(l-1)}{2}$	$l-1$	1	$\frac{a^2(l+1)^2+3a(l+1)+3a^2+7a}{2}^*$
C_l		$\frac{l(l-1)}{2}$	$l-2$	2	$\frac{a^2(l+1)^2+3a(l+1)+6a^2+16a}{2}^*$
D_l		$\frac{l(l-1)}{2}$	l	0	$\frac{a^2(l+1)^2+3a(l+1)-2a}{2}$
E_l		$\frac{l(l-1)}{2}$	l	0	$\frac{a^2(l+1)^2+3a(l+1)-2a}{2}$
F_4		$6 = \frac{4\cdot 3}{2}$	$3 = 4-1$	1	$14a^2 + 11a$ *

1. *If G has type A_l and $l \geqslant 3$, we have $r(P) \leqslant \frac{a^2(l+1)^2+3a(l+1)}{2}$.*

2. *For type B_l and $l \geqslant 3$, we have $r(P) \leqslant \frac{a^2(l+1)^2+3a(l+1)+3a^2+7a}{2}$ for $p \geqslant 3$, and $r(P) \leqslant \frac{a^2(l+1)^2+3a(l+1)+14a^2-4a}{2}$ for $p = 2$.*

3. *For type C_l and $l \geqslant 3$, we have $r(P) \leqslant \frac{a^2(l+1)^2+3a(l+1)+6a^2+16a}{2}$ and $p \geqslant 3$, and $r(P) \leqslant \frac{a^2(l+1)^2+3a(l+1)+28a^2-6a}{2}$ for $p = 2$.*

4. *For type D_l and $l \geqslant 4$, we have $r(P) \leqslant \frac{a^2(l+1)^2+3a(l+1)-2a}{2}$.*

5. *For type E_l and $l \in \{6, 7, 8\}$, we have $r(P) \leqslant \frac{a^2(l+1)^2+3a(l+1)-2a}{2}$.*

6. *For type F_4, we have $r(P) \leqslant 14a^2 + 11a$ for $p \geqslant 3$, and $r(P) \leqslant 15a^2 + 4a$ for $p = 2$.*

.

Proof. It remains to prove the lower bound. For this we use the Golod-Shafarevich inequalities as stated in the Propostion below, with $Q = P$ and $d(P) = a(l + 1)$. □

Proposition 2.8. *Let Q be a pro-p subgroup of $\mathbf{G}\big(\mathbf{F}_q(\!(t)\!)\big)$ as in Theorem 2.7. Then, with the obvious definitions for $d(Q)$ and $r(Q)$, we have $r(Q) \geqslant \dfrac{d(Q)^2}{4}$.*

Proof. We follow the lines given by the proof of Prop. 5.4 and the discussion after Prop. 5.5 in [LS94]. With the notation and terminology there, the group Q is commensurable with an $\mathbf{F}_q[[t]]$-standard group [loc. cit., Def. 2.1], which implies the subexponential growth of the sequence $(r_n)_{n\geqslant 0}$ related to the powers of the augmentation ideal Δ of the group ring $\mathbf{F}_q Q$ (more precisely: r_n is defined to be $\dim_{\mathbf{F}_p}(\Delta^n/\Delta^{n+1})$ [loc. cit., p. 320]). Subexponential growth of $(r_n)_{n\geqslant 0}$ implies the desired Golod-Shafarevich inequality. □

The equality $P = \Gamma_{\hat{p}} = (U_+)_{\hat{p}}$ was used to derive an upper bound on the number of relations needed to present P as a pro-p group. But it can be also used to deduce a lower bound on the number of relations needed to present $\Gamma = U_+$ in the discrete category.

