

# Counting lattices in simple Lie groups: the positive characteristic case.

Alireza Salehi Golsefidy\*

July 29, 2011

## Abstract

In this article we prove a conjecture of A. Lubotzky: let  $G = \mathbb{G}_0(K)$ , where  $K$  is a local field of characteristic  $p \geq 5$ ,  $\mathbb{G}_0$  is a simply connected, absolutely almost simple  $K$ -group of  $K$ -rank at least 2. We give the rate of growth of

$$\rho_x(G) := |\{\Gamma \subseteq G \mid \Gamma \text{ a lattice in } G, \text{ vol}(G/\Gamma) \leq x\}| / \sim |,$$

where  $\Gamma_1 \sim \Gamma_2$  if and only if there is an abstract automorphism  $\theta$  of  $G$  such that  $\Gamma_2 = \theta(\Gamma_1)$ . We also study the rate of subgroup growth  $s_x(\Gamma)$  of any lattice  $\Gamma$  in  $G$ . As a result we show that these two functions have the same rate of growth which proves Lubotzky's conjecture.

Along the way, we also study the rate of growth of the number of equivalence classes of maximal lattices in  $G$  with covolume at most  $x$ .

## 1 Introduction and statement of results.

Let  $G$  be a semisimple Lie group with a fixed Haar measure  $\mu$ . Let  $\rho_x(G)$  be the number of lattices (i.e. discrete subgroups of finite covolume) in  $G$  of covolume at most  $x$ , up to an automorphism of  $G$ , i.e. the same definition as the one given in the abstract for any semisimple Lie group. Much attention has been given in recent years to the question of determining the rate of growth of  $\rho_x(G)$  where  $G$  is a simple real Lie group. In this paper, we focus on the case when  $G$  is a simple group over a local field of positive characteristic and determine the rate of growth of  $\rho_x(G)$ . For the most general cases, our result depends on several well-founded conjectures, which are known to hold in most cases. We should say that in the characteristic zero case, as the group of outer automorphisms of  $G$  is finite, one can instead count conjugacy classes of lattices. However in the positive characteristic the group of outer automorphisms  $\text{Aut}(G)/\text{Inn}(G)$  is an infinite compact group, which adds more complications to all the arguments in this work.

---

\*A. S-G. was partially supported by the NSF grant DMS-0635607 and the NSF grant DMS-1001598.

**Theorem 1.** *Let  $G = \mathbb{G}_0(K)$ , where  $K$  is a local field of characteristic  $p \geq 5$  and  $\mathbb{G}_0$  is a simply connected absolutely almost simple  $K$ -group of  $K$ -rank bigger than 1. Assuming the CSP, MP and the Weil conjecture hold for any group with the same absolute type as  $\mathbb{G}_0$ , there exist positive numbers  $C$  and  $D$  depending only on  $G$  such that*

$$x^C \log x \leq \rho_x(G) \leq x^{D \log x},$$

*for all sufficiently large  $x$ . Moreover the lower bound is unconditional.*

We will explain below what the Weil conjecture, CSP and MP are and when they are known to hold. Let us first put this theorem in the perspective of the previous works as it represents a phenomenon which is different than the characteristic zero case.

M. Burger, T. Gelander, A. Lubotzky, and S. Mozes [BGLM02] studied this problem for  $G = \mathrm{PO}(n, 1)$ , for  $n \geq 4$ . Their approach was geometric and they counted the torsion free lattices. As a result, they proved that the rate of growth of  $\rho_x^\circ(G)$  is the same as the rate of growth of the number  $s_x(\Gamma)$  of subgroups of index at most  $x$  in a certain lattice  $\Gamma$  in  $G$ . Lubotzky conjectured that this should be a general phenomenon, namely the rate of growth of  $\rho_x(G)$  should be the same as the rate of subgroup growth of any lattice in  $G$  (for further developments for the arithmetic subgroups in  $\mathrm{PO}(2, 1)$  or  $\mathrm{PO}(3, 1)$  see [BGLS]). Belolipetsky and Lubotzky [BL] showed that this conjecture is not true in the characteristic zero case. In contrast, Theorem 1 proves Lubotzky's conjecture in the positive characteristic case.

The general strategy is to divide the problem into three parts. First one has to understand the asymptotic behavior of  $m_x(G)$ , the number of maximal lattices, up to an automorphism of  $G$ , with covolume at most  $x$ . Second the rate of growth of  $s_x(\Gamma)$ , where  $\Gamma$  is a lattice in  $G$ , has to be described. Finally these results have to be carefully combined to get the rate of growth of  $\rho_x(G)$ . Our result for counting maximal lattices is:

**Theorem 2.** *For a given  $G$  as above. Assuming the Weil conjecture holds for any group with the same absolute type as  $\mathbb{G}_0$ , there are positive numbers  $A$  and  $B$  which depend only on  $G$  such that,*

$$x^A \leq m_x(G) \leq x^{B \log \log x},$$

*for all sufficiently large  $x$ . The lower bound holds unconditionally.*

This is the characteristic  $p$  analogue of Belolipetsky's [Be07] result for the characteristic zero case; but we should stress that his proof relies on various results which are either only suitable for number fields or only known in that case. In the positive characteristic case, we have to employ certain results from algebraic geometry and prove a local-global theorem for adjoint quasi-split groups. We also give a method to get an upper bound for the class number of a coherent family of parahorics which also works in the characteristic zero case. As a result,

in the characteristic  $p$  case, our upper bound  $x^{B \log \log x}$  is better than Belolipetsky's upper bound  $x^{(\log x)^\varepsilon}$ .

Another challenge we face is with the subgroup growth. Here the results on counting congruence subgroups were known only for globally split lattices. One of the difficulties lies on the fact that structure of certain graded Lie algebras is complicated if the global form is not split. In order to overcome this difficulty, conceptually, we make a base change to an unramified extension in order to get a quasi-split group. Then using results of Prasad-Raghunathan [PR84] and changing the grading on the Lie algebra, we get the rate of  $c_x(\mathbb{G}(\mathcal{O}(\mathfrak{p}_0)))$  congruence subgroup growth of  $\mathbb{G}(\mathcal{O}(\mathfrak{p}_0))$ , where  $\mathfrak{p}_0$  is a place of a global function field  $k$ ,  $\mathcal{O}(\mathfrak{p}_0)$  is the ring of  $\mathfrak{p}_0$ -integers of  $k$ ,  $\mathbb{G}$  is an absolutely almost simple  $k$ -group with a fixed  $k$ -embedding into  $\mathbb{GL}_n$  and  $\mathbb{G}(\mathcal{O}(\mathfrak{p}_0)) = \mathbb{G} \cap \mathbb{GL}_n(\mathcal{O}(\mathfrak{p}_0))$ . This result extends the result of Abért, Nikolov and Szegedy [ANS03], who showed it for  $k$ -split groups.

**Theorem 3.** *In the above setting, there exist positive numbers  $C$  and  $D$  depending on  $\Lambda_0 = \mathbb{G}(\mathcal{O}(\mathfrak{p}_0))$  such that*

$$x^{C \log x} \leq c_x(\Lambda_0) \leq x^{D \log x},$$

for all sufficiently large  $x$ .

Indeed, our method of proof refines the above theorem and gives an explicit dependence of the constants on a given lattice in  $G$ .

**Corollary 4.** *Assuming the CSP, MP and the Weil conjecture hold for any group with the same absolute type as  $\mathbb{G}_0$ , there are positive numbers  $C$ ,  $D$ , and  $x_0$  depending only on  $G$  such that for any lattice  $\Gamma$  in  $G$*

$$x^{C \log x / \log(\text{vol}(G/\Gamma))} \leq s_x(\Gamma) \leq (\text{vol}(G/\Gamma) \cdot x)^{D \log(\text{vol}(G/\Gamma) \cdot x)},$$

for any positive number  $x \geq x_0$ .

After proving Theorem 1 or Corollary 4, the next natural questions are about their asymptotic behavior.

**Question 5.** In the above setting, does the following limit exist?

$$\lim_{x \rightarrow \infty} \frac{\log \rho_x(G)}{(\log x)^2}$$

In the characteristic zero case, as a result of works of D. Goldfeld, A. Lubotzky, N. Nikolov, L. Pyber [GLP04, LN04], we know the asymptotic behavior of  $s_x(\Gamma)$ . It is interesting to understand the exact asymptotic behavior of  $s_x(\Gamma)$  in the positive characteristic.

**Question 6.** In the above setting, for a given  $\Gamma$  a lattice in  $G$ , does the following limit exist?

$$\lim_{x \rightarrow \infty} \frac{\log s_x(\Gamma)}{(\log x)^2}$$

One can also ask what the rate of growth of  $m_x(G)$  is exactly.

**Question 7.** In the above setting, are there positive numbers  $A$  and  $B$  depending on  $G$  such that

$$x^A \leq m_x(G) \leq x^B,$$

for sufficiently large  $x$ ?

In fact our proof shows that Question 7 has an affirmative answer if a question of de Jong and Katz [dJK] and the Weil conjecture hold. de Jong and Katz [dJK] asked if for any  $q$  there is  $c = c(q)$  such that the number of smooth projective curves of genus  $g$  over  $\mathbb{f}_q$  is at most  $c^g$ .

In order to prove Theorems 1 and 3, we will prove the following theorem on graded Lie algebras. It essentially says as we “unwind” a  $\mathbb{Z}/m\mathbb{Z}$ -graded perfect finite dimensional Lie algebra, it does not lose its perfectness by much.

**Theorem 8.** *Let  $m$  be a natural number and  $\widehat{\mathfrak{g}} = \bigoplus_{i=0}^{m-1} \mathfrak{g}_i$  be a perfect  $\mathbb{Z}/m\mathbb{Z}$ -graded  $\mathfrak{F}$ -Lie algebra,*

$$\mathfrak{L} = \bigoplus_{i=1}^{\infty} \mathfrak{g}_i \otimes t^i,$$

where  $\mathfrak{g}_i = \mathfrak{g}_{i \pmod{m}}$ ,  $D$  a positive integer, and  $\mathfrak{h}$  an  $\mathfrak{F}$ -sub-algebra with finite co-dimension in  $\mathfrak{L}^D$ , where  $\mathfrak{L}^D$  denotes the direct sum of  $D$  copies of  $\mathfrak{L}$ . There exists a constant  $C = C(\widehat{\mathfrak{g}})$  depending only on  $\widehat{\mathfrak{g}}$ , such that

$$\text{codim}_{\mathfrak{L}^D}[\mathfrak{h}, \mathfrak{h}] \leq C(\text{codim}_{\mathfrak{L}^D} \mathfrak{h} + D).$$

Let us finish the introduction, by saying a few words on the mentioned conjectures. Let  $k$  be global field and  $\mathbb{G}$  a simply connected absolutely almost simple  $k$ -group. Weil conjectured that  $\tau_k(\mathbb{G}) = 1$ , where  $\tau_k(\mathbb{G})$  is the Tamagawa number. We refer the reader to [We82] for the exact definition of the Tamagawa number. Weil’s conjecture is known to hold when  $\mathbb{G}/k$  is either an inner form of type A, any form of type B, of type C, of type D except triality forms of type  $D_4$ , of type  $G_2$  [We82], or a  $k$ -split group [H74]. Indeed what we need in this article is only a uniform lower bound for  $\tau_k(\mathbb{G})$ .

Congruence subgroup property (CSP) essentially says that any arithmetic lattice has a subgroup of finite index such that any of its finite index subgroups is congruence and Margulis-Platonov (MP) conjecture describes structure of normal subgroups of  $\mathbb{G}(k)$ . For the precise statements, we refer the reader to the nice survey of these problems by Prasad and Rapinchuk [PR]. We should add that MP holds for  $k$ -isotropic groups and inner forms of type A [PR] and CSP holds for  $k$ -isotropic groups, by works of Raghunathan [Ra76, Ra86]. On the other hand, by a result of G. Harder [H75], if  $k$  is a global function field and  $\mathbb{G}$  is anisotropic over  $k$ , then it is of type A. Hence, assuming  $k$  is a global function field, MP is true for all absolutely almost simple  $k$ -groups except possibly for an anisotropic outer form of type A and CSP is true for all absolutely almost simple  $k$ -groups except possibly for an anisotropic form of type A.

In particular, by the above discussion, all of our results are unconditional for groups of type B, C, D (except  $D_4$ ) and  $G_2$ .

## 1.1 Outline of the argument

In order to prove the upper bound of Theorem 2, we essentially follow Borel-Prasad [BP89]. However here we have to provide estimates for all the finiteness results required for our quantitative statement. We first use Rohlfs' maximality criterion to get a description of maximal lattices in  $G = \mathbb{G}_0(K)$ . It essentially says we have to understand the following parameters:

- 1- A function field  $k$  and a place  $\mathfrak{p}_0$  over  $k$ , such that  $k_{\mathfrak{p}_0} \simeq K$ .
- 2- A simply connected absolutely almost simple  $k$ -group  $\mathbb{G}$ , such that  $\mathbb{G} \simeq \mathbb{G}_0$  over  $k_{\mathfrak{p}_0}$  ( $K$  is identified with  $k_{\mathfrak{p}_0}$ .)
- 3- A coherent family of parahoric subgroups  $\{P_{\mathfrak{p}}\}$  for any  $\mathfrak{p} \neq \mathfrak{p}_0$ .

Indeed as part of the criterion, we have that  $\Gamma = N_G(\Lambda)$ , where

$$\Lambda = \mathbb{G}(k) \cap \prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}.$$

Moreover, we can start with  $\mathcal{G}$  the unique quasi-split  $k$ -inner form of  $\mathbb{G}$  and parameterize  $\mathbb{G}$ , more or less, via elements of  $H^1(k, \overline{\mathcal{G}})$ , where  $\overline{\mathcal{G}}$  is the adjoint form of  $\mathcal{G}$ . Furthermore there is a field extension  $l$  of degree at most 3 over  $k$ , over which  $\mathcal{G}$  splits, and for a given  $l$  and  $k$  there is a unique quasi-split  $k$ -group of a given type which splits over  $l$ .

On the other hand, instead of giving coherent families of parahoric subgroups, first we will determine possible types of such families up to isomorphisms of the local Dynkin diagrams, and then give an upper bound on the number of admissible coherent families having the same type up to isomorphisms of the local Dynkin diagrams. Overall we have to estimate the number of:

- 1- possible function fields  $k$  and  $l$  and a place  $\mathfrak{p}_0$  over  $k$  with the above properties. (This give us a unique  $\mathcal{G}$  in the above notation.)
- 2- possible elements of  $H^1(k, \overline{\mathcal{G}})$ . (This give us  $\mathbb{G}$ .)
- 3- possible coherent types, up to an isomorphism of the local Dynkin diagram at each place. (This gives us  $\{P_{\mathfrak{p}}\}$  a coherent family of parahoric subgroups of this given type, up to action of  $\overline{\mathbb{G}}(\mathbb{A}_k)$ .)
- 4- elements of  $\text{Cl}(\overline{\mathbb{G}}, \{\overline{P}_{\mathfrak{p}}\})$ . (Altogether we get  $\Lambda$  and therefore  $\Gamma$ .)

To get the lower bound of Theorem 2, we shall appeal to results of Margulis and Prasad on the abstract isomorphisms between two lattices in a semisimple Lie group over a positive characteristic local field.