Corollary 2.9. *For $\Gamma = U_+$ we have:*

$$d(\Gamma) = a(l + 1) \quad \textit{and} \quad \frac{a^2(l + 1)^2}{4} \leqslant r(\Gamma) \leqslant 6.25 \cdot \frac{a^2(l + 1)^2}{4}.$$

Proof. The result on $d(\Gamma)$ was shown above (Proposition 2.6) and so was the upper bound on $r(\Gamma)$ (in fact, slightly better bounds are given in Table 1). The lower bound is deduced from the fact that $r(\Gamma) \geqslant r_p(\Gamma_{\hat{p}}) = r_p(P)$ and the Golod-Shafarevich inequality given in Proposition 2.8. □

Remark 2.10. *The last corollary is slightly surprising: usually the Steinberg type presentations of groups are far from being optimal. In our case the Steinberg-like presentations are essentially optimal.*

3 The characteristic 0 case

Some results like Theorems 0.1 and 0.2 can be proved also in characteristic 0. But our results in this case are weaker than the above theorems.

In this section let k be a number field, $\mathcal{O}$ its ring of integers and V the set of its finite valuations. For $v \in V$, let k_v be the completion of k with respect to v, and $\mathcal{O}_v$ the closure of $\mathcal{O}$ in k_v. For such a v, denote by $\mathbf{F}_{p_v^{a_v}}$ the finite residue field of k. Let $\mathbf{G}$ be a simple simply connected Chevalley group scheme of arbitrary rank $l \geqslant 1$, let $G = \mathbf{G}(\mathcal{O}_v)$ and let P be a Sylow pro-p_v subgroup of G. Here is what we can prove in this situation.

Theorem 3.1. *There exists a constant $C_1 = C_1(k)$ such that for every $v \in V$ and every $\mathbf{G}$ as above, $G = \mathbf{G}(\mathcal{O}_v)$ has a presentation $\Sigma(G)$, with $D_{\Sigma(G)}$ generators and $R_{\Sigma(G)}$ relations, satisfying*

$$D_{\Sigma(G)} + R_{\Sigma(G)} \leqslant C_1.$$

Theorem 3.2. *With the notations as above, assume that the following conditions hold:*

1. *If $l = 1$, then $p_v > 2$.*
2. *If $l = 2$, then $p_v > 2$ if $\mathbf{G}$ is $B_2 = C_2$ and that $p_v > 3$ if $\mathbf{G} = G_2$.*
3. *If $l \geqslant 3$, then one of the following conditions hold:*
   (a) *$p_v^{a_v} \geqslant 16$, or*
   (b) *if $p_v^{a_v} < 16$, then $p_v > 2$ if $\mathbf{G}$ is B_l, C_l or F_4.*

Then P is generated by at least $a_v l$ and at most $a_v(l+1)$ generators. Moreover, there exist absolute constants $C_2 \geqslant 0$ and $C_3 \geqslant 0$ such that:

- *the group P has a presentation with $a_v(l+1)$ generators and at most $C_2 a_v^2 l^4$ relations;*
- *any presentation of P needs at least $C_3 a_v^2 l^2$ relations.*

Theorem 3.1 can be deduced from the following result.

Theorem 3.3. *There exists a constant $C_4 = C_4(k)$ such that $\Lambda = \mathbf{G}(\mathcal{O})$ has a presentation Σ_Λ, with D_{Σ_Λ} generators and R_{Σ_Λ} relations, satisfying*

$$D_{\Sigma_\Lambda} + R_{\Sigma_\Lambda} \leqslant C_4.$$

Let us make the following remark.

Remark 3.4.
1. *We believe that the lower bound in Theorem 3.2 above is sharp.*
2. *We do not know if the constant $C_1(k)$ in Theorem 3.1 really depends on k.*
3. *On the other hand, C_4 does depend on k, or at least on the degree $[k : \mathbf{Q}]$. To see this, let k_i be a sequence of number fields with $[k_i : \mathbf{Q}] = n_i \to \infty$ such that there exists a rational prime p which splits completely in all the k_i's. Then by the Strong Approximation Theorem, the group $\mathbf{G}(\mathcal{O})$ is mapped onto $G(\mathbf{F}_p)^{n_i}$ and since $d(\mathbf{G}(\mathbf{F}_p)^{n_i})$ grows logarithmically with n_i [Wie74], $d(\mathbf{G}(\mathcal{O}))$ grows to infinity with $[k : \mathbf{Q}]$.*

Such a sequence of fields exists. For example, denote by $\{p_i\}_{i\in\mathbf{N}}$ the sequence of odd primes congruent to $2 = 3^2$ modulo 7 : $p_1 = 23$, $p_2 = 37$, etc. and then set $k_0 = \mathbf{Q}$ and then $k_{i+1} = k_i(\sqrt{p_{i+1}})$. The polynomial $x^2 - p_{i+1}$ is irreducible over k_i, but reducible over $\mathbf{F}_7$. Hence, if $\mathcal{O}_i$ denotes the ring of integers of k_i, we should have $\mathcal{O}_i/7\mathcal{O}_i = (\mathbf{Z}/7\mathbf{Z})^{2^i}$.