To prove the upper bound of Theorem 1, as the number of maximal lattices is relatively small, it is enough to understand  $s_x(\Gamma)$  the number of subgroups of index at most  $x$  in  $\Gamma$ , where  $\Gamma$  is a maximal lattice with covolume at most  $x$ . Then we will go through the following steps:

- 1- Using Rohlf's short exact sequence and previous estimates, we show that  $\Gamma/\Lambda \leq x^{c_1}$ , where  $c_1$  only depends on  $G$ .
- 2- Following Lubotzky [Lu95], we use a result of Babai, Cameron and Palfy to reduce the problem to  $s_x(\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)})$ , where  $P_{\mathfrak{p}}^{(1)}$  is the first congruence subgroup of  $P_{\mathfrak{p}}$  and  $\deg T = \sum_{\mathfrak{p} \in T} \deg \mathfrak{p} \leq \log x$ .
- 3- We consider  $\mathcal{L}$  the graded Lie algebra associated to the filtrations of the parahoric subgroups  $\{P_{\mathfrak{p}}\}_{\mathfrak{p} \in T}$ , similar to Lubotzky and Shalev [LS94] (also see [LS03, Section 6.2] or [ANS03]) and reduce the problem to the following statement:

$$\text{codim}_{\mathcal{H}}[\mathcal{H}, \mathcal{H}] \leq c_2 \deg T + c_3 \text{codim}_{\mathcal{L}} \mathcal{H},$$

where  $\mathcal{H}$  is an  $\mathfrak{f}_p$ -subalgebra of  $\mathcal{L}$ , and  $c_2$  and  $c_3$  just depend on  $\mathbb{G}_0$  and  $K$ .

- 4- Finally we deduce the above statement from Theorem 8. Using a result of [PR84], we view  $\mathcal{L} \otimes_{\mathfrak{f}_k} \mathfrak{F}$  as the direct sum of graded algebras of certain parahoric subgroups of  $\mathbb{G}(\widehat{k}_{\mathfrak{p}})$ , and then change these parahoric subgroups to the "largest" parahoric subgroups, where we have a very good understanding of the graded Lie algebras and get the desired result.

To get the lower bound, we essentially follow [Sh92]. However we have to be extra careful as we are counting up to the action of  $\text{Aut}(G)$ , and so we again appeal to the results of Margulis and Prasad on the abstract isomorphism of lattices in  $G$ .

At the end, we point out that the same arguments, not only gives us Theorem 3, but also its uniform version, namely Corollary 4.

## 1.2 Acknowledgment.

I would like to thank Professor A. Lubotzky for introducing me to these problems. I am also very grateful for all the conversations that I had with him both from math and presentation points of view. I am in Professor G. Prasad's debt for very helpful correspondences. Special thanks are due to Professor B. Conrad for providing the proof of Theorem 9, on "Shapiro's lemma" for flat cohomologies. I also thank Professor J. Ellenberg and Professor M. Belolipetsky for pointing out some minor mistakes. I also would like to thank anonymous referees for their valuable comments that have improved the quality of the initial manuscript.

## 2 Notation, conventions and preliminaries.

### 2.1 Field related notations.

In this paper,  $k$  is a global function field. Let  $V_k$  be the set of places of  $k$ . For any  $\mathfrak{p} \in V_k$ , let  $k_{\mathfrak{p}}$  be the  $\mathfrak{p}$ -adic completion of  $k$ ,  $\mathfrak{f}_{\mathfrak{p}}$  its residue field. Let  $\mathbb{A}_k$  be the ring of adèles of  $k$ . For any non-archimedean local field  $K$ , let  $\widehat{K}$  be the maximal unramified extension of  $K$ ,  $\mathfrak{f}$  residue field of  $K$ , and  $\mathfrak{F}$  the residue field of  $\widehat{K}$ .

Let  $\mathbb{G}_0$  be a simply connected, absolutely almost simple  $K$ -group of  $K$ -rank at least 2. Let  $G = \mathbb{G}_0(K)$ .

For any finite set  $X$ , the cardinality of  $X$  is denoted by either  $|X|$  or  $\#X$ . If  $H_1$  is a subgroup of  $H_2$ , the index of  $H_1$  in  $H_2$  is denoted by  $[H_2 : H_1]$ .

### 2.2 Flat and Galois cohomology.

Let  $E$  be a field and  $\mathbb{H}$  an affine algebraic group-scheme over  $E$ . In this article,  $H^1(E, \mathbb{H})$  denotes the flat cohomology  $H^1(\mathrm{Spec}(E), \mathbb{H})$  and, similarly,  $H^i(E, \mathbb{H})$  denotes the  $i^{\mathrm{th}}$  flat cohomology if  $\mathbb{H}$  is an abelian  $E$ -group-scheme.

Let us summarize theorems on flat cohomology that will be used in the course of this article.

**Theorem 9.** *1- If  $\mathbb{H}$  is a smooth  $E$ -group-scheme, then the flat cohomology is canonically isomorphic to the Galois cohomology.*

*2- If there is a short exact sequence of abelian  $E$ -group schemes, then one functorially gets a long exact sequence of flat cohomologies.*

*3- If  $\mathbb{H}$  is an abelian  $k$ -group-scheme and  $l$  is a finite separable extension of  $k$  a global field, then naturally*

$$H^i(k_{\mathfrak{p}}, R_{l/k}(\mathbb{H})) \simeq \bigoplus_{\mathfrak{q}|\mathfrak{p}} H^i(l_{\mathfrak{q}}, \mathbb{H}),$$

for any  $\mathfrak{p} \in V_k$  and  $i \geq 1$ .

*Proof.* (We would like to thank B. Conrad for providing the proof of the third part.) The first part is proved in [M80, Chapter III, Theorem 2.10, Theorem 3.9, Theorem 4.7 and Theorem 4.8(a)]. The second one is part of the delta-functor structure of cohomology. (It is worth mentioning that starting with a short exact sequence with non-commutative  $E$ -group-schemes, one still gets a long exact sequence involving cohomology of degree zero and one [M80, Chapter III, proposition 4.5] or [Sh72]). The following proof of the third part was provided to us by B. Conrad. Since the Weil restriction is pushforward on fppf abelian sheaves, this isomorphism comes from the degenerate Leray spectral sequence [M80, Chapter III, Theorem 1.18(a)] for fppf cohomology relative to the finite étale covering  $f : \mathrm{Spec}(l \otimes_k k_{\mathfrak{p}}) \rightarrow \mathrm{Spec}(k_{\mathfrak{p}})$ . The degeneration is due to the fact that the Weil restriction functor  $f_*$  on fppf abelian sheaves is exact (and

hence has vanishing higher derived functors) since étale-locally (and hence fppf-locally) on  $\text{Spec}(k_{\mathfrak{p}})$  it becomes a totally split covering, for which exactness is obvious.  $\square$

### 3 Variations on the results of Prasad and Raghunathan.

This section has a threefold purpose:

1. We recall the construction of the graded algebras associated with parahoric subgroups over either a local field or its maximal unramified extension. (We follow Prasad and Raghunathan's treatment [PR84].)
2. Using [PR84], we make a connection between the graded algebras associated with various parahoric subgroups (see Corollary 11).
3. As another corollary of the results of [PR84], we give the precise structure of the graded algebra associated with the "largest" parahoric subgroup (see Corollary 13).

As it was pointed out in the introduction, these results play a crucial role in finding the rate of growth of  $\rho_x(G)$  and the subgroup growth of any lattice in  $G$  (see Section 5.2). As the nature of this section is completely different from the rest of the article, reader can easily skip it and return to the mentioned corollaries whenever needed.

#### 3.1 Root system related notations.

Let  $\mathbb{G}$  be an absolutely simple, simply connected algebraic group defined over  $K$ . Let  $\mathbb{T}$  be a maximal  $\widehat{K}$ -split torus defined over  $K$ , such a torus exists as part of Bruhat-Tits theory [T79]. Let  $\widehat{\mathbb{T}}$  be the centralizer of  $\mathbb{T}$  which is also a torus defined over  $K$  as  $\mathbb{G}$  is quasi-split over  $\widehat{K}$  and  $\mathbb{T}$  is defined over  $K$ . Let  $\Phi = \Phi(\mathbb{T})$  be the  $\widehat{K}$ -root system of  $\mathbb{G}$  with respect to  $\mathbb{T}$ ,  $\mathbb{B}$  a Borel subgroup defined over  $\widehat{K}$  containing the centralizer of  $\mathbb{T}$ ,  $\Phi^+$  the set of positive roots in  $\Phi$  with respect to this ordering,  $\Pi$  the basis with respect to this ordering,  $\Phi^\bullet$  the set of non-divisible roots of  $\Phi$ ,  $\Phi^{\bullet\bullet}$  the set of non-multipliable roots in  $\Phi$ . Let  $\widehat{L}$  be the smallest Galois extension of  $\widehat{K}$  over which  $\widehat{\mathbb{T}}$  splits. Galois group of  $\widehat{L}$  over  $\widehat{K}$  acts on  $X^*(\widehat{\mathbb{T}})$  the group of characters of  $\widehat{\mathbb{T}}$ , and it is well-known that there are correspondences between  $\text{Gal}(\widehat{L}/\widehat{K})$ -orbits of  $\Phi(\widehat{\mathbb{T}})$ , restriction of these roots to  $\mathbb{T}$ , and  $\Phi$ . In particular, for any  $\phi \in \Phi$ , there is  $\widehat{\phi}$  a root in  $\Phi(\widehat{\mathbb{T}})$  whose restriction to  $\mathbb{T}$  is  $\phi$ . Let  $\widehat{K} \subseteq \widehat{L}_\phi$  be the smallest subfield of  $\widehat{L}$  such that  $\widehat{\phi}$  is defined over  $\widehat{L}_\phi$ . Let  $r = \text{lcm}_{\phi \in \Phi} [\widehat{L}_\phi : \widehat{K}]$  and  $r_\phi = r / [\widehat{L}_\phi : \widehat{K}]$ .



### 3.2 Affine functions and inner product.

Let  $V = X_*(\mathbb{T}) \otimes_{\mathbb{Z}} \mathbb{R}$  and  $V^* = X^*(\mathbb{T}) \otimes_{\mathbb{Z}} \mathbb{R}$  be its dual. Let  $\langle \cdot, \cdot \rangle$  be a Weyl group-invariant positive definite inner product on  $V^*$  such that in case the root system  $\Phi$  is reduced and contains roots of unequal lengths, any short root has length  $\sqrt{2}$  (we are using the same description of inner product as in [PR84]). Let  $\langle \cdot, \cdot \rangle$  also denote its extension to  $V^* \times \mathbb{R}$  the space of all affine functions on  $V$  (inner product of two affine functions is the inner product of their gradient i.e. the  $V^*$ -component).

### 3.3 Explicit absolute affine roots.

Let  $\Psi \subset V^* \times \mathbb{R}$  be the set of (absolute) affine roots of  $\mathbb{G}$  relative to  $\mathbb{T}$ . If  $\mathbb{G}$  splits over  $\widehat{K}$ , then  $\Psi = \Phi \times \mathbb{Z}$ . If  $\mathbb{G}$  does not split over  $\widehat{K}$  but the  $\widehat{K}$ -root system  $\Phi$  is reduced, then  $\Psi^\vee = \Phi^\vee \times \mathbb{Z}$ , where  $\Psi^\vee = \{\frac{2\psi}{\langle \psi, \psi \rangle} \mid \psi \in \Psi\}$  and  $\Phi^\vee = \{\frac{2\phi}{\langle \phi, \phi \rangle} \mid \phi \in \Phi\}$ . If the  $\widehat{K}$ -root system is non-reduced, then  $\mathbb{G}/\widehat{K}$  is an outer form of type  $A_n$ , where  $n$  is even. In this case,

$$\Psi = \{(\phi, n) \mid n \in \mathbb{Z}, \phi \in \Phi^\bullet\} \cup \{(\phi, 2n+1) \mid n \in \mathbb{Z}, \phi \notin \Phi^\bullet\}.$$

We refer the reader to [PR84, Section 2.8] for details and further discussions.

### 3.4 Congruence subgroups of root groups.

For any  $\widehat{K}$ -root  $\phi$ , we let  $\mathbb{U}_\phi$  be the corresponding root subgroup. There is a natural filtration on the  $\widehat{K}$ -points of this group, coming from the discrete valuation of  $\widehat{K}$ . Using this filtration, for any affine function  $\psi = (\phi, s)$ , one can define  $U_\psi$  (sometimes denoted by  $U_{\phi, s}$ ) a subgroup of  $\mathbb{U}_\phi(\widehat{K})$ . We refer the reader to either [PR84, Section 2.3] or [MP94, Section 2.4] for details. Let  $\mathbb{G}_\phi$  be the group generated by  $\mathbb{U}_\phi$  and  $\mathbb{U}_{-\phi}$ ,  $\widehat{\mathbb{T}}_\phi = \mathbb{G}_\phi \cap \widehat{\mathbb{T}}$ ,  $\widehat{T}_0^\phi$  the maximal bounded subgroup of  $\widehat{\mathbb{T}}_\phi(\widehat{K})$ ,  $\widehat{T}_0$  the maximal bounded subgroup of  $\widehat{\mathbb{T}}(\widehat{K})$ , and for any positive integer  $s$ ,  $\widehat{T}_{s\delta}^\phi$  the congruence subgroups of  $\widehat{\mathbb{T}}(\widehat{K})$ , where  $\delta = (0, 1)$  is the constant function. Again we refer the reader to [PR84, Section 2.6] for the precise description of  $\widehat{T}_{s\delta}^\phi$ . Finally let  $\widehat{T}_{s\delta}$  be the group generated by  $\widehat{T}_{s\delta}^\phi$ 's for  $\phi \in \Phi$ .

### 3.5 Iwahori subgroup and explicit absolute affine basis.

Let  $\widehat{I}$  be an Iwahori subgroup of  $\mathbb{G}(\widehat{K})$  which is stable under the action of the Galois group of  $\widehat{K}$  over  $K$ , and  $I = \mathbb{G}(K) \cap \widehat{I}$ . By changing the Borel subgroup  $\mathbb{B}$  if needed we can assume that the product mapping

$$\prod_{\phi \in \Phi^\bullet \cap \Phi^+} U_{\phi, 0} \times \prod_{\phi \in \Phi^\bullet \cap \Phi^-} U_{\phi, r'_\phi} \times \widehat{T}_0 \rightarrow \widehat{I}$$

is bijective for every ordering of the factors of the product, where  $r'_\phi$  is the smallest number such that  $U_{\phi, r'_\phi}$  is a proper subgroup of  $U_{\phi, 0}$ . Having the

Iwahori subgroup, we get an ordering on  $\Psi$  the affine root system and a basis  $\Delta$ . The local index of  $\mathbb{G}/K$  consists of the Dynkin diagram of  $\Delta$ , together with the action of the Galois group of  $\widehat{K}$  over  $K$ . If  $\mathbb{G}$  splits over  $\widehat{K}$ ,

$$\Delta = \{(\alpha, 0) \mid \alpha \in \Pi\} \cup \{(-\rho, 1)\},$$

where  $\rho$  is the highest root in  $\Phi$ . In this case, let  $\psi_s = (-\rho, 1)$ . If  $\mathbb{G}$  does not split over  $\widehat{K}$  but its  $\widehat{K}$ -root system is not reduced, then

$$\Delta = \{(\alpha, 0) \mid \alpha \in \Pi\} \cup \{(-\rho_m, 1)\},$$

where  $\rho_m$  is the dominant short root in  $\Phi$ . In this case, let  $\psi_s = (-\rho_m, 1)$ . If  $\Phi$  is non-reduced, then

$$\Delta = \{(\alpha, 0) \mid \alpha \in \Pi\} \cup \{(-2\phi_m, 1)\},$$

where  $\phi_m$  is the unique multipliable root in  $\Pi$ . In this case, let  $\psi_s = (-2\phi_m, 1)$ .

### 3.6 Standard parahoric subgroups.

For any  $\Xi \subseteq \Delta$ , let  $\widehat{P}_\Xi$  be the associated standard parahoric, i.e. the subgroup of  $\mathbb{G}(\widehat{K})$  which is generated by  $\widehat{I}$  and  $U_\alpha$  for any  $\alpha \in \Delta \setminus \Xi$ . If  $\widehat{P}_\Xi$  is invariant under the action of  $Gal(\widehat{K}/K)$  the Galois group, then it is said to be defined over  $K$  and we denote  $\mathbb{G}(K) \cap \widehat{P}_\Xi$  the set of its  $K$ -rational points by  $P_\Xi$ . This happens if and only if  $\Xi$  is invariant under the action of  $Gal(\widehat{K}/K)$ . Let us recall that any parahoric subgroup is conjugate to one and only one of these standard parahorics (one can consider this as a definition of a parahoric subgroup). A parahoric subgroup of  $\mathbb{G}(\widehat{K})$  (resp.  $\mathbb{G}(K)$ ) is called of type  $\Xi \subseteq \Delta$  if it is conjugate to  $\widehat{P}_\Xi$  (resp.  $P_\Xi$ ).

### 3.7 Filtrations of parahoric subgroups.

Following notations of [PR84], let  $m_\alpha$  be the uniquely determined positive integers such that

$$\sum_{\alpha \in \Delta} m_\alpha \alpha = \delta,$$

where  $\delta$  is the constant function  $(0, 1)$ . For any  $\Xi \subseteq \Delta$  and affine function  $\psi$ , let

$$l_\Xi(\psi) = \sum_{\alpha \in \Xi} t_\alpha,$$

where  $\psi = \sum_{\alpha \in \Delta} t_\alpha \alpha$ . Using  $l_\Xi$ , we can define congruence subgroups of  $\widehat{P} = \widehat{P}_\Xi$  (resp.  $P = P_\Xi$ ). More precisely, let  $\widehat{P}_t$  be the subgroup of  $\widehat{P}$  generated by  $U_\psi$  with  $l_\Xi(\psi) \geq t$  and  $\widehat{T}_{s\delta}$  where  $s$  is the smallest integer greater than or equal to  $t/l_\Xi(\delta)$ . If  $\Xi$  is  $Gal(\widehat{K}/K)$  invariant, then we set  $P_t = \widehat{P}_t \cap \mathbb{G}(K)$ .

### 3.8 Associated graded Lie algebras.

Let  $\widehat{P} = P_{\Xi}$  be a standard parahoric subgroup of  $\mathbb{G}(\widehat{K})$ . For any natural number  $t$ , let  $\mathfrak{L}_t^{\Xi} = \widehat{P}_t/\widehat{P}_{t+1}$ . When there is no ambiguity, we simply write  $\mathfrak{L}_t$ . For any natural number  $t$ ,  $\mathfrak{L}_t$  is a finite dimensional  $\mathfrak{F}$ -vector space. Let

$$\mathfrak{L}_{\Xi} = \bigoplus_{i=1}^{\infty} \mathfrak{L}_i^{\Xi},$$

and consider it as a graded  $\mathfrak{F}$ -Lie algebra via the following definition:

$$[g_i \widehat{P}_{i+1}, g_j \widehat{P}_{j+1}] := (g_i, g_j) \widehat{P}_{i+j+1},$$

for any natural numbers  $i, j$ ,  $g_i$  in  $\widehat{P}_i$  and  $g_j$  in  $\widehat{P}_j$ , where  $(g, h) = ghg^{-1}h^{-1}$ . When  $\Xi$  is  $Gal(\widehat{K}/K)$  invariant, we also consider the described filtration of  $P = P_{\Xi}$ . For any natural number  $t$ , let  $L_t^{\Xi} = P_t/P_{t+1}$ . Again if there is no ambiguity, we simply write  $L_t$ . One can view  $L_t$  as a finite subgroup of  $\mathfrak{L}_t$ . Indeed in this case,  $Gal(\widehat{K}/K) = Gal(\mathfrak{F}/\mathfrak{f})$  acts semi-linearly on  $\mathfrak{L}_t$ . Thus we get  $\mathfrak{L}_t(\mathfrak{f})$  an  $\mathfrak{f}$ -structure on  $\mathfrak{L}_t$  and one can show that, in fact,  $\mathfrak{L}_t(\mathfrak{f})$  can be identified with  $L_t$ . Therefore the graded  $\mathfrak{f}$ -Lie algebra

$$L_{\Xi} = \bigoplus_{i=1}^{\infty} L_i^{\Xi},$$

can be considered as an  $\mathfrak{f}$ -structure on  $\mathfrak{L}_{\Xi}$ . We refer the reader to [PR84, Sections 2.16, 2.18, 2.23, 2.24]. G. Prasad and M. S. Raghunathan [PR84, Section 2.19, 2.20] give a ‘‘Chevalley basis’’ of  $\mathfrak{L}_{\Xi}$ . For any absolute affine root  $\psi$ , they introduce an element  $X_{\psi}$ , and for a given  $\beta$  in  $\Phi$  and a natural number  $s$  which is divisible by  $r_{\beta}$ , they give an element  $H_{s\delta}^{\beta}$ . They prove that

$$\{X_{\psi} \mid l_{\Xi}(\psi) \geq 1\} \cup \{H_{s\delta}^{\alpha} \mid \alpha \in \Pi, s > 0, r_{\alpha} \mid s\} \quad (1)$$

is an  $\mathfrak{F}$ -vector space basis of  $\mathfrak{L}_{\Xi}$ . They also show that  $\mathfrak{L}_t^{\Xi}$  is spanned by

$$\{X_{\psi} \mid l_{\Xi}(\psi) = t\} \cup \{H_{s\delta}^{\alpha} \mid \alpha \in \Pi, r_{\alpha} \mid s, sl_{\Xi}(\delta) = t\}. \quad (2)$$

Further they give the following relations between the elements of this basis:

- 1- Let  $\psi, \eta \in \Psi$  with  $l_{\Xi}(\psi), l_{\Xi}(\eta) \geq 1$ , such that  $\psi + \eta$  is not a constant. Then

$$[X_{\psi}, X_{\eta}] = 0 \quad \text{if } \psi + \eta \notin \Psi.$$

- 2- Let  $\psi, \eta \in \Psi$  such that  $\psi - \eta \in \Psi$  and  $l_{\Xi}(\psi - \eta), l_{\Xi}(\eta) \geq 1$ . Then

$$[X_{\eta}, X_{\psi - \eta}] = \pm n X_{\psi},$$

where  $n$  is the largest positive integer such that  $\psi - n\eta$  is in  $\Psi$ .

- 3- Let  $\psi = (\alpha, s), \eta = (-\alpha, s') \in \Psi$  and  $l_{\Xi}(\psi), l_{\Xi}(\eta) \geq 1$ . Then

$$[X_{\psi}, X_{\eta}] = \begin{cases} \pm H_{(s+s')\delta}^{\alpha} & \text{if } \alpha \in \Phi^{\bullet\bullet}, \\ \pm 2H_{(s+s')\delta}^{\alpha} & \text{if } \alpha \in \Phi \setminus \Phi^{\bullet\bullet}. \end{cases}$$

Moreover, for any positive integral multiple  $s''$  of  $r_\alpha$ ,

$$[H_{s''\delta}^\alpha, X_\psi] = \begin{cases} 2X_{\psi+s''\delta} & \text{if } \alpha \in \Phi^{\bullet\bullet}, \\ (2 - (-1)^{s''})X_{\psi+s''\delta} & \text{if } \alpha \in \Phi \setminus \Phi^{\bullet\bullet}. \end{cases}$$

- 4- Let  $\psi = (\alpha, s) \in \Psi$  and  $l_\Xi(\psi) \geq 1$ ,  $\beta \in \Phi$ ,  $\beta \neq \pm\alpha$ , and  $r_\beta | s$ . Then  $[H_{s\delta}^\beta, X_\psi]$  is an integral multiple of  $X_{\psi+s\delta}$ . Moreover, in case  $r | \text{char}(\mathfrak{f})r_\alpha s$ ,

$$[H_{s\delta}^\beta, X_\psi] = \begin{cases} \frac{2\langle\beta, \alpha\rangle}{\langle\beta, \beta\rangle} X_{\psi+s\delta} & \text{if } r_\alpha | s \text{ and } \beta \in \Phi^{\bullet\bullet}, \\ \frac{\langle\beta, \alpha\rangle}{\langle\beta, \beta\rangle} X_{\psi+s\delta} & \text{if } r_\alpha | s \text{ and } \beta \in \Phi \setminus \Phi^{\bullet\bullet}, \\ 0 & \text{if } r_\alpha \nmid s. \end{cases}$$

- 5- For any  $\beta \in \Phi$ ,  $H_{s\delta}^\beta = -H_{s\delta}^{-\beta}$ , and  $H_{2s\delta}^\beta = H_{2s\delta}^{2\beta}$  if  $\beta$  is a multipliable root, and all elements of the form  $H_{s\delta}^\beta$  commute with each other.
- 6- Let  $\beta = \sum_{\alpha \in \Pi} n_\alpha \alpha \in \Phi$ . Then in case  $r | s$ ,

$$H_{s\delta}^\beta = \begin{cases} \sum_{\alpha \in \Pi} \frac{n_\alpha \langle\alpha, \alpha\rangle}{\langle\beta, \beta\rangle} (1 + \sigma(\alpha)) H_{s\delta}^\alpha & \text{if } \beta \in \Phi^{\bullet\bullet}, \\ \sum_{\alpha \in \Pi} \frac{n_\alpha \langle\alpha, \alpha\rangle}{2\langle\beta, \beta\rangle} (1 + \sigma(\alpha)) H_{s\delta}^\alpha & \text{otherwise.} \end{cases}$$

where  $\sigma(\alpha)$  is the  $\mathbb{R}$ -valued linear functional on  $V^*$  which is identically zero in case  $\Phi$  is reduced; otherwise, it takes 1 at the unique multipliable root in  $\Pi$  and 0 at all the other elements of  $\Pi$ .

- 7- If  $r \nmid s$  and  $\beta = \sum_{\alpha \in \Pi} n_\alpha \alpha$  is a short positive root, then

$$H_{s\delta}^\beta = (-1)^{rn(\beta)} \sum_{\alpha' \in \Phi'(\beta)} H_{s\delta}^{\alpha'},$$

where  $\Phi'(\beta) = \{\alpha' \in \Pi \mid \alpha' \text{ is short, } r \nmid n_{\beta'}\}$  and  $n(\beta) = \sum_{\alpha \text{ short}} n_\alpha$ .

**Remark 10.** In number 4, in general, the integral coefficient just depends on  $\alpha$ ,  $\beta$  and  $s l_\Xi(\delta) \pmod{r}$ .

**Corollary 11** (Comparison). *Let  $\Xi \subseteq \Delta$ .  $\mathfrak{L}_\Xi$  can be naturally embedded into  $\mathfrak{L}_\Delta$  as a subalgebra of codimension at most  $\dim \mathbb{G}$ .*

*Proof.* Clearly  $l_\Xi(\psi) \leq l_\Delta(\psi)$  for any  $\Xi \subseteq \Delta$  and  $\psi \in \Psi$ . Thus, by the above commutation relations,  $\mathfrak{L}_\Xi$  can be viewed as a subalgebra of  $\mathfrak{L}_\Delta$ . The codimension assertions are direct consequence of the fact that there are at most  $\dim \mathbb{G}$  many  $\psi \in \Psi$  such that  $l_\Xi(\psi) = 0$ .

It should be also clarified that the choice of signs in the commutative relations 2 and 3 are inherited from the group structure and so they are the same in both of the Lie algebras.  $\square$

**Remark 12.** First we remark that  $\mathfrak{H}$ , in the above argument, only lacks the first grade of  $\mathfrak{L}_\Xi$ . Second we emphasize that this embedding is only at the level of Lie algebras and not graded Lie algebras. Via this embedding, we change the grading, drastically.

**Corollary 13** (Special graded Lie algebras). *Let  $\psi_s$  be as in 3.5. Then*

- 1-  $\mathfrak{L}_{\{\psi_s\}} \simeq \mathfrak{g}(\mathfrak{F}) \otimes_{\mathfrak{F}} t \mathfrak{F}[t]$  if  $\mathbb{G}$  splits over  $\widehat{K}$ ,
- 2-  $\mathfrak{L}_{\{\psi_s\}} \simeq \bigoplus_{i=1}^{\infty} \mathfrak{g}_{i(\bmod r)} \otimes t^i$  if  $\mathbb{G}$  does not split over  $\widehat{K}$  and  $\Phi$  is reduced,
- 3-  $\mathfrak{L}_{\{\psi_s\}} \simeq \bigoplus_{i=1}^{\infty} \mathfrak{g}_{i(\bmod 2)} \otimes t^i$  if  $\Phi$  is non-reduced,

where  $\mathfrak{g}(\mathfrak{F}) = \mathfrak{g}_0$  is the split simple Lie algebra of type  $\Phi^\bullet$ , and  $\widehat{\mathfrak{g}} = \bigoplus_{i=0}^{r-1} \mathfrak{g}_i$  is a perfect  $\mathbb{Z}/r\mathbb{Z}$ -graded algebra if  $\text{char}(\mathfrak{F})$  is bigger than all the entries of the Cartan matrix of  $\Phi$ .

*Proof.* Because of the way, we chose  $\psi_s$ , one can see that  $l_{\{\psi_s\}}((\phi, n)) = n$ ; in particular,  $l_{\{\psi_s\}}(\delta) = 1$ . First assume that  $\Phi$  is reduced, and let

$$\{x_\phi | \phi \in \Phi\} \cup \{h_\alpha | \alpha \in \Pi\}$$

be the Chevalley basis associated to the root system  $\Phi$  and  $\mathfrak{g}$  the corresponding Lie algebra. Then by the above commutation relations and those of the Chevalley basis, one can easily see that the map

$$x_\phi \otimes t^n \mapsto X_{(\phi, n)} \quad \& \quad h_\alpha \otimes t^n \mapsto H_{n\delta}^\alpha,$$

where  $r|n$ , extends to a graded Lie algebra isomorphism between  $\bigoplus_{n=1}^{\infty} \mathfrak{g}(\mathfrak{F}) \otimes t^{rn}$  and  $\bigoplus_{n=1}^{\infty} \mathfrak{L}_{rn}^{\{\psi_s\}}$ . In particular, when  $\mathbb{G}$  splits over  $\widehat{K}$ ,  $r = 1$  and

$$\mathfrak{L}_{\{\psi_s\}} \simeq \mathfrak{g}(\mathfrak{F}) \otimes_{\mathfrak{F}} t \mathfrak{F}[t].$$

If  $\Phi$  is non-reduced, then by the above commutation relations and those of the Chevalley basis, we can see that the following map

$$\begin{cases} x_\phi \otimes t^n \mapsto X_{(\phi, n)} & \text{if } 2|n, \\ h_\alpha \otimes t^n \mapsto H_{n\delta}^\alpha & \text{if } 2|n \text{ and } \alpha \in \Pi \cap \Phi^{\bullet\bullet}, \\ h_\alpha \otimes t^n \mapsto 2H_{n\delta}^\alpha & \text{if } 2|n \text{ and } \alpha \in \Pi \setminus \Phi^{\bullet\bullet}, \end{cases}$$

extends to a graded Lie algebra isomorphism between  $\bigoplus_{n=1}^{\infty} \mathfrak{g}(\mathfrak{F}) \otimes t^{2n}$  and  $\bigoplus_{n=1}^{\infty} \mathfrak{L}_{2n}^{\{\psi_s\}}$ , where  $\mathfrak{g}$  is the Chevalley Lie algebra of type  $\Phi^\bullet$  and

$$\{x_\phi | \phi \in \Phi^\bullet\} \cup \{h_\alpha | \alpha \in \Pi\}$$

is a Chevalley basis of  $\mathfrak{g}$ . (By our assumption,  $\text{char}(\mathfrak{F}) \neq 2$ .)