Let us postpone the proof of Theorem 3.3 until Section 4. Instead now we show how it implies Theorem 3.1.

Proof of Theorem 3.1. Let us first assume that $\mathbf{G}$ is of rank $\geqslant 2$. Then the group $\mathbf{G}(\mathcal{O})$ has the congruence subgroup property in the sense that $\widehat{\mathbf{G}(\mathcal{O})} \to \mathbf{G}(\widehat{\mathcal{O}})$ is onto with a cyclic kernel (see Theorem 1.3). The presentation of $\mathbf{G}(\mathcal{O})$, promised in Theorem 3.3, gives a profinite presentation of $\widehat{\mathbf{G}(\mathcal{O})}$ and so, with one additional relation used to kill the cyclic kernel if needed, it serves as a presentation of $\mathbf{G}(\widehat{\mathcal{O}})$. As in the proof of Proposition 1.2, since $\mathbf{G}(\widehat{\mathcal{O}}) = \mathbf{G}(\mathcal{O}_v) \times M$ where M is normally generated by one element, Theorem 3.1 is proved with $C_1 \leqslant C_4 + 2$.

The remaining case is when $\mathbf{G} = \mathrm{SL}_2$. In this situation, we pick a prime v_0 of $\mathcal{O}$ and work with the arithmetic group $\mathrm{SL}_2(\mathcal{O}[\frac{1}{v_0}])$ which enjoys the congruence subgroup property: we can then use the surjective map with trivial kernel $\widehat{\mathrm{SL}_2(\mathcal{O}[\frac{1}{v_0}])} \to \widehat{\mathrm{SL}_2(\mathcal{O}[\frac{1}{v_0}])} = \prod_{v\neq v_0} \mathrm{SL}_2(\mathcal{O}_v)$ as before, in order to see that the family $\{\mathbf{G}(\mathcal{O}_v)\}_{v\neq v_0}$ is boundedly presented. At last, the single remaining group $\mathrm{SL}_2(\mathcal{O}_{v_0})$ does not cause any problem since it is analytic over k_{v_0} and therefore finitely presented. □

In order to prove Theorem 3.2 we will need the following statement.

Lemma 3.5. *Let G be a finite p-group that is an extension of U by N*

$$1 \to N \to G \to U \to 1.$$

Suppose further that N is abelian, the action of U on N is fixed, and let G_0 be such an extension that splits. Then $d(G) \leqslant d(G_0)$.

Proof. The minimal number of generators of a p-group H is $\dim(H/[H,H]H^p)$. We can therefore assume that N is an elementary abelian p-group. Moreover, if H is either G or G_0, we can factor out the subgroup $[N,H]$, and so assume that the action of U on N is trivial. In the split case we are looking now at $N \times U$, and so the number of generators is $d(G_0) = d(N) + d(U)$. This is certainly an upper bound for the number of generators of the non-split case. The latter will indeed be smaller in general as can be seen easily in any non-abelian p-group with elementary abelian centre where the number of generators of such H is strictly less than $d(Z(H)) + d(H/Z(H))$ since $Z(H)$ has a non-trivial intersection with the Frattini subgroup $\Phi(H)$. □

And now on with the proof of Theorem 3.2.