We notice that all the commutation relations depend on the gradient part of the affine roots and the constant parts modulo  $r$ . In particular,  $\mathfrak{L}_i^{\{\psi_s\}}$  can be

naturally identified with  $\mathfrak{L}_j^{\{\psi_s\}}$  if  $i \equiv j \pmod{r}$ , and, via this identification, we get a  $\mathfrak{g}(\mathfrak{F})$ -module structure on all of them. Indeed, by the same argument, we get  $\widehat{\mathfrak{g}}$ , a  $\mathbb{Z}/r\mathbb{Z}$ -graded Lie algebra, such that

$$\mathfrak{L}_{\{\psi_s\}} \simeq \bigoplus_{i=1}^{\infty} \mathfrak{g}_{i \pmod{r}} \otimes t^i.$$

More precisely, if  $\Phi$  is reduced, then let

$$\{x_{(\phi,i)} | \phi \text{ short root}\} \cup \{h_{(\alpha,i)} | \alpha \in \Pi, \alpha \text{ short root}\},$$

be a basis of  $\mathfrak{g}_i$  for  $1 \leq i \leq r-1$ ,  $\mathfrak{g}_0 = \mathfrak{g}(\mathfrak{F})$ ,

$$\{x_{(\phi,0)} | \phi \in \Phi\} \cup \{h_{(\alpha,0)} | \alpha \in \Pi\}$$

a Chevalley basis of  $\mathfrak{g}$  of type  $\Phi$ , and

$$\overline{\Psi} = \Phi \times \{0\} \cup \bigcup_{i=1}^{r-1} \{(\phi,i) | \phi \text{ short root}\}.$$

If  $\Phi$  is non-reduced, then let

$$\{x_{(\phi,1)} | \phi \in \Phi\} \cup \{h_{(\alpha,1)} | \alpha \in \Pi\},$$

be a basis of  $\mathfrak{g}_1$ ,  $\mathfrak{g}_0 = \mathfrak{g}(\mathfrak{F})$ ,

$$\{x_{(\phi,0)} | \phi \in \Phi^\bullet\} \cup \{h_{(\alpha,0)} | \alpha \in \Pi\}$$

a Chevalley basis of  $\mathfrak{g}$  of type  $\Phi^\bullet$ , and

$$\overline{\Psi} = \{(\phi,0) | \phi \in \Phi^\bullet\} \cup \Phi \times \{1\}.$$

Then define the commutation relations between the elements of this chosen basis, by looking at those of  $\mathfrak{L}_{\{\psi_s\}}$  and modifying the constant parts of affine roots modulo  $r$ . (Since  $r_\phi$ 's are either 1 or  $r$ , there will not be any ambiguity.)

The isomorphisms are direct results of the way we defined  $\widehat{\mathfrak{g}}$ , and the perfectness of  $\widehat{\mathfrak{g}}$  is a consequence of the commutation relations coupled with our assumption on the characteristic of  $\mathfrak{F}$ .  $\square$

## 4 Counting maximal lattices in $G$ .

### 4.1 Description of maximal lattices.

Let  $\Gamma$  be a maximal lattice in  $G = \mathbb{G}_0(K)$ . By Margulis' arithmeticity [M91] and Rohlfs' maximality criteria [BP89, Proposition 2.9], there are a function field  $k$ ,  $\mathfrak{p}_0 \in V_k$ , a simply connected absolutely almost simple  $k$ -group  $\mathbb{G}$ , and a family of parahoric subgroups  $\{P_{\mathfrak{p}}\}$  of  $\mathbb{G}(k_{\mathfrak{p}})$  for any  $\mathfrak{p} \in V_k^\circ = V_k \setminus \{\mathfrak{p}_0\}$  such that

- 1-  $k_{\mathfrak{p}_0} \simeq K$ .
- 2-  $\mathbb{G} \simeq \mathbb{G}_0$  over  $K$  after identifying it with  $k_{\mathfrak{p}_0}$ .
- 3-  $\{P_{\mathfrak{p}}\}$  is a coherent family of parahoric subgroups, i.e.  $\mathbb{G}(k_{\mathfrak{p}_0}) \cdot \prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}$  is an open subgroup of  $\mathbb{G}(\mathbb{A}_k)$ .
- 4-  $\Gamma = N_G(\Lambda)$ , where  $\Lambda = \mathbb{G}(k) \cap \prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}$  is a principal congruence subgroup.
- 5- The following is a short exact sequence:

$$1 \rightarrow \mu(k_{\mathfrak{p}_0})/\mu(k) \rightarrow \Gamma/\Lambda \rightarrow \delta(\mathbb{G}(k))_{\Theta^\circ} \rightarrow 1,$$

where  $\mu$  is the center of  $\mathbb{G}$ ,  $\delta$  is the boundary map in the exact sequence

$$1 \rightarrow \mu(k) \rightarrow \mathbb{G}(k) \rightarrow \overline{\mathbb{G}}(k) \xrightarrow{\delta} H^1(k, \mu),$$

and  $\delta(\overline{\mathbb{G}}(k))_{\Theta^\circ}$  is the subgroup of  $\delta(\overline{\mathbb{G}}(k))$  which preserves  $\Theta^\circ = \{\Theta_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^\circ}$  the type of parahoric subgroups  $P_{\mathfrak{p}}$  (See [BP89, Section 2]).

## 4.2 Covolume of a principal congruence subgroup.

Here we will recall the main result of G. Prasad from [Pr89]. The notations are the same as in 4.1.

For any  $\mathbb{G}$  and  $k$  as above, there is a unique quasi-split  $k$ -group  $\mathcal{G}$  which is an inner  $k$ -form of  $\mathbb{G}$ . Let  $l$  be either a degree two or a degree three extension of  $k$  over which  $\mathcal{G}$  splits if it is not of type  $D_4^{(6)}$ . It is a Galois extension of  $k$  or the unique degree three extension of  $k$  in a degree 6 Galois extension of  $k$ , respectively when  $\mathbb{G}$  is not a  $k$  form of type  $D_4^{(6)}$  or it is. Because of the uniqueness of  $\mathcal{G}$ , it is determined by its absolute type,  $k$  and  $l$ . Let

$$\mathfrak{s} = \mathfrak{s}(\mathcal{G}) = \begin{cases} 0 & \text{if } \mathcal{G} \text{ is } k\text{-split,} \\ \frac{1}{2}(r-1)(r+2) & \text{if } \mathcal{G} \text{ is an outer form of type } A_r \text{ with } r \text{ odd,} \\ \frac{1}{2}r(r+3) & \text{if } \mathcal{G} \text{ is an outer form of type } A_r \text{ with } r \text{ even,} \\ 2r-1 & \text{if } \mathcal{G} \text{ is an outer form of type } D_r, \\ 26 & \text{if } \mathcal{G} \text{ is an outer form of type } E_6. \end{cases}$$

Also let

$$B(\mathcal{G}) = q_k^{(g_k-1)\dim \mathcal{G}} \left( \frac{q_l^{g_l-1}}{q_k^{(g_k-1)[l:k]}} \right)^{\mathfrak{s}}.$$

For any  $\mathfrak{p} \in V_k$ , let  $\mathcal{P}_{\mathfrak{p}}$  be a parahoric subgroup of  $\mathcal{G}(k_{\mathfrak{p}})$  chosen as in [Pr89, Section 1]. Let us recall that these parahoric subgroups have maximum volume among all the parahoric subgroups of  $\mathcal{G}(k_{\mathfrak{p}})$ , (as a consequence) always are special parahoric subgroups (and hyper-special whenever possible), and  $\prod_{\mathfrak{p} \in V_k} \mathcal{P}_{\mathfrak{p}}$

is an open compact subgroup of  $\mathcal{G}(\mathbb{A}_k)$ .

For any  $\mathfrak{p} \in V_k$ , Bruhat-Tits theory provides us  $\mathbb{G}_{\mathfrak{p}}$  and  $\mathcal{G}_{\mathfrak{p}}$  two smooth affine group schemes over  $\mathcal{O}_{\mathfrak{p}}$ , such that

- 1- The generic fibers of  $\mathbb{G}_{\mathfrak{p}}$  and  $\mathcal{G}_{\mathfrak{p}}$  are isomorphic to  $\mathbb{G}$  and  $\mathcal{G}$  over  $k_{\mathfrak{p}}$ , respectively.
- 2- The  $\mathcal{O}_{\mathfrak{p}}$  points of  $\mathbb{G}_{\mathfrak{p}}$  and  $\mathcal{G}_{\mathfrak{p}}$  are isomorphic with  $P_{\mathfrak{p}}$  and  $\mathcal{P}_{\mathfrak{p}}$ , respectively.

Let  $\overline{\mathbb{M}}_{\mathfrak{p}}$  and  $\overline{\mathcal{M}}_{\mathfrak{p}}$  be a fixed maximal reductive subgroups of the special fibers of  $\mathbb{G}_{\mathfrak{p}}$  and  $\mathcal{G}_{\mathfrak{p}}$ , respectively. Let  $P_{\mathfrak{p}_0}$  be a parahoric subgroup of  $\mathbb{G}(k_{\mathfrak{p}_0})$  with maximum volume among all parahoric subgroups, and  $\text{vol}$  be the Haar measure on  $\mathbb{G}(k_{\mathfrak{p}_0})$  such that  $\text{vol}(P_{\mathfrak{p}_0}) = 1$ . Let

$$e(\mathfrak{p}) = \frac{q_{\mathfrak{p}}^{(\dim \overline{\mathbb{M}}_{\mathfrak{p}} + \dim \overline{\mathcal{M}}_{\mathfrak{p}})/2}}{\#\overline{\mathbb{M}}_{\mathfrak{p}}(\mathfrak{f}_{\mathfrak{p}})}, e_{qs}(\mathfrak{p}) = \frac{q_{\mathfrak{p}}^{\dim \overline{\mathcal{M}}_{\mathfrak{p}}}}{\#\overline{\mathcal{M}}_{\mathfrak{p}}(\mathfrak{f}_{\mathfrak{p}})}, \text{ and } e'(\mathfrak{p}) = \frac{e(\mathfrak{p})}{e_{qs}(\mathfrak{p})}.$$

Whenever  $P_{\mathfrak{p}}$  is a hyper-special parahoric subgroup,  $e'(\mathfrak{p}) = 1$ . So for almost every  $\mathfrak{p}$ , we have  $e'(\mathfrak{p}) = 1$ . Let  $Z(\mathcal{G}) = \prod_{\mathfrak{p} \in V_k} e_{qs}(\mathfrak{p})$ . It is clear that  $Z(\mathcal{G})$  is larger than 1. Prasad's main theorem in [Pr89] says that

**Theorem 14** ([Pr89]). *Following the above notations,*

$$\text{vol}(G/\Lambda) = \tau_k(\mathbb{G})B(\mathcal{G})Z(\mathcal{G}) \prod_{\mathfrak{p} \in V_k} e'(\mathfrak{p}),$$

where  $\tau_k(\mathbb{G})$  is the Tamagawa number of  $\mathbb{G}/k$ .

**Remark 15.** A. Weil conjectured that, if  $\mathbb{G}$  is simply connected, absolutely almost simple,  $k$ -group, then  $\tau_k(\mathbb{G}) = 1$ . This conjecture is proved in most of the cases. However it is still open for some twisted forms of type A and most of the exceptional types.

**Remark 16.** In the rest of this article, we will assume that Weil's conjecture holds. Indeed, what we need is only a uniform lower bound for the Tamagawa numbers.

### 4.3 Lower bound on $\text{vol}(G/\Gamma)$ and local factors.

In this section, we will summarize and adapt some of the results of A. Borel and G. Prasad from [BP89], and then give a lower bound on the covolume of  $\Gamma$ . Following them, let

$$\varepsilon = \varepsilon(\mathbb{G}) = \begin{cases} 2 & \text{if } \mathbb{G} \text{ is of type } D_r \text{ with } r \text{ even,} \\ 1 & \text{otherwise.} \end{cases}$$



Let  $t$  be the exponent of  $\mu$ , i.e.

$$t = t(\mathbb{G}) = \begin{cases} r+1 & \text{if } \mathbb{G} \text{ is of type } A_r, \\ 2 & \text{if } \mathbb{G} \text{ is of type } B_r, C_r, D_r \text{ with } r \text{ even, or } E_7, \\ 3 & \text{if } \mathbb{G} \text{ is of type } E_6, \\ 4 & \text{if } \mathbb{G} \text{ is of type } D_r \text{ with } r \text{ odd,} \\ 1 & \text{if } \mathbb{G} \text{ is of type } E_8, F_4 \text{ or } G_2. \end{cases}$$

By the definition,  $\varepsilon$  and  $t$  just depend on the absolute type of  $\mathbb{G}$ , and so, in particular, they are completely determined by  $G$ .

For any  $\mathfrak{p}$ ,  $H^1(k, \mu)$  acts on  $\mathcal{D}_{\mathfrak{p}}$  the local Dynkin diagram of  $\mathbb{G}/k_{\mathfrak{p}}$ . Let  $\xi_{\mathfrak{p}}$  be the induced homomorphism to the group of isometries of the local Dynkin diagram and  $\Xi_{\mathfrak{p}}$  the subgroup of the image of  $\xi_{\mathfrak{p}}$  which preserves  $\Theta_{\mathfrak{p}}$ . Let  $\xi^{\circ} = (\xi_{\mathfrak{p}})_{\mathfrak{p} \in V_k^{\circ}}$ ,  $\xi = (\xi_{\mathfrak{p}})_{\mathfrak{p} \in V_k}$ ,  $H^1(k, \mu)_{\xi^{\circ}} = \ker \xi^{\circ}$ , and  $H^1(k, \mu)_{\xi} = \ker \xi$ . So it is clear that

$$\#\delta(\mathbb{G}(k))_{\Theta^{\circ}} \leq \#H^1(k, \mu)_{\xi^{\circ}} \cdot \prod_{\mathfrak{p} \in V_k^{\circ}} \#\Xi_{\mathfrak{p}} \leq \#H^1(k, \mu)_{\xi} \cdot \prod_{\mathfrak{p} \in V_k} \#\Xi_{\mathfrak{p}} \cdot \#\text{Aut } \mathcal{D}_{\mathfrak{p}_0}.$$

We note that  $\#\text{Aut } \mathcal{D}_{\mathfrak{p}_0}$  just depends on  $G$ .

So, by Theorem 14 and the short exact sequence given in 4.1, we have that

$$\text{vol}(G/\Gamma) \geq c_4 B(\mathcal{G}) \cdot t^{-\varepsilon} (\#H^1(k, \mu)_{\xi})^{-1} \prod_{\mathfrak{p} \in V_k} \frac{e(\mathfrak{p})}{\#\Xi_{\mathfrak{p}}}.$$

On the other hand, by virtue of [BP89, Proposition 5.1, Proposition 5.6], (note that  $H^1(k, C)_{\xi}$  in [BP89] is denoted by  $H^1(k, \mu)_{\xi^{\circ}}$  in our paper) we have

**Proposition 17.** *In the above setting,*

$$\#H^1(k, \mu)_{\xi} \leq \begin{cases} c_5 h_k^{\varepsilon} t^{\varepsilon} \#T(\mathbb{G}) & \text{if } \mathcal{G} \text{ splits over } k, \\ c_5 h_l 4^{\#T(\mathbb{G})} \cdot \frac{q_l^{2(g_l-1)}}{q_k^{2(g_k-1)[l:k]}} & \text{if } \mathbb{G} \text{ is of type } D_r \text{ with } r \text{ even,} \\ c_5 h_l t^{\#T(\mathbb{G})} & \text{otherwise,} \end{cases}$$

where we assume  $\mathcal{G}$  does not split over  $k$  in the second and the third cases,  $c_5$  is a constant depending on  $G$ ,

$$T(\mathbb{G}) = \{\mathfrak{p} \in V_k \mid \mathbb{G} \text{ splits } / \widehat{k}_{\mathfrak{p}} \text{ and } \mathbb{G} \text{ is not quasi-split } / k_{\mathfrak{p}}\},$$

and  $h_k$  (resp.  $h_l$ ) is the class number of  $k$  (resp.  $l$ ).

From the above discussions, we have

**Proposition 18.** *In the above setting,*

$$\text{vol}(G/\Gamma) \geq c_6 \cdot q_k^{(g_k-1) \dim \mathcal{G}} \cdot h_l^{-\varepsilon'} \cdot \left( \frac{q_l^{(g_l-1)}}{q_k^{(g_k-1)[l:k]}} \right)^{s'(\mathcal{G})} \prod_{\mathfrak{p} \in V_k} f(\mathfrak{p}),$$

where  $c_6$  just depends on  $G$ ,  $\varepsilon' = 1$  (resp.  $\varepsilon$ ) if  $l = k$  (resp. otherwise),  $\mathfrak{s}'(\mathcal{G}) = \mathfrak{s}(\mathcal{G}) - 2$  (resp.  $\mathfrak{s}(\mathcal{G})$ ) if  $G$  is of type  $D_r$  with  $r$  even (resp. otherwise), and

$$f(\mathfrak{p}) = \begin{cases} e(\mathfrak{p})/\#\Xi_{\mathfrak{p}} & \text{if } \mathfrak{p} \notin T(\mathbb{G}), \\ e(\mathfrak{p})/(\#\Xi_{\mathfrak{p}} \cdot t^\varepsilon) & \text{if } \mathfrak{p} \in T(\mathbb{G}). \end{cases}$$

Here, we would like to give a lower bound for the local factors associated to the “bad” primes.

**Proposition 19.** *There is a positive constant  $\sigma = \sigma(G)$  such that*

$$f(\mathfrak{p}) \geq q_{\mathfrak{p}}^\sigma$$

if either  $\mathbb{G}$  is not quasi-split over  $k_{\mathfrak{p}}$ ,  $P_{\mathfrak{p}}$  is not special, or  $\mathbb{G}$  is quasi-split over  $k_{\mathfrak{p}}$ ,  $\mathbb{G}$  splits over  $\widehat{k}_{\mathfrak{p}}$  and  $P_{\mathfrak{p}}$  is not hyper-special.

*Proof.* We will follow the proof given in the appendix C of [BP89], where Borel and Prasad essentially show that  $f(\mathfrak{p}) > 1$ , for any  $\mathfrak{p}$ .

We start with the case where  $\mathbb{G}$  is not quasi-split over  $k_{\mathfrak{p}}$ . For any such  $\mathfrak{p}$ , let  $P_{\mathfrak{p}}^m$  be a parahoric subgroup of  $\mathbb{G}(k_{\mathfrak{p}})$  of maximum volume such that  $P_{\mathfrak{p}} \cap P_{\mathfrak{p}}^m$  contains an Iwahori subgroup and whenever  $P_{\mathfrak{p}}$  is such a parahoric subgroup, we set them equal; then for almost all  $\mathfrak{p}$ ,  $P_{\mathfrak{p}} = P_{\mathfrak{p}}^m$ . It is proved in [BP89, Section 3] that

$$(\#\Xi_{\mathfrak{p}})^{-1}e(\mathfrak{p}) \geq e_m(\mathfrak{p}).$$

By [Pr89, proposition 2.10], for any such  $\mathfrak{p}$ ,

$$e_m(\mathfrak{p}) \geq \frac{q_{\mathfrak{p}}^{r_{\mathfrak{p}}+1}}{q_{\mathfrak{p}} + 1},$$

where  $r_{\mathfrak{p}}$  is the  $\widehat{k}_{\mathfrak{p}}$ -rank of  $\mathcal{G}$ . Now as it has been pointed out in [Be07, Section 4.3], the same proof as in the mentioned appendix gives us the claimed  $\sigma$ .

Now, assume that  $\mathbb{G}$  is quasi-split over  $k_{\mathfrak{p}}$ , it is split over  $\widehat{k}_{\mathfrak{p}}$ , and  $P_{\mathfrak{p}}$  is not hyper-special; then, by [Pr89, proposition 2.10],

$$e(\mathfrak{p}) \geq \frac{q_{\mathfrak{p}}^{r_{\mathfrak{p}}+1}}{q_{\mathfrak{p}} + 1}.$$

Since  $\mathbb{G}$  splits over  $\widehat{k}_{\mathfrak{p}}$  and  $\#\Xi_{\mathfrak{p}} \leq t^\varepsilon$ , the same argument works.

Finally assume that  $\mathbb{G}$  is quasi-split over  $k_{\mathfrak{p}}$  and not split over  $\widehat{k}_{\mathfrak{p}}$ , and  $P_{\mathfrak{p}}$  is not special. In this case,  $\mathbb{G}/k_{\mathfrak{p}}$  is a residually split group. By looking at the table of such groups in [T79], we see that local Dynkin diagrams of only two of

them have a non-trivial automorphism, for both of which we have  $\#\Xi_{\mathfrak{p}} \leq 2$  and  $r_{\mathfrak{p}} \geq 2$ . On the other hand, again by [Pr89, proposition 2.10], we have

$$e(\mathfrak{p}) \geq \frac{q_{\mathfrak{p}}^{r_{\mathfrak{p}}+1}}{q_{\mathfrak{p}}+1}. \quad (3)$$

So either  $\Xi_{\mathfrak{p}}$  has a non-trivial element, in which case by the above argument and a similar reasoning as in the previous cases we get the desired  $\sigma$ , or not, in which case getting  $\sigma$  is a straightforward conclusion of (3).  $\square$

**Definition 20.** Let  $\mathfrak{R}(\Gamma) := T_c \cup T_l$  be the set of *ramified primes* of  $\Gamma$ , where  $T_c$  and  $T_l$  are defined as follows:

- 1- (Ramified at the level of commensurability) This is the set of  $\mathfrak{p} \in V_k$  such that  $\mathbb{G}$  is not quasi-split over  $k_{\mathfrak{p}}$ . We shall denote it by  $T_c$ .
- 2- (Ramified at the local level) This set consists of either  $\mathfrak{p} \in V_k$  which is ramified over  $l$  (alternatively  $\mathcal{G}$  does not split over  $k_{\mathfrak{p}}$ ) and  $P_{\mathfrak{p}}$  is not special, or  $\mathfrak{p} \in V_k \setminus T_c$  and is not ramified over  $l$  and  $P_{\mathfrak{p}}$  is not hyper-special. We shall denote it by  $T_l$ .

#### 4.4 The main inequality.

Here we will use Riemann hypothesis for curves over finite fields proved by A. Weil to estimate  $h_l$  and couple it with an estimate of  $g_k$  in terms of  $g_l$  to prove the following inequality.

**Theorem 21** (Main Inequality). *In the above setting, there are positive numbers  $c, \sigma, \sigma_1$  and  $\sigma_2$  depending only on  $G$  such that*

$$\text{vol}(G/\Gamma) \geq c \cdot q_k^{\sigma_1 g_k + \sigma_2 g_l} \cdot \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma}.$$

*Proof.* By Riemann hypothesis for curves over finite fields, we know that

$$(\sqrt{q_l} - 1)^{2g_l} \leq h_l \leq (\sqrt{q_l} + 1)^{2g_l}. \quad (4)$$

By Proposition 18, Proposition 19 and inequality (4), we have that

$$\begin{aligned} \text{vol}(G/\Gamma) &\geq c_6 \cdot (\sqrt{q_l} + 1)^{-2g_l \varepsilon'} \cdot q_k^{(g_k - 1) \dim \mathcal{G}} \cdot \left( \frac{q_l^{(g_l - 1)}}{q_k^{(g_k - 1)[l:k]}} \right)^{s'(\mathcal{G})} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma} \\ &= c_7 \cdot (\sqrt{q_l} + 1)^{-2g_l \varepsilon'} \cdot q_k^{g_k(\dim \mathcal{G} - [l:k]s')} \cdot q_l^{g_l s'} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma}, \end{aligned} \quad (5)$$

where  $c_7$  just depends on  $G$  as  $q_k$  is at most equal to the number of elements of the residue field of  $K$  and  $\dim \mathcal{G}$  just depends on  $G$ .

We consider inner forms and outer forms separately. First assume that  $k = l$ ; then, by inequality (5), we have

$$\text{vol}(G/\Gamma) \geq c_7(\sqrt{q_k} + 1)^{-2g_k} \cdot q_k^{g_k \dim \mathcal{G}} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma}.$$

Since we assumed that the characteristic of  $K$  is at least 3,  $q_k$  is at least 3. Hence  $\sqrt{q_k} + 1 < q_k^{1-\sigma_3}$ , for a positive number  $\sigma_3$ . Thus  $\sigma_4 = \dim \mathcal{G} - 2(1 - \sigma_3)$  is a positive number and

$$\text{vol}(G/\Gamma) \geq c_7 \cdot q_k^{\sigma_4 g_k} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma}. \quad (6)$$

Now assume that  $q_l = q_k^2$ ; then  $g_l = g_k$ , and so by inequality (5), we have

$$\text{vol}(G/\Gamma) \geq c_7 \cdot (q_k + 1)^{-2g_k} q_k^{g_k \dim \mathcal{G}} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma}.$$

We notice that on one hand we have  $q_k + 1 < q_k^{2-\sigma_5}$ , for a fixed positive number  $\sigma_5$  and any  $q_k$ , and on the other hand  $\sigma_6 = \dim \mathcal{G} - 2(2 - \sigma_5)$  is positive as the  $K$ -rank of  $\mathbb{G}_0$  is at least 2. Therefore we have

$$\text{vol}(G/\Gamma) \geq c_7 \cdot q_k^{\sigma_6 g_k} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma}. \quad (7)$$

Now assume that  $q = q_l = q_k$ ; then, by inequality (5) coupled with the fact that  $\sqrt{q} + 1 \leq q$  as  $q \geq 3$ , we have

$$\text{vol}(G/\Gamma) \geq c_7 \cdot q^{g_k(\dim \mathcal{G} - [l:k]\mathfrak{s}') + g_l(\mathfrak{s}' - 2\varepsilon')} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma}. \quad (8)$$

In the following table, we give the possible values of  $\sigma_7 = \dim \mathcal{G} - [l:k]\mathfrak{s}'$  and  $\sigma_8 = \mathfrak{s}' - 2\varepsilon'$  for all the possible types.

	$\dim \mathcal{G}$	$\mathfrak{s}$	$\mathfrak{s}'$	$\dim \mathcal{G} - [l:k]\mathfrak{s}'$	$\mathfrak{s}' - 2\varepsilon'$
$A_r^{(2)}, 2 r$	$r(r+2)$	$\frac{r(r+3)}{2}$	$\frac{r(r+3)}{2}$	$-r$	$\frac{(r+4)(r-1)}{2}$
$A_r^{(2)}, 2 \nmid r$	$r(r+2)$	$\frac{(r-1)(r+2)}{2}$	$\frac{(r-1)(r+2)}{2}$	$r+2$	$\frac{(r+3)(r-2)}{2}$
$D_r^{(2)}, 2 r$	$r(2r-1)$	$2r-1$	$2r-3$	$(2r-1)(r-2)+4$	$2r-7$
$D_r^{(2)}, 2 \nmid r$	$r(2r-1)$	$2r-1$	$2r-1$	$(2r-1)(r-2)$	$2r-3$
$E_6^{(2)}$	78	26	26	26	24
$D_4^{(3),(6)}$	28	7	5	13	1

We observe that both of these values are positive except when  $\mathbb{G}$  is of type  $A_r$  with  $r$  even. When  $\mathbb{G}$  is of this type, we have

$$\begin{aligned} \text{vol}(G/\Gamma) &\geq c_7 \cdot q^{-g_k r + g_l (r+4)(r-1)/2} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma} \\ &\geq c_8 \cdot q^{[-(g_k-1)r + (g_l-1)r/2] + (g_l-1)[(r+4)(r-1)-r]/2} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma} \quad (9) \\ &\geq c_9 \cdot q^{g_l[(r+1)^2-5]/2} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma}, \end{aligned}$$

where  $c_8$  and  $c_9$  just depend on  $G$  as  $(g_l - 1) - [l : k](g_k - 1)$  is non-negative and  $q$  is at most equal to the number of elements of the residue field of  $K$ . We also note that  $\sigma_9 = [(r + 1)^2 - 5]/2$  is positive since  $r$  is even and positive.

The only remaining case is when  $\mathcal{G}$  is of type  $D_4^{(3)}$  and  $q_l = q_k^3$ , in which case  $g_l = g_k$  and, by inequality (5), we have

$$\text{vol}(G/\Gamma) \geq c_7 \cdot (\sqrt{q_k}^3 + 1)^{-4g_k} \cdot q_k^{28(g_k-1)} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma}.$$

We note that  $\sqrt{q_k}^3 + 1 \leq q_k^2$  for any  $q_k \geq 3$ . Hence we have

$$\text{vol}(G/\Gamma) \geq c_{10} \cdot q_k^{20g_k} \prod_{\mathfrak{p} \in \mathfrak{R}(\Gamma)} q_{\mathfrak{p}}^{\sigma}, \quad (10)$$

where  $c_{10}$  just depends on  $G$ .

It is straightforward to finish the proof using inequalities (6), (7), (8), (9) and (10).  $\square$

#### 4.5 Number of possible pair of function fields $(k, l)$ .

Here we will use a result of de Jong and Katz [dJK] on the number of curves over a finite field to give an upper bound on the number of possible pairs of function fields  $(k, l)$ .

First we point out that since  $k_{\mathfrak{p}_0}$  is isomorphic to  $K$  for some  $\mathfrak{p}_0 \in V_k$ ,  $q_k^{\deg \mathfrak{p}_0} = \#\mathfrak{f}$  where  $\mathfrak{f}$  is the residue field of  $K$ . Hence the number of possibilities for  $q_k$  is bounded only by  $G$  and this upper bound is independent of  $x$  the bound on the covolume of  $\Gamma$ . So without loss of generality we can assume that  $q_k$  is fixed.

If  $\text{vol}(G/\Gamma) \leq x$ , then by Theorem 21, we have

$$x \geq cp^{\sigma_1 g_k + \sigma g_l}.$$

Hence  $g_k \leq \sigma_1^{-1} \log(x/c)$  and  $g_l \leq \sigma_2^{-1} \log(x/c)$ . By de Jong and Katz [dJK], the number of function fields with a given constant field of size  $q$  and genus  $g$  is at most  $c' g^{\log g}$ , where  $c' = c'(q)$  just depends on  $q$ . Hence number of possible pair of function fields  $(k, l)$  is at most

$$x^{c_{11} \log \log x},$$

where  $c_{11}$  is a positive number which just depends on  $G$ .

**Remark 22.** It is worth mentioning that by a similar argument as above one gets that the number of possible pairs of the function fields  $(k, l)$  is at most  $x^{c_{11}}$  (where  $c_{11}$  is a number which just depends on  $G$ ) if Question 7 has a positive answer.

## 4.6 Number of possible $\mathbb{G}$ .

Here we use local-global principle to give an upper bound for the number of admissible  $\mathbb{G}$ 's.

From now on we shall fix  $(k, l)$  and as a consequence  $\mathcal{G}$ . Since  $\mathbb{G}$  is a  $k$ -inner form of  $\mathcal{G}$ , in order to find an upper bound on the number of possible such groups, we can give an upper bound on the number of possible elements of  $H^1(k, \overline{\mathcal{G}})$ . (We note that  $\overline{\mathcal{G}}$  is a smooth  $k$ -group scheme, and so the Galois and the flat cohomologies are the same.) First we show that

$$H^1(k, \overline{\mathcal{G}}) \rightarrow \prod_{\mathfrak{p} \in V_k} H^1(k_{\mathfrak{p}}, \overline{\mathcal{G}})$$

is an injective map, and then we count at the local level.

**Lemma 23.** *Let  $\phi_n$  be the homomorphism  $x \mapsto x^n$  from the multiplicative  $k$ -group scheme  $\mathbb{G}_m$  to itself. Let  $\mu_n$  be the  $k$ -group scheme kernel of  $\phi_n$ . Then*

$$H^2(k, \mu_n) \rightarrow \prod_{\mathfrak{p} \in V_k} H^2(k_{\mathfrak{p}}, \mu_n)$$

is an injective map.