Proof of Theorem 3.2. The group P is an extension of the Sylow p_v-subgroup U of $\mathbf{G}(\mathbf{F}_{p_v^{a_v}})$ by the first congruence subgroup $N := \mathrm{Ker}\big(\mathbf{G}(\mathcal{O}_v) \to \mathbf{G}(\mathbf{F}_{p_v^{a_v}})\big)$ of $\mathbf{G}(\mathcal{O}_v)$. This group N is a uniform powerful group whose Frattini subgroup $\Phi(N)$ is equal to the second congruence subgroup of $\mathbf{G}(\mathcal{O}_v)$. In fact $N/\Phi(N)$ can be identified with $\mathrm{Lie}(\mathbf{G})(\mathbf{F}_{p_v^{a_v}})$ and $\mathbf{G}(\mathcal{O}_v)/N \cong \mathbf{G}(\mathbf{F}_{p_v^{a_v}})$ acts on $N/\Phi(N)$ by the natural adjoint action of $\mathbf{G}(\mathbf{F}_{p_v^{a_v}})$ on its Lie

algebra $\mathrm{Lie}(\mathbf{G})(\mathbf{F}_{p_v^{a_v}})$ [Wei84, Lemma 5.2]. It follows that $d(P)$ is equal to $d\big(P/\Phi(N)\big)$ and $P/\Phi(N)$ is an extension of $\mathrm{Lie}(\mathbf{G})(\mathbf{F}_{p_v^{a_v}})$ by U.

Now if $\widetilde{P}$ is the corresponding Sylow pro-p subgroup in the group $\mathbf{G}(\mathbf{F}_{p_v^{a_v}}[[t]])$ over the characteristic p ring $\mathbf{F}_{p_v^{a_v}}[[t]]$, then $\widetilde{P}$ is the split extension of U with $\widetilde{N}$, where $\widetilde{N}$ is the first congruence subgroup there, i.e., $\widetilde{N} = \mathrm{Ker}\big(\mathbf{G}(\mathbf{F}_{p_v^{a_v}}[[t]]) \to \mathbf{G}(\mathbf{F}_{p_v^{a_v}})\big)$. Also there, the Frattini subgroup $\Phi(\widetilde{N})$ of $\widetilde{N}$ is the second congruence subgroup of $\mathbf{G}(\mathbf{F}_{p_v^{a_v}}[[t]])$ and we have $d(\widetilde{P}) = d\big(\widetilde{P}/\Phi(\widetilde{N})\big)$. In this situation $\widetilde{P}/\Phi(\widetilde{N})$ is also an extension of $\mathrm{Lie}(\mathbf{G})(\mathbf{F}_{p_v^{a_v}})$ by U (via the adjoint action), but this time the extension splits.

We may therefore apply Lemma 3.5 to deduce that

$$d(P) = d\big(P/\Phi(N)\big) \leqslant d\big(\widetilde{P}/\Phi(\widetilde{N})\big) = d(\widetilde{P}).$$

In §2, using the Kac-Moody methods, we showed that $d(\widetilde{P}) = a_v(l+1)$ for $l \geqslant 3$ and $p_v^{a_v} \geqslant 16$. But in fact, as was shown in [CR14, Corollary 2.5], this result is true for all l as long as $p > 2$ for $\mathbf{G}$ being A_1, B_l, C_l or F_4 and $p > 3$ for $\mathbf{G} = G_2$. Hence, under our hypotheses, $d(P) \leqslant a_v(l+1)$. On the other hand, as P surjects onto U, we have $d(P) \geqslant d(U) = a_v l$.

Observe that N is a powerful uniform group on $a_v \cdot \dim(\mathbf{G})$ generators and hence can be presented by $C' a_v^2 \dim(\mathbf{G})^2$ relations [DDMS, Theorem 4.35]. The group U has a presentation with $a_v l$ generators and at most $C'' a_v^2 l^2$ relations. Indeed, U is a Sylow p-subgroup of $\mathbf{G}(\mathbf{F}_{p_v^{a_v}})$. But the latter group is a special case of Kac-Moody group, namely a Chevalley group over a finite field. Thus in particular, $U = U_+$ for this class of groups and so if $l \geqslant 3$, Proposition 2.6 holds for U implying the desired estimate. If $l \leqslant 2$, then U is a group on la_v generators and of order $p_v^{a_v m}$ with $m \leqslant 6$ by [GLS98, Theorem 3.3.1]. Now [LS94, Proposition 3.4.1] implies that U has a presentation on those generators with at most $12a_v^2$ relations. Thus for all l, U has a presentation with $a_v l$ generators and at most $C'' a_v^2 l^2$ relations. Now we may use P. Hall's lemma to glue together the presentations of N and U to obtain a presentation of P. As a result we conclude that P has a presentation with at most $a_v(l+1)$ generators and at most $C_3 a_v^2 l^4$ relations, as claimed.