*Proof.* By the definition, we have the following short exact sequence

$$1 \rightarrow \mu_n \rightarrow \mathbb{G}_m \xrightarrow{\phi_n} \mathbb{G}_m \rightarrow 1.$$

Therefore we get the following diagrams (each row is a long exact sequence)

$$\begin{array}{ccccc} H^1(k, \mathbb{G}_m) & \rightarrow & H^2(k, \mu_n) & \rightarrow & H^2(k, \mathbb{G}_m) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{\mathfrak{p} \in V_k} H^1(k_{\mathfrak{p}}, \mathbb{G}_m) & \rightarrow & \prod_{\mathfrak{p} \in V_k} H^2(k_{\mathfrak{p}}, \mu_n) & \rightarrow & \prod_{\mathfrak{p} \in V_k} H^2(k_{\mathfrak{p}}, \mathbb{G}_m). \end{array} \quad (11)$$

Since  $\mathbb{G}_m$  is a smooth  $k$ -group scheme, the flat cohomologies are isomorphic to the Galois cohomologies. Hence  $H^1(k, \mathbb{G}_m) = 1$ ,  $H^1(k_{\mathfrak{p}}, \mathbb{G}_m) = 1$ , for any  $\mathfrak{p}$ ,  $H^2(k, \mathbb{G}_m) \simeq Br(k)$  and  $H^2(k_{\mathfrak{p}}, \mathbb{G}_m) \simeq Br(k_{\mathfrak{p}})$ . By Brauer-Hasse-Noether theorem, we have that

$$0 \rightarrow Br(k) \rightarrow \bigoplus_{\mathfrak{p} \in V_k} Br(k_{\mathfrak{p}}) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

is a short exact sequence. Thus the last vertical arrow in diagram (11) is injective. So, following the arrows in diagram (11), one can easily finish the argument.  $\square$

**Lemma 24.** *Let  $\mu_n$  be as above; then*

$$H^2(k, R_{l/k}(\mu_n)) \rightarrow \prod_{\mathfrak{p} \in V_k} H^2(k_{\mathfrak{p}}, R_{l/k}(\mu_n))$$

is an injective map.

*Proof.* By Shapiro's lemma (see Theorem 9), we have

$$H^2(k, R_{l/k}(\mu_n)) \simeq H^2(l, \mu_n) \ \& \ H^2(k_{\mathfrak{p}}, R_{l/k}(\mu_n)) \simeq \bigoplus_{\mathfrak{p} \in V_l} H^2(l_{\mathfrak{p}}, \mu_n).$$

Hence the map in question is induced by the map

$$H^2(l, \mu_n) \rightarrow \prod_{\mathfrak{p} \in V_l} H^2(l_{\mathfrak{p}}, \mu_n),$$

which is an embedding by Lemma 23 and we are done.  $\square$

**Lemma 25.** *Let  $\mu_n$  be as above,  $\nu = R_{l/k}(\mu_n)$ , and  $\nu^{(1)} = R_{l/k}^{(1)}(\mu_n)$  be a  $k$ -group scheme which is the kernel of the norm map  $\ker(R_{l/k}(\mu_n) \xrightarrow{N_{l/k}} \mu_n)$ ; then*

$$\phi : H^2(k, \nu^{(1)}) \rightarrow \prod_{\mathfrak{p} \in V_k} H^2(k_{\mathfrak{p}}, \nu^{(1)})$$

*is an injective map if either  $[l : k]$  and  $n$  are coprime, or  $[l : k] = 2$ .*

*Proof.* By the definition, the following is a short exact sequence

$$1 \rightarrow \nu^{(1)} \rightarrow \nu \rightarrow \mu_n \rightarrow 1.$$

Hence we get the following diagram (each row is an exact sequence):

$$\begin{array}{ccccc} H^1(k, \mu_n) & \xrightarrow{\delta} & H^2(k, \nu^{(1)}) & \rightarrow & H^2(k, \nu) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{\mathfrak{p} \in V_k} H^1(k_{\mathfrak{p}}, \mu_n) & \xrightarrow{(\delta_{\mathfrak{p}})} & \prod_{\mathfrak{p} \in V_k} H^2(k_{\mathfrak{p}}, \nu^{(1)}) & \rightarrow & \prod_{\mathfrak{p} \in V_k} H^2(k_{\mathfrak{p}}, \nu). \end{array} \quad (12)$$

As all the group schemes are abelian, it is enough to show that the kernel of  $\phi$  is trivial. Since, by Lemma 24, the last vertical arrow is an embedding and the first row is an exact sequence, kernel of  $\phi$  is in the image of the boundary map  $\delta$ . On the other hand,  $H^1(k, \mu_n) \simeq k^{\times}/k^{\times n}$ ,  $H^1(k_{\mathfrak{p}}, \mu_n) \simeq k_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times n}$ , and we have the following diagram (each row is an exact sequence):

$$\begin{array}{ccccc} l^{\times}/l^{\times n} & \rightarrow & k^{\times}/k^{\times n} & \xrightarrow{\delta} & H^2(k, \nu^{(1)}) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{\mathfrak{p} \in V_k} (l \otimes_k k_{\mathfrak{p}})^{\times}/(l \otimes_k k_{\mathfrak{p}})^{\times n} & \rightarrow & \prod_{\mathfrak{p} \in V_k} k_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times n} & \xrightarrow{(\delta_{\mathfrak{p}})} & \prod_{\mathfrak{p} \in V_k} H^2(k_{\mathfrak{p}}, \nu^{(1)}) \end{array}$$

So overall, by the above discussion and following the arrows in diagram 12 and the above one, for any  $\eta \in \ker \phi$ , one can find  $x \in k^{\times}$  such that

- 1-  $\delta(xk^{\times n}) = \eta$ .
- 2- For any  $\mathfrak{p} \in V_k$ , there is  $y_{\mathfrak{p}} \in \bigoplus_{\mathfrak{p} \in V_l} l_{\mathfrak{p}}^{\times}$  such that  $xk_{\mathfrak{p}}^{\times n} = N_{l/k}(y_{\mathfrak{p}})k_{\mathfrak{p}}^{\times n}$ .

If  $[l : k]$  and  $n$  are coprime, then for some  $y \in l$ , we have  $xk^{\times n} = N_{l/k}(y)k^{\times n}$ , and so  $\eta$  is trivial, and we are done.

If they are not coprime, then, by the assumptions,  $[l : k] = 2$  and  $n$  is even, in which case,  $k^{\times n} \subseteq N_{l/k}(l^\times)$  and  $k_{\mathfrak{p}}^{\times n} \subseteq N_{l/k}((l \otimes_k k_{\mathfrak{p}})^\times)$ . Hence for any  $\mathfrak{p}$ ,  $x$  is in the image of the norm map, i.e.  $x \in N_{l/k}((l \otimes_k k_{\mathfrak{p}})^\times)$ . Thus, by Hasse norm theorem [Sc85, Chapter 10], there is  $y \in l$  such that  $N_{l/k}(y) = x$  and so  $\eta$  is again trivial, and we are done.  $\square$

**Theorem 26.** *Let  $\mathcal{G}, k$  and  $l$  be as before; then*

$$\phi : H^1(k, \overline{\mathcal{G}}) \rightarrow \prod_{\mathfrak{p} \in V_k} H^1(k_{\mathfrak{p}}, \overline{\mathcal{G}})$$

*is an injective map.*

*Proof.* Since  $\mathbb{G}$  is a  $k$ -inner form of  $\mathcal{G}$ , their centers are  $k$ -isomorphic. Hence we have the following short exact sequence:

$$1 \rightarrow \mu \rightarrow \mathcal{G} \rightarrow \overline{\mathcal{G}} \rightarrow 1,$$

and either  $\mu$  is  $k$ -isomorphic to  $\mu_t^\varepsilon$  or  $R_{l/k}^{(1)}(\mu_t)$ , where  $\varepsilon = \varepsilon(\mathbb{G})$  and  $t = t(\mathbb{G})$ . From the above short exact sequence, one can conclude the following diagram (each row is an exact sequence):

$$\begin{array}{ccccc} H^1(k, \mathcal{G}) & \rightarrow & H^1(k, \overline{\mathcal{G}}) & \xrightarrow{\delta} & H^2(k, \mu) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{\mathfrak{p} \in V_k} H^1(k_{\mathfrak{p}}, \mathcal{G}) & \rightarrow & \prod_{\mathfrak{p} \in V_k} H^1(k_{\mathfrak{p}}, \overline{\mathcal{G}}) & \rightarrow & \prod_{\mathfrak{p} \in V_k} H^2(k_{\mathfrak{p}}, \mu) \end{array} \quad (13)$$

By [BT87, H75], we know that  $H^1(k, \mathcal{G}) = 1$  and  $H^1(k_{\mathfrak{p}}, \mathcal{G}) = 1$ , for any  $\mathfrak{p}$ . Furthermore, by Lemma 23 and Lemma 25, the last vertical map is injective. Thus following arrows in the diagram 13, we have that  $\delta(\mathfrak{c}_1) = \delta(\mathfrak{c}_2)$  if  $\phi(\mathfrak{c}_1) = \phi(\mathfrak{c}_2)$  for  $\mathfrak{c}_1$  and  $\mathfrak{c}_2$  in  $H^1(k, \overline{\mathcal{G}})$ . So in order to show that  $\phi$  is injective, it is enough to show that  $\delta$  the boundary map is injective. To this end, we shall use the trick of twisting by a cocycle. Namely for a given  $\mathfrak{c}$  in  $H^1(k, \overline{\mathcal{G}})$ , we consider the following short exact sequence

$$1 \rightarrow \mu \rightarrow \mathcal{G}_{\mathfrak{c}} \rightarrow \overline{\mathcal{G}}_{\mathfrak{c}} \rightarrow 1.$$

Since  $\mathcal{G}_{\mathfrak{c}}$  is again simply connected  $k$ -group, by [BT87, H75], the fiber of  $\delta_{\mathfrak{c}}$  over the trivial element is trivial. Hence, by the trick of twisting (see [G71, Chapter IV, Proposition 4.3.4]), the fiber of  $\delta$  over  $\delta(\mathfrak{c})$  has only one element.  $\square$

For a given  $k$  and  $l$ , any admissible  $\mathbb{G}$  is a  $k$ -inner form of  $\mathcal{G}$ . Hence there is an element in the image of  $H^1(k, \overline{\mathcal{G}})$  in  $H^1(k, \text{Aut}(\mathcal{G}))$  (these are Galois cohomologies and since  $\overline{\mathcal{G}}$  is a smooth  $k$ -group scheme, the first one is naturally isomorphic to the flat cohomology) which corresponds to  $\mathbb{G}$ . By the main inequality, Theorem 21, we know that

$$\prod_{\mathfrak{p} \in T_{\mathfrak{c}}} q_{\mathfrak{p}} \leq x^{c_{12}}$$



where  $T_c$  is the set of places over which  $\mathbb{G}$  is not quasi-split and  $c_{12}$  just depends on  $G$ . This is equivalent to saying that

$$\deg(D(T_c)) \leq c_{12} \log(x),$$

where  $D(T_c) = \sum_{\mathfrak{p} \in T_c} \mathfrak{p}$ . The next lemma gives us an upper bound on the number of possibilities of effective divisors, i.e. a divisor  $\sum_{\mathfrak{p} \in V_k} a_{\mathfrak{p}} \mathfrak{p}$  with non-negative coefficients, with a given upper bound on their degree.

**Lemma 27.** *Let  $k$  be any global function field; then, for any  $y$ ,*

$$\#\{D \in \text{Div}^+(k) \mid \deg(D) \leq y\} \leq 4h_k q^y,$$

where  $\text{Div}^+(k)$  is the set of all the effective divisors of  $k$ ,  $q = q_k$  is the number of elements of the constant field of  $k$ , and  $h_k$  is the class number of  $k$ .

*Proof.* By Riemann-Roch theorem [R02], there is a divisor  $C$  such that for any divisor  $D$ ,

$$l(D) = \deg(D) - g + 1 + l(C - D),$$

where  $l(D) = \dim_{\mathbb{F}_k} \{x \in k^\times \mid (x) + D \geq 0\} \cup \{0\}$ . Moreover  $l(C) = g$  and  $\deg(C) = 2g - 2$ . As a corollary of Riemann-Roch theorem [R02], one can show that for any non-negative integer number  $N$ , there are  $h = h_k$  effective divisors  $\{D_1, \dots, D_h\}$  of degree  $N$  such that

$$b_N = \#\{D \in \text{Div}^+(k) \mid \deg(D) = N\} = \sum_{i=1}^{h_k} \frac{q^{l(D_i)} - 1}{q - 1},$$

where  $q = q_k$ . On the other hand,  $l(C - D_i) \leq l(C) = g$  as  $D_i$  is an effective divisor. Hence

$$b_N \leq h \frac{q^{N+1} - 1}{q - 1} \leq 2hq^N.$$

Thus

$$\#\{D \in \text{Div}^+(k) \mid \deg(D) \leq y\} \leq 2h \sum_{N=0}^y q^N \leq 4hq^y,$$

which finishes the argument.  $\square$

Hence by the above argument and Lemma 27, for a given admissible  $k$  and  $l$ , the number of possible sets for  $T_c$  is at most  $4h_k x^{c_{12}}$ . On the other hand, by Weil's theorem on Riemann hypothesis for curves over finite fields, we have

$$h_k \leq (\sqrt{q} + 1)^{2g} \leq q^{2g},$$

and, by the discussions in 4.5, we have that for an admissible  $k$ ,  $q^g \leq x^{c_{13}}$  where  $c_{13}$  just depends on  $G$ . Thus for a given admissible pair of function fields  $(k, l)$ , the number of possible  $T_c$ 's is at most  $x^{c_{14}}$ , where  $c_{14}$  just depends on  $G$ .

Let  $\mathfrak{c}$  be the element in  $H^1(k, \overline{\mathcal{G}})$  which gives us  $\mathbb{G}$ . By Theorem 26, it is enough to give an upper bound for the number of possible elements in  $\prod_{\mathfrak{p} \in V_k} H^1(k_{\mathfrak{p}}, \overline{\mathcal{G}})$  for  $\phi(\mathfrak{c})$ . Since  $\mathbb{G}$  is quasi-split over any place not in  $T_c$ , any admissible element in  $\prod_{\mathfrak{p} \in V_k} H^1(k_{\mathfrak{p}}, \overline{\mathcal{G}})$  is non-trivial only in the  $T_c$  components. On the other hand,  $H^1(k_{\mathfrak{p}}, \overline{\mathcal{G}})$  can be embedded into  $H^2(k_{\mathfrak{p}}, \mu)$  and the latter can be embedded into a direct product of at most  $2\varepsilon(\mathcal{G})$  torsion quotients of  $\mathbb{Q}/\mathbb{Z}$ , where each quotient has exponent at most  $t = t(\mathcal{G})$ . One gets such an embedding as the second flat cohomology of  $\mathbb{G}_m$  is isomorphic to the Brauer group and the Brauer group of a non-archimedean local field is isomorphic to  $\mathbb{Q}/\mathbb{Z}$ . Therefore, for any  $\mathfrak{p}$ ,

$$\#H^1(k_{\mathfrak{p}}, \overline{\mathcal{G}}) \leq c_{15},$$

where  $c_{15}$  just depends on  $G$ . As  $\#T_c \leq c_{12} \log x$ , overall we have that, for a given admissible  $k$  and  $l$ , the number of possible  $\phi(\mathfrak{c})$  and therefore the number of  $\mathbb{G}$  admissible  $k$ -forms of  $\mathcal{G}$  is at most  $x^{c_{16}}$ , where  $c_{16}$  just depends on  $G$ .

#### 4.7 Number of possible $\{P_{\mathfrak{p}}\}$ 's up to $\overline{\mathbb{G}}(\mathbb{A}_k)$ .

We have already given an upper bound on the number of possible  $k$ ,  $l$ , and  $k$ -forms  $\mathbb{G}$ . Now, we will fix such  $\mathbb{G}$ , and count the number of possibilities of  $\{P_{\mathfrak{p}}\}$ , a coherent family of parahoric subgroups. To this end, first we will give an upper bound on the number of  $\Theta$  admissible types up to the action of  $\overline{\mathbb{G}}(\mathbb{A}_k)$ , the adjoint group on local Dynkin diagrams, and then, in the next section, provide an upper bound on the class number of  $\mathbb{G}$  with respect to a coherent family of parahoric subgroups with a given admissible type.