The lower bound on the number of relations now follows from the Golod-Shafarevich inequality [LS94, Proposition 5.4]. □

4 Characteristic 0: the global case

In this section, we prove Theorem 3.3. The proof follows the line of [Cap13] where Theorem 1.1 is proved. Some results from K-theory are needed along the way.

4.1 Definitions and facts from K-theory

In what follows, Φ is a reduced, irreducible root system and R a commutative unit ring. We denote by $\mathrm{St}_\Phi(R)$ the Steinberg group of type Φ over R, which is a group defined by a presentation based on the root subgroups and commutator relation between them.

If G_Φ is the simply connected Chevalley group scheme of type Φ, there is a natural group homomorphism $\mathrm{St}_\Phi(R) \to G_\Phi(R)$ whose image is precisely the subgroup $E_\Phi(R)$ generated by the root groups $U_a(R)$, $a \in \Phi$, with respect to the standard maximal split torus. By the very definition of the low-degree K-groups of a root system and a ring, we have an exact sequence:

$$(\dagger) \quad 1 \to \mathrm{K}_2(\Phi, R) \to \mathrm{St}_\Phi(R) \to G_\Phi(R) \to \mathrm{K}_1(\Phi, R) \to 1,$$

where (the image of) $\mathrm{K}_2(\Phi, R)$ is central in $\mathrm{St}_\Phi(R)$. Roughly speaking, $\mathrm{K}_1(\Phi, R)$ measures the failure for $G_\Phi(R)$ to be generated by its unipotent elements. When $\mathrm{K}_1(\Phi, R)$ is trivial, the group $\mathrm{St}_\Phi(R)$ is a central extension of the Chevalley group $G_\Phi(R)$.

In the proof below, an important argument is the fact that the Steinberg version of a celebrated theorem of Curtis and Tits holds over rings. This result was announced almost 40 years ago by R.K. Dennis and M.R. Stein [DS74, Th. B]. Our reference is D. Allcock's recent paper [All13] which contains a vast generalization of Curtis-Tits amalgamation theorem to Steinberg groups associated to some classes of Kac-Moody groups.

Theorem 4.1. *Let Φ be a reduced irreducible root system of rank $l \geqslant 2$ with $\Pi = \{\alpha_1, ..., \alpha_l\}$ a system of simple roots in Φ. For each pair of integers $\{i, j\}$ with $1 \leqslant i, j \leqslant l$, denote by Φ_{ij} the subsystem of Φ spanned by α_i and α_j. Let R be a commutative ring with 1, and define $\Sigma(\Phi, R)$ to be the group with generators $x_\alpha(t)$ for $\alpha \in \bigcup \Phi_{ij}$ and $t \in R$ subject to the relations:*

1. $x_\alpha(s)x_\alpha(t) = x_\alpha(s + t)$, $\alpha \in \bigcup \Phi_{ij}$, $s, t \in R$,
2. $[x_\alpha(s), x_\beta(t)] = \prod x_{a\alpha+b\beta}(N_{\alpha\beta ab}s^a t^b)$

for all $\alpha, \beta \in \Phi_{ij}$ for some $1 \leqslant i, j \leqslant l$ such that $\alpha+\beta \neq 0$, where the product and the integers $N_{\alpha\beta ab}$ are as in (R2) *of* [Ste71, 3.7]. *Then $\Sigma(\Phi, R) \cong \mathrm{St}_\Phi(R)$.*

4.2 Proof of Theorem 3.3

The proof of Theorem 3.3 is now as follows.

Step I: The groups $G_\Phi(\mathcal{O})$ are all arithmetic groups and hence are finitely presented [Rag68]. So in particular the groups $G_\Phi(\mathcal{O})$, for Φ of rank $l \leqslant 5$, are all presented by at most $C_4'(k)$ generators and relations. As there are only finitely many roots systems of bounded rank, we have to deal from now on only with those of degree at least 6.