By the main inequality, we know that

$$\deg(D(T_l)) \leq c_{17} \log_q x,$$

where  $D(T_l) = \sum_{\mathfrak{p} \in T_l} \mathfrak{p}$  and  $c_{17}$  just depends on  $G$ . Hence, by Lemma 27, the number of possible sets for  $T_l$  is at most  $4h_k x^{c_{17}}$ . Thus again, by using Weil's theorem on Riemann hypothesis for curves over finite fields, we have that the number of possible sets for  $T_l$  is at most  $x^{c_{18}}$ , where  $c_{18}$  just depends on  $G$ . Hence, without loss of generality, we can and we will fix  $T_l$ , the set of primes ramified at the local level.

The adjoint group acts transitively on the set of hyper-special vertices. So if  $\mathfrak{p}$  is not in  $T_l$ , then either it is ramified over  $l$  or  $\Theta_{\mathfrak{p}}$  is unique up to  $\overline{\mathbb{G}}(k_{\mathfrak{p}})$ . Again, by the main inequality,  $\#T_l \leq c_{17} \log_q x$ , and, on the other hand, the number of possible types for any given  $\mathfrak{p}$  is bounded by a constant depending only on  $G$ . Thus the number of possible  $\Theta$ 's up to  $\overline{\mathbb{G}}(\mathbb{A}_k)$  is at most  $x^{c_{19}}$ .

#### 4.8 Number of possible $\{P_{\mathfrak{p}}\}$ .

By the discussion in 4.7, we can and will fix  $\{P_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^{\circ}}$  a coherent family of parahoric subgroups up to an element of  $\overline{\mathbb{G}}(\mathbb{A}_k)$ . Here we will give an upper bound

on the number of admissible  $\{P'_p\}_{p \in V_k^\circ}$  within the  $\overline{\mathbb{G}}(\mathbb{A}_k)$ -orbit of  $\{P_p\}_{p \in V_k^\circ}$  such that the corresponding lattices in  $\mathbb{G}(k_{p_0})$  are not conjugate of each other.

Let  $\overline{P}_p$  be the stabilizer of  $P_p$  in  $\overline{\mathbb{G}}(k_p)$ ,

$$\text{Cl}(\overline{\mathbb{G}}, \{\overline{P}_p\}_{p \in V_k^\circ}) = \overline{\mathbb{G}}(\mathbb{A}_k)/\overline{\mathbb{G}}(k) \cdot \overline{\mathbb{G}}(k_{p_0}) \prod_{p \in V_k^\circ} \overline{P}_p$$

the class group of  $\overline{\mathbb{G}}$  with respect  $\{\overline{P}_p\}_{p \in V_k^\circ}$ , and  $\text{cl}(\overline{\mathbb{G}}, \{\overline{P}_p\}) = \#\text{Cl}(\overline{\mathbb{G}}, \{\overline{P}_p\})$  the class number of  $\overline{\mathbb{G}}$  with respect  $\{\overline{P}_p\}_{p \in V_k^\circ}$ . It is well-known that there is a correspondence between the double cosets of  $\overline{\mathbb{G}}(k)$  and  $\overline{\mathbb{G}}(k_{p_0}) \prod_{p \in V_k^\circ} \overline{P}_p$  in  $\overline{\mathbb{G}}(\mathbb{A}_k)$  and  $\text{Cl}(\overline{\mathbb{G}}, \{\overline{P}_p\}_{p \in V_k^\circ})$ . Let  $\pi$  be the projection from  $\overline{\mathbb{G}}(\mathbb{A}_k)$  onto

$$\overline{\mathbb{G}}(k) \backslash \overline{\mathbb{G}}(\mathbb{A}_k)/\overline{\mathbb{G}}(k_{p_0}) \prod_{p \in V_k^\circ} \overline{P}_p.$$

**Lemma 28.** *Let  $g^{(1)}, g^{(2)} \in \overline{\mathbb{G}}(\mathbb{A}_k)$  such that  $\pi(g^{(1)}) = \pi(g^{(2)})$ ,*

$$\prod_{p \in V_k^\circ} P_p^{(i)} = g^{(i)} \left( \prod_{p \in V_k^\circ} P_p \right),$$

and  $\Lambda^{(i)} = \mathbb{G}(k) \cap \prod_{p \in V_k^\circ} P_p^{(i)}$  for  $i = 1, 2$ ; then  $\Lambda^{(1)}$  and  $\Lambda^{(2)}$  are the same up to an element of  $\overline{\mathbb{G}}(k)$ .

*Proof.* Since  $\pi(g^{(1)}) = \pi(g^{(2)})$ , there are  $g_k \in \overline{\mathbb{G}}(k)$  and  $g \in \overline{\mathbb{G}}(k_{p_0}) \prod_{p \in V_k^\circ} \overline{P}_p$  such that  $g^{(2)} = g_k g^{(1)} g$ . By the definition,

$$g^{(2)} \left( \prod_{p \in V_k^\circ} P_p \right) = g_k g^{(1)} \left( \prod_{p \in V_k^\circ} P_p \right),$$

and so  $g_k(\Lambda^{(1)}) = \Lambda^{(2)}$ , as we claimed.  $\square$

As we would like to count number of maximal lattices up to an automorphism of  $G$ , by the above comments and Lemma 28, it is enough to give an upper bound on  $\text{cl}(\overline{\mathbb{G}}, \{\overline{P}_p\})$ .

**Theorem 29.** *In the above setting, there is a constant  $c$  depending only on  $G$ , such that*

$$\text{cl}(\overline{\mathbb{G}}, \{\overline{P}_p\}) \leq x^c.$$

*Proof.* By the strong approximation [Pr77, M77] for simply connected groups, we have

$$\mathbb{G}(\mathbb{A}_k) = \mathbb{G}(k) \cdot \mathbb{G}(k_{p_0}) \prod_{p \in V_k^\circ} P_p.$$

Hence  $\text{Cl}(\overline{\mathbb{G}}, \{\overline{P}_p\})$  is a quotient of

$$\overline{\mathbb{G}}(\mathbb{A}_k)/(\overline{\mathbb{G}}(k)\text{Ad}(\mathbb{G}(\mathbb{A}_k)) \prod_{p \in V_k} \overline{P}_p).$$

On the other hand, for any  $\mathfrak{p}$ , we have that

$$\overline{\mathbb{G}}(k_{\mathfrak{p}})/\mathrm{Ad}(\mathbb{G}(k_{\mathfrak{p}})) \simeq H^1(k_{\mathfrak{p}}, \mu).$$

As before, let  $\xi_{\mathfrak{p}}$  be the homomorphism from  $H^1(k_{\mathfrak{p}}, \mu)$  to  $\mathrm{Aut}(\mathcal{D}_{\mathfrak{p}})$ . Then there is an onto map from  $H^1(k_{\mathfrak{p}}, \mu)/\ker(\xi_{\mathfrak{p}})$  to

$$\overline{\mathbb{G}}(k_{\mathfrak{p}})/\mathrm{Ad}(\mathbb{G}(k_{\mathfrak{p}}))\overline{P}_{\mathfrak{p}}.$$

So altogether  $\mathrm{Cl}(\overline{\mathbb{G}}, \{\overline{P}_{\mathfrak{p}}\})$  is a homomorphic image of

$$\mathcal{C} = (\oplus_{\mathfrak{p} \in V_k} H^1(k_{\mathfrak{p}}, \mu)/\ker(\xi_{\mathfrak{p}}))/\Delta(H^1(k, \mu)),$$

where  $\Delta$  is the natural diagonal homomorphism.

First, we assume that  $\mathbb{G}$  is an inner form. In this case,  $\mu$  is isomorphic to  $(\mu_t)^\varepsilon$  as a  $k$ -group scheme, where  $t = t(\mathcal{G})$  and  $\varepsilon = \varepsilon(\mathcal{G})$ . Hence  $H^1(k_{\mathfrak{p}}, \mu) \simeq (k_{\mathfrak{p}}^\times/k_{\mathfrak{p}}^{\times t})^\varepsilon$  and  $H^1(k, \mu) \simeq (k^\times/k^{\times t})^\varepsilon$ . If  $\mathfrak{p}$  is not in  $T_c$ , i.e.  $\mathbb{G}$  is split over  $k_{\mathfrak{p}}$ , then, by [Pr89, Lemma 2.3, Proposition 2.7],  $\ker \xi_{\mathfrak{p}} = (k_{\mathfrak{p}}^{\times t} \mathcal{O}_{\mathfrak{p}}^\times/k_{\mathfrak{p}}^{\times t})^\varepsilon$ . Hence a subgroup of index at most  $c_{15}^{\#T_c}$  in  $\mathcal{C}$  is a homomorphic image of

$$((\oplus_{\mathfrak{p} \in V_k} k_{\mathfrak{p}}^\times/(k_{\mathfrak{p}}^{\times t} \mathcal{O}_{\mathfrak{p}}^\times))/\Delta(k^\times/k^{\times t})^\varepsilon \simeq (\mathrm{Div}(k)/(t\mathrm{Div}(k) + (k))))^\varepsilon,$$

where  $\mathrm{Div}(k)$  is the group of divisors of  $k$  and  $(k)$  is its subgroup of principal divisors. Since the latter has at most  $h_k \leq x^{c_{20}}$  elements and  $\#T_c \leq c_{12} \log x$ ,  $\mathrm{cl}(\overline{\mathbb{G}}, \{\overline{P}_{\mathfrak{p}}\}) \leq \#\mathcal{C}$  is at most  $x^{c_{21}}$ , where all the constants just depend on  $G$ , which is the desired result.

Now, let us assume that  $\mathbb{G}$  is an outer form. In this case,  $\mu$  is isomorphic to  $\nu^{(1)} = R_{l/k}^{(1)}(\mu_n)$  as a  $k$ -group scheme, where  $R_{l/k}^{(1)}(\mu_n)$  is as in Lemma 25 and  $n = t(\mathbb{G})$  unless  $\mathbb{G}$  is of type  $D_r$  with  $r$  even. Hence we have the following exact sequence

$$\mu_n(l \otimes_k k_{\mathfrak{p}}) \xrightarrow{N_{l/k}} \mu_n(k_{\mathfrak{p}}) \rightarrow H^1(k_{\mathfrak{p}}, \mu) \rightarrow (l \otimes_k k_{\mathfrak{p}})^\times / (l \otimes_k k_{\mathfrak{p}})^{\times n} \xrightarrow{N_{l/k}} k_{\mathfrak{p}}^\times / k_{\mathfrak{p}}^{\times n},$$

for any  $\mathfrak{p}$  and a similar exact sequence for  $k$  instead of  $k_{\mathfrak{p}}$ . For any  $\mathfrak{p}$ ,  $l \otimes_k k_{\mathfrak{p}} \simeq \oplus_{\mathfrak{q}|\mathfrak{p}} l_{\mathfrak{q}}$  and moreover again by [Pr89, Lemma 2.3, Proposition 2.7], if  $\mathfrak{p}$  is not ramified over  $l$  and not in  $T_c$ , i.e.  $\mathbb{G}$  is quasi-split over  $k_{\mathfrak{p}}$  and splits over  $\widehat{k}_{\mathfrak{p}}$ , then the image of  $\ker(\xi_{\mathfrak{p}})$  contains the intersection of the kernel of the norm map and  $\oplus_{\mathfrak{q}|\mathfrak{p}} \mathcal{O}_{\mathfrak{q}}^\times l_{\mathfrak{q}}^{\times n} / l_{\mathfrak{q}}^{\times n}$ . On the other hand, the following diagram is commutative

$$\begin{array}{ccc} \mu_n(k_{\mathfrak{p}}^\times)/N_{l/k}(\mu_n(l \otimes_k k_{\mathfrak{p}})) & \rightarrow & H^1(k_{\mathfrak{p}}, \mu) \\ \downarrow & & \downarrow \\ \mu_n(\widehat{k}_{\mathfrak{p}}^\times)/N_{l/k}(\mu_n(l \otimes_k \widehat{k}_{\mathfrak{p}})) & \rightarrow & H^1(\widehat{k}_{\mathfrak{p}}, \mu), \end{array}$$

and so if  $\mathfrak{p}$  is not ramified over  $l$  and  $\mathbb{G}$  is quasi-split over  $\mathfrak{p}$ , then the image of  $\mu_n(k_{\mathfrak{p}}^\times)/N_{l/k}(\mu_n(l \otimes_k k_{\mathfrak{p}}))$  is in  $\ker(\xi_{\mathfrak{p}})$ .

From the given long exact sequence, one can get an exact sequence for  $\mathcal{C}$  and by the above discussions both the kernel and the cokernel have at most  $x^{c_{22}}$  elements, where  $c_{22}$  just depends on  $G$ , and so we get the desired result.  $\square$

Theorem 29 completes the proof of the upper bound part of Theorem 2. Indeed by Remark 22, we also see that an affirmative answer to Question 7 gives us a polynomial upper bound on the number of possible maximal lattices.

#### 4.9 A lower bound on the number of maximal lattices.

By Tits' classification, there is  $k$  a global function field, a place  $\mathfrak{p}_0$ , and  $\mathbb{G}$  a simply connected absolutely almost simple  $k$ -group, such that

- 1-  $k_{\mathfrak{p}_0} \simeq K$ .
- 2-  $\mathbb{G} \simeq \mathbb{G}_0$  as  $K$ -groups after identifying  $k_{\mathfrak{p}_0}$  with  $K$ .

Let  $\{P_{\mathfrak{p}}^m\}_{\mathfrak{p} \in V_k^\circ}$  be a coherent family of parahoric subgroups of maximum volume and  $\{P'_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^\circ}$  be a family of parahoric subgroups of  $\{\Theta'_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^\circ}$  such that

- 1- If either  $\mathbb{G}$  is not quasi-split over  $k_{\mathfrak{p}}$  or it does not split over  $\widehat{k}_{\mathfrak{p}}$ , then  $P'_{\mathfrak{p}} = P_{\mathfrak{p}}^m$ .
- 2- If  $\mathbb{G}$  is not an inner form of type A, then  $\Theta'_{\mathfrak{p}}$  is a single vertex which is not hyper-special whenever  $\mathbb{G}$  is quasi-split over  $k_{\mathfrak{p}}$  and splits over  $\widehat{k}_{\mathfrak{p}}$ .
- 3- If  $\mathbb{G}$  is an inner form of type  $A_r$ , then we can and will assume that  $k = \mathfrak{f}_q(t)$  and  $|f/g|_{\mathfrak{p}_0} = q^{\deg(f) - \deg(g)}$ . In this case, whenever  $\mathbb{G}$  splits over  $k_{\mathfrak{p}}$ , its local Dynkin diagram over  $k_{\mathfrak{p}}$  is a cycle of length  $r + 1$  and  $\overline{\mathbb{G}}(k_{\mathfrak{p}})$  acts on it by rotations. Let  $p$  be a prime factor of  $r + 1$  and  $\Theta'_{\mathfrak{p}}$  an orbit of rotation of length  $(r + 1)/p$ . In particular,  $\#\Theta'_{\mathfrak{p}} = p$ .

For any  $D$  a finite subset of  $V_k^\circ$ , let

$$P_{\mathfrak{p}}^D = \begin{cases} P'_{\mathfrak{p}} & \text{if } \mathfrak{p} \in D \\ P_{\mathfrak{p}}^m & \text{if } \mathfrak{p} \in V_k^\circ \setminus D \end{cases}, \quad \Lambda_D = \mathbb{G}(k) \cap \prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}^D,$$

and  $\Gamma_D = N_G(\Lambda_D)$ .