Step II: Recall that $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ have presentations with a bounded number of generators and relations independent of n [GKKL07]. This was used (together with the fact that $\mathrm{SL}_4(\mathbf{Z})$ is finitely presented) in [GKKL11] to show that the groups $\mathrm{SL}_n(\mathbf{Z})$, for $n \geqslant 6$, are boundedly presented. The proof works word to word to show that $\mathrm{St}_{A_l}(\mathcal{O})$ are boundedly presented for $l \geqslant 6$.

Step III: We now show that every Dynkin diagram Φ of rank at least 6 can be covered by three subdiagrams Φ_i (for $i = 1, 2, 3$) such that:

1. Each Φ_i has at most two connected components, and every connected component is either of type A_l (for $l \geqslant 2$) or of rank at most 5,
2. Every two nodes of Φ belong to at least one of the Φ_i's, and
3. Each intersection $\Phi_i \cap \Phi_j$ (for $i \neq j$) has at most two components, each either empty or of type A_l (for $l \geqslant 2$), B_3 or C_3.

Let us list explicitly Φ_i, $i = 1, 2, 3$, in each particular case:

- For B_l, $l \geqslant 6$, take $\Phi_1 = A_{l-1}$, $\Phi_2 = B_3 \sqcup A_{l-4}$ and $\Phi_3 = \varnothing$,

- For C_l, $l \geqslant 6$, take $\Phi_1 = A_{l-1}$, $\Phi_2 = C_3 \sqcup A_{l-4}$ and $\Phi_3 = \varnothing$,
- For D_l, $l \geqslant 6$, take $\Phi_1 = A_{l-1}$, $\Phi_2 = A_{l-1}$ (different from Φ_1) and $\Phi_3 = A_3$ (the one containing the "fork"),
- For E_l, $l \in \{6, 7, 8\}$, take $\Phi_1 = A_{l-1}$, $\Phi_2 = A_4$ (the one containing one of the end-nodes and the vertex missed by Φ_1) and $\Phi_3 = A_{l-2}$ (the one containing the other end-node and containing the vertex missed by Φ_1).

Step IV: Given $\Phi = \bigcup_{i=1}^{3} \Phi_i$ as in the previous step, the Curtis-Tits Theorem guarantees that a presentation for $\mathrm{St}_\Phi(\mathcal{O})$ is obtained by taking the union of the presentation of $\mathrm{St}_{\Phi_i}(\mathcal{O})$ and gluing them along the intersections. As we have arranged that all the $\mathrm{St}_{\Phi_i}(\mathcal{O})$ as well as their intersections have bounded presentations, the same now applies to $\mathrm{St}_\Phi(\mathcal{O})$.

Step V: We now use the stability results to deduce that by adding a bounded number of relations to the presentation of $\mathrm{St}_\Phi(\mathcal{O})$, we obtain a bounded presentation for $G_\Phi(\mathcal{O})$ as promised, where the bound depends on $\mathcal{O}$ only.

First of all notice that by the results of Mennicke, Bass-Milnor-Serre and Matsumoto (cf. Theorem 7.4 of [Spl86]), the group $\mathrm{K}_1(\Phi, \mathcal{O})$ is trivial when $l \geqslant 2$, and therefore definitely in our case.

Thus in view of (†) and the result just obtained in Step IV, to finish our proof it remains to show that for all Φ of rank at least 6, the corresponding family of groups $\{K_2(\Phi, \mathcal{O})\}_\Phi$ is boundedly generated.

To do that, let us recall the stability results of Dennis, Van der Kallen and Stein that are summarised in [Spl86, Theorem 7.5] and in the example following it. Applied to our situation they imply that for $l \geqslant 6$ and $\Phi_l = A_l, B_l, C_l$ or D_l, the maps

$$K_2(\Phi_6, \mathcal{O}) \to K_2(\Phi_l, \mathcal{O})$$

are surjective as well as for $l = 6, 7, 8$, are the maps

$$K_2(A_6, \mathcal{O}) \to K_2(E_l, \mathcal{O}).$$

It follows that $K_2(\Phi_l, \mathcal{O})$, $l \geqslant 6$, is boundedly generated provided we can show that $K_2(\Phi_6, \mathcal{O})$ are finitely generated. But this follows immediately as $\mathrm{St}_{\Phi_6}(\mathcal{O})$ is boundedly presented (as we showed in the previous step) while $G_{\Phi_6}(\mathcal{O})$ is finitely presented (as an arithmetic group): this implies that $K_2(\Phi_6, \mathcal{O})$ is finitely generated as a normal subgroup; being central, it is also finitely generated as a group.

Remark 4.2. *As pointed out above in Remark 3.4, the constant $C_4(k)$ in Theorem 3.3 does depend on k. In fact we observed there that there exist sequences of fields k_i with $|k_i : \mathbf{Q}| \to \infty$ such that $C_4(k_i) \geqslant c_0 \log |k_i : \mathbf{Q}|$ for some absolute constant c_0. One can carefully analyse the proof of Theorem 3.3 to deduce that $C_4(k) \leqslant C_0 |k : \mathbf{Q}|^2$ (when $l \geqslant 6$).*

Acknowledgements. The authors would like to thank the anonymous referee for his/her detailed comments that helped to improve the paper.

The first author was supported by the Leverhume Research Grant RPG-2014-106. The second author wishes to acknowledge support by the ISF, the NSF, Dr. Max Rössler, the Walter Haefner Foundation and the ETH Foundation. The third author would like to thank Amaury Thuillier for many useful discussions and was supported by the ANR GDSous/GSG project ANR-12-BS01-0003 and the Alexander von Humboldt Foundation.

References

[All13] Daniel Allcock, *Steinberg groups as amalgams*, http://arxiv.org/abs/1307.2689, 2013.

[BD01] Daniel K. Biss and Samit Dasgupta, *A presentation for the unipotent group over rings with identity*, J. Algebra **237** (2001), no. 2, 691–707. MR 1816711 (2002k:20091)

[Cap13] Inna Capdeboscq, *Bounded presentations of Kac-Moody groups*, J. Group Theory **16** (2013), no. 6, 899–905. MR 3198724

[CR14] Inna Capdeboscq and Bertrand Rémy, *On some pro-p groups from infinite-dimensional Lie theory*, Mathematische Zeitschrift **278** (2014), no. 1-2, 39–54. MR 3267568.

[Car05] Roger W. Carter. *Lie algebras of finite and affine type.* Cambridge Studies in Advanced Mathematics, 96. Cambridge University Press, Cambridge, 2005. MR 2188930 (2006i:17001)

[DDMS] John D. Dixon, Marcus du Sautoy, Avinoam Mann, Dan Segal. *Analytic pro-p groups.* Second edition. Cambridge Studies in Advanced Mathematics, 61. Cambridge University Press, Cambridge, 1999. MR 1720368

[DM07] Alice Devillers and Bernhard Mühlherr, *On the simple connectedness of certain subsets of buildings*, Forum Math. **19** (2007), no. 6, 955–970. MR 2367950 (2008i:20042)

[DS74] R. Keith Dennis and Michael R. Stein, *Injective stability for K_2 of local rings*, Bull. Amer. Math. Soc. **80** (1974), 1010–1013. MR 0371880 (51 #8097)

[GLS98] Daniel Gorenstein, Richard Lyons, and Ronald Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A*, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, Providence, RI, 1998, Almost simple K-groups. MR 1490581 (98j:20011)

[GKKL07] Robert Guralnick, William Kantor, Martin Kassabov and Alexander Lubotzky, *Presentations of finite simple groups: profinite and cohomological approaches.* Groups Geom. Dyn. 1 (2007), no. 4, 469–523. MR 2357481 (2008j:20089)

[GKKL08] ———, *Presentations of finite simple groups: a quantitative approach.* J. Amer. Math. Soc. 21 (2008), no. 3, 711–774. MR 2393425 (2010c:20011)

[GKKL11] ———, *Presentations of finite simple groups: a computational approach*, J. Eur. Math. Soc. (JEMS) **13** (2011), no. 2, 391–458. MR 2746771 (2011m:20035)

[KL06] Inna Korchagina and Alexander Lubotzky, *On presentations and second cohomology of some finite simple groups.* Publ. Math. Debrecen 69 (2006), no. 3, 341–352. MR 2273986 (2007i:20057)

[LSe03] Alexander Lubotzky and Dan Segal, *Subgroup growth.* Progress in Mathematics, **212**. Birkhuser Verlag, Basel, 2003. MR 1978431(2004k:20055)

[LS94] Alexander Lubotzky and Aner Shalev, *On some Λ-analytic pro-p groups*, Israel J. Math. **85** (1994), no. 1-3, 307–337. MR 1264349 (95f:20047)

[Lub01] Alexander Lubotzky, *Pro-finite presentations*, J. Algebra **242** (2001), no. 2, 672–690. MR 1848964 (2002i:20045)

[Lub05] _____, *Finite presentations of adelic groups, the congruence kernel and cohomology of finite simple groups*, Pure Appl. Math. Q. (2005), no. 2, Special Issue: In memory of Armand Borel. Part 1, 241–256.

[Mar91] Grigory A. Margulis, *Discrete subgroups of semisimple Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 17, Springer-Verlag, Berlin, 1991. MR 1090825 (92h:22021)

[PR83] Gopal Prasad and M. S. Raghunathan, *On the congruence subgroup problem: determination of the metaplectic kernel*, Invent. Math. **71** (1983), 21–42.

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994.

[Pra77] Gopal Prasad, *Strong approximation for semi-simple groups over function fields*, Ann. of Math. (2) **105** (1977), no. 3, 553–572. MR 0444571 (56 #2921)

[Rag68] M. S. Raghunathan, *A note on quotients of real algebraic groups by arithmetic subgroups*, Invent. Math. **4** (1967/1968), 318–335. MR 0230332 (37 #5894)

[Rag76] _____, *On the congruence subgroup problem*, Publications Mathématiques IHÉS **46** (1976), 107–161. MR 0507030 (58 #22325)

[Rém02] Bertrand Rémy, *Groupes de Kac-Moody déployés et presque déployés*, Astérisque, vol. 277, Société mathématique de France, 2002.

[Rém04] _____, *Topological simplicity, commensurator super-rigidity and non-linearities of Kac-Moody groups*, Geom. Funct. Anal. **14** (2004), 810–852.

[RR06] Bertrand Rémy and Mark Ronan, *Topological groups of Kac-Moody type, right-angled twinnings and their lattices*, Comment. Math. Helv. **81** (2006), 191–219.

[Spl86] Siegfried Splitthoff, *Finite presentability of Steinberg groups and related Chevalley groups*, Applications of algebraic K-theory to algebraic geometry and number theory, Part I, II (Boulder, Colo., 1983), Contemp. Math., vol. 55, Amer. Math. Soc., Providence, RI, 1986, pp. 635–687. MR 862658 (88b:20069)

[Ste71] Michael R. Stein, *Generators, relations and coverings of Chevalley groups over commutative rings*, Amer. J. Math. **93** (1971), 965–1004. MR 0322073 (48 #437)

[Tit79] Jacques Tits, *Reductive groups over local fields*, Automorphic forms, representations and L-functions, Part 1, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 29–69. MR 546588 (80h:20064)

[Wei84] Boris Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups*, Annals of Mathematics **120** (1984), 271–315. MR 763908 (86m:20053)

[Wie74] James Wiegold. *Growth sequences of finite groups.* Collection of articles dedicated to the memory of Hanna Neumann, VI. J. Austral. Math. Soc. 17 (1974), pp. 133–141. MR 0349841

Inna Capdeboscq
Mathematics Institute
University of Warwick
Zeeman Building Coventry CV4 7AL – United Kingdom
I.Capdeboscq@warwick.ac.uk

Alexander Lubotzky
Einstein institute of mathematics
Hebrew University
Givat Ram, Jerusalem 91904 – Israel
alex.lubotzky@mail.huji.ac.il

Bertrand Rémy
Centre de Mathématiques Laurent Schwartz UMR 7640
École polytechnique
F-91128 Palaiseau cedex – France
bertrand.remy@polytechnique.edu