**Lemma 30.** *In the above setting,  $\Gamma_D$  is a maximal lattice in  $G$  for any  $D$  and moreover  $\Gamma_D \cap \mathbb{G}(k) = \Lambda_D$ .*

*Proof.* Let  $\Gamma$  be a maximal lattice which contains  $\Gamma_D$  and  $\Lambda = \Gamma \cap \mathbb{G}(k)$ . Then by Rohlfs' maximality criterion (for the treatment in the case of positive characteristic see [BP89, Section2]), there is  $\{P_{\mathfrak{p}}\}$  a coherent family of parahoric subgroups such that

$$\Lambda = \mathbb{G}(k) \cap \prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}},$$

and  $\Gamma = N_G(\Lambda)$ . Thus  $\Lambda_D \subseteq \Lambda$  and so  $P_{\mathfrak{p}}^D \subseteq P_{\mathfrak{p}}$ , for any  $\mathfrak{p} \in V_k^\circ$ . If  $\mathbb{G}$  is not an inner form of type A, then  $P_{\mathfrak{p}}^D$  is a maximal parahoric subgroup, and so we are done. So let us assume that  $\mathbb{G}$  is an inner form of type  $A_r$  and  $P_{\mathfrak{p}}^D$  is a proper parahoric subgroup of  $P_{\mathfrak{p}}$ , for some  $\mathfrak{p}$ . Because of the way we defined  $P_{\mathfrak{p}}^D$ ,  $\mathbb{G}$  splits over  $k_{\mathfrak{p}}$  and no element of  $\text{Aut}(\mathcal{D}_{\mathfrak{p}})$  preserves type of  $P_{\mathfrak{p}}$  whenever  $P_{\mathfrak{p}}^D \neq P_{\mathfrak{p}}$ . Now we will appeal to Rohlfs' exact sequences (for a treatment of the positive characteristic case see [BP89, Proposition 2.9]).

$$1 \rightarrow \mu(k_{\mathfrak{p}_0})/\mu(k) \rightarrow \Gamma/\Lambda \xrightarrow{\delta} \delta(\overline{\mathbb{G}}(k))_{\Theta^\circ} \rightarrow 1,$$

and a similar short exact sequence for  $\Gamma_D/\Lambda_D$ . Since  $\Gamma_D$  is a subgroup of  $\Gamma$ ,  $\delta(\overline{\mathbb{G}}(k))_{\Theta^D}$  is a subgroup of  $\delta(\overline{\mathbb{G}}(k))_{\Theta^\circ}$ , where  $\Theta^D = \{\Theta_{\mathfrak{p}}^D\}_{\mathfrak{p} \in V_k^\circ}$  is the set of types of the parahoric subgroups  $\{P_{\mathfrak{p}}^D\}$  and  $\Theta^\circ = \{\Theta_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^\circ}$  is the set of types of the parahoric subgroups  $\{P_{\mathfrak{p}}\}$ . On the other hand, by a result of Harder [H75],  $H^1(k, \mathbb{G})$  is trivial and so  $\delta(\overline{\mathbb{G}}(k)) = H^1(k, \mu)$ . Since  $\mathbb{G}$  is an inner form of type  $A_r$ ,  $\mu$  is isomorphic to  $\mu_{r+1}$  as a  $k$ -group scheme. Thus  $H^1(k, \mu)$  is isomorphic to  $k^\times/(k^\times)^{r+1}$ . If  $P_{\mathfrak{p}}^D$  is a proper subgroup of  $P_{\mathfrak{p}}$ , then  $\mathfrak{p}^{(r+1)/p}(k^\times)^{r+1}$  is in  $\delta(\overline{\mathbb{G}}(k))_{\Theta^D}$  but not in  $\delta(\overline{\mathbb{G}}(k))_{\Theta^\circ}$ , which is a contradiction and completes the proof.  $\square$

**Lemma 31.** *In the above setting, there is a fixed finite set  $D_0$  of places of  $k$  such that if  $\theta(\Gamma_{D_1}) = \Gamma_{D_2}$  where  $D_1$  and  $D_2$  are two finite subsets of  $V_k^\circ$  and  $\theta \in \text{Aut}(G)$ , then there is  $\theta_1 \in \text{Aut}(k)$  such that the symmetric difference of  $D_1$  and  $\theta_1(D_2)$*

$$D_1 \triangle \theta_1(D_2) = (D_1 \setminus \theta_1(D_2)) \cup (\theta_1(D_2) \setminus D_1)$$

*is a subset of  $D_0$ .*

*Proof.* First we will prove that  $\theta(\mathbb{G}(k)) = \mathbb{G}(k)$ . Since  $\Lambda_{D_i} \subseteq \mathbb{G}(k)$ 's are of finite index in  $\Gamma_{D_i}$ 's, going to  $\Lambda_1 \subseteq \mathbb{G}(k)$  a finite index subgroup of  $\Lambda_{D_1}$  we can assume that  $\theta(\Lambda_1) = \Lambda_2 \subseteq \mathbb{G}(k)$ . By a theorem of Margulis [M91, Theorem C, Chapter VIII], there exist an automorphism  $\theta_1 : k \rightarrow k$ , a  $k$ -isomorphism  $\theta_2 : {}^{\theta_1}\mathbb{G} \rightarrow \mathbb{G}$  and a homomorphism  $\theta_3 : \Lambda_1 \rightarrow \mu(k_{\mathfrak{p}_0})$  such that

$$\theta(\lambda) = \theta_3(\lambda) \cdot \theta_2(\theta_1(\lambda)),$$

for all  $\lambda \in \Lambda_1$ . As  $\mu(k_{\mathfrak{p}_0})$  is a finite group, on a lattice  $\theta$  is equal to  $\theta_2 \circ \theta_1$ . Hence by a theorem of G. Prasad [Pr75],  $\theta = \theta_2 \circ \theta_1$ . In particular,  $\theta(\mathbb{G}(k)) = \mathbb{G}(k)$  and it can be uniquely extended to a continuous isomorphism between  $\mathbb{G}(k_{\mathfrak{p}})$  and  $\mathbb{G}(k_{\theta_1(\mathfrak{p})})$  for any  $\mathfrak{p}$ .

By Lemma 30 and the above discussion,  $\theta(\Lambda_{D_1}) = \Lambda_{D_2}$ . Therefore, again by the above discussion,  $\theta(P_{\mathfrak{p}}^{D_1}) = P_{\theta_1(\mathfrak{p})}^{D_2}$ , for any  $\mathfrak{p} \in V_k^\circ$ . However, if  $\mathbb{G}$  is quasi-split over  $k_{\mathfrak{p}}$ ,  $\mathbb{G}$  splits over  $\widehat{k}_{\mathfrak{p}}$ , and  $\mathfrak{p} \in D_1 \triangle \theta_1(D_2)$ , then on one hand  $\Theta_{\mathfrak{p}}^{D_1}$  and  $\Theta_{\theta_1(\mathfrak{p})}^{D_2}$  can be considered to be the same subset of  $\mathcal{D}_{\mathfrak{p}}$ , after identifying  $\mathcal{D}_{\mathfrak{p}}$  with  $\mathcal{D}_{\theta_1(\mathfrak{p})}$ , and on the other hand one of them is hyper-special and the other one is

not, which is a contradiction. Therefore  $D_1 \triangle \theta_1(D_2)$  is a subset of  $D_0$  the set of places such that either  $\mathbb{G}$  is not quasi-split over  $k_{\mathfrak{p}}$  or it does not split over  $\widehat{k}_{\mathfrak{p}}$ , which completes our proof.  $\square$

We notice that, by Theorem 14,

$$\text{vol}(G/\Gamma_D) \leq c_{23} q_k^{\dim \mathbb{G} \cdot \deg(\text{Div}(D))},$$

where  $\text{Div}(D) = \sum_{\mathfrak{p} \in D} \mathfrak{p}$  and  $c_{23}$  just depends on  $\mathbb{G}$  and  $k$ . On the other hand, as a consequence of Weil's theorem on Riemann hypothesis for curves over finite fields [R02, Proposition 17.2], for any  $N$ , the number of square-free effective divisors of  $k$  whose degree is  $N$  is at least  $c_{24} q_k^N$ , where  $c_{24}$  only depends on  $k$ . We also know that the group of automorphism of  $k$  is finite [Sc38]. Hence, by Lemmas 30 and 31, we get the desired polynomial lower bound on the number of maximal lattices in  $G$ .

#### 4.10 An upper bound on $\#\Gamma/\Lambda$ .

Here we will give a polynomial upper bound on  $\#\Gamma/\Lambda$  which is needed on counting the number of all the lattices with covolume at most  $x$ .

Let  $\Gamma$  be a maximal lattice in  $G$  with covolume at most  $x$  and  $k, l, \mathbb{G}, \Lambda$ , and  $\{P_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^\circ}$  as before.

**Lemma 32.** *In the above setting,  $\#\Gamma/\Lambda \leq x^c$ , where  $c$  just depends on  $G$ .*

*Proof.* By Rohlf's short exact sequence [BP89, Proposition 2.9] and arguments in 4.3, we know that

$$\#\Gamma/\Lambda \leq c_{25} \#H^1(k, \mu)_\xi \cdot \prod_{\mathfrak{p} \in V_k} \#\Xi_{\mathfrak{p}} \cdot \#\text{Aut } \mathcal{D}_{\mathfrak{p}_0},$$

where  $c_{25}$  just depends on  $G$ . By the main inequality, we have  $\#\mathfrak{R}(\Gamma) \leq \log x$ . On the other hand,  $\#\Xi_{\mathfrak{p}} \leq c_{26}$  where  $c_{26}$  just depends on  $G$ . Now, by Proposition 17, the upper bounds obtained for  $g_k$  and  $g_l$  in the proof of the main inequality and finally using Weil's Riemann hypothesis, we can conclude the desired inequality.  $\square$

## 5 Counting all the lattices and subgroup growth.

Sections 5.1 and 5.2 are devoted to the proof of the upper bound of Theorem 1 modulo Theorem 8, which is proved in Section 5.3, the lower bound of Theorem 1 is given in Section 5.4 and, finally, the proof of Theorem 3 is completed in Section 5.5.

## 5.1 Reduction to subgroup growth of certain pro- $p$ groups.

Let  $G = \mathbb{G}_0(K)$  as above. For any  $x$ , let  $\mathfrak{M}_x$  be a set of representatives of maximal lattices in  $G$  with covolume at most  $x$  up to  $\text{Aut}(G)$ . Hence, by Theorem 2,

$$\begin{aligned} \rho_x(G) &\leq \sum_{\Gamma \in \mathfrak{M}_x} s_{x/\text{vol}(G/\Gamma)}(\Gamma) \leq \#\mathfrak{M}_x \cdot \max_{\Gamma \in \mathfrak{M}_x} s_x(\Gamma) \\ &\leq x^{B \log \log x} \cdot \max_{\Gamma \in \mathfrak{M}_x} s_x(\Gamma). \end{aligned}$$

Thus, in order to prove the upper bound of Theorem 1, it is enough to show the following.

**Theorem 33.** *Let  $\Gamma$  be a maximal lattice in  $G$ . If CSP, MP and Weil conjecture hold and  $\text{vol}(G/\Gamma) \ll x$ , then*

$$\log s_x(\Gamma) \ll (\log x)^2,$$

where the implied constants only depend on  $G$ .

In this section we reduce the proof of Theorem 33 to understanding the subgroup growth of certain pro- $p$  groups. Let  $\Gamma$  be a maximal lattice in  $G$  with covolume at most  $x$  and  $k, l, \mathfrak{p}_0, \mathbb{G}, \Lambda$  and  $\mathcal{P} = \{P_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^\circ}$  as before. Let  $\mathfrak{R}(\mathcal{P})$  be the set of all the places in  $V_k^\circ$  such that  $P_{\mathfrak{p}}$  is not hyper-special.

**Lemma 34.** *In the above setting, we have that*

1-  $\deg(\text{Div}(\mathfrak{R}(\mathcal{P}))) \leq c_2 \log x$  where  $\text{Div}(\mathfrak{R}(\mathcal{P})) = \sum_{\mathfrak{p} \in \mathfrak{R}(\mathcal{P})} \mathfrak{p}$  and  $c_2$  just depends on  $G$ .

2-  $\#\Gamma/\Lambda \leq x^{c_3}$ , where  $c_3$  just depends on  $G$ .

*Proof.* Note that  $\deg(\text{Div}(\mathfrak{R}(\mathcal{P}))) \leq \deg(\text{Div}(\mathfrak{R}(\Gamma))) + \sum_{\mathfrak{p}/l \text{ ramified}} \deg(\mathfrak{p})$ . By Hurwitz genus formula,  $\sum_{\mathfrak{p}/l \text{ ramified}} \deg(\mathfrak{p}) \leq 2[\mathfrak{f}_l : \mathfrak{f}_k](g_l - 1) + 2[l : k]$ , and, by the main inequality,  $\deg(\mathfrak{R}(\Gamma)) \leq c_4 \log x$  where  $c_4$  just depends on  $G$ . On the other hand, by discussions in 4.5,  $g_l \leq c_5 \log x$  where  $c_5$  just depends on  $G$ . This finishes the proof of the first part. The second part is the direct consequence of Lemma 32.  $\square$

By Lemma 34 and [LS03, Lemma 1.2.2, Proposition 1.3.2],

$$s_x(\Gamma) \leq s_x(\Lambda) \cdot s_x(\Gamma/\Lambda) \cdot x^{c_3 \log x} \leq s_x(\Lambda) \cdot x^{(c_3^2 + c_3) \log x}.$$

So in order to get the desired result it is enough to give the right upper bound for  $s_x(\Lambda)$ . Let  $\widehat{\Lambda}$  be the profinite closure of  $\Lambda$ . Then there is a correspondence between the open subgroups of  $\widehat{\Lambda}$  and subgroups of finite index in  $\Lambda$ . As we assume the congruence subgroup property and Margulis-Platonov's conjecture, because of strong approximation,  $\widehat{\Lambda} \simeq \prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}$ .



Using a result of Babai-Cameron-Palfy [BCP82], Lubotzky [Lu95, Proposition 4.3] proved that if  $H$  is a subgroup of index at most  $x$  in  $\prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}$ , then it contains a subnormal subgroup of  $\prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}$  of index at most  $x^{c_6}$  where  $c_6$  just depends on  $G$ .<sup>1</sup> Hence, by [LS03, Lemma 1.2.3],

$$s_x\left(\prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}\right) \leq x^{c_6^2 \log x} \cdot s_{x^{c_6}}^{\lll} \left(\prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}\right),$$

where  $s_x^{\lll}(\bullet)$  is the number of subnormal subgroups of index at most  $x$ . Thus it is enough to get the right upper bound for  $s_x^{\lll}(\prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}})$ .

**Lemma 35.** *Let  $H$  be a subnormal subgroup of  $\prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}$  of index at most  $x$ . Then there is  $V(H)$  a finite subset  $V_k$  such that*

- 1- If  $\mathfrak{p}$  is not in  $V(H)$ , then  $P_{\mathfrak{p}} \subseteq H$ .
- 2-  $\deg(\text{Div}(V(H))) \leq c_7 \log x$ , where  $\text{Div}(V(H)) = \sum_{\mathfrak{p} \in V(H)} \mathfrak{p}$  and  $c_7$  just depends on  $G$ .

*Proof.* Let  $V(H) = \{\mathfrak{p} \in V_k^\circ \mid H \cap P_{\mathfrak{p}} \neq P_{\mathfrak{p}}\}$ . By Lemma 34,  $\deg(\mathfrak{R}(\mathcal{P})) \leq c_2 \log x$ . So it is enough to focus on places where  $P_{\mathfrak{p}}$  is hyper-special. Let  $P_{\mathfrak{p}}^{(1)}$  be the first congruence subgroup of  $P_{\mathfrak{p}}$ . As  $P_{\mathfrak{p}}$  is a hyper-special parahoric subgroup,  $P_{\mathfrak{p}}/P_{\mathfrak{p}}^{(1)}$  is a finite quasi-simple group. Hence any proper normal subgroup of  $P_{\mathfrak{p}}/P_{\mathfrak{p}}^{(1)}$  is contained in its center. Let  $Z_{\mathfrak{p}}$  be the preimage of the center of  $P_{\mathfrak{p}}/P_{\mathfrak{p}}^{(1)}$ . By the above discussion, if  $\mathfrak{p} \in V(H) \setminus \mathfrak{R}(\mathcal{P})$ , then either  $H \cap P_{\mathfrak{p}}$  is contained in  $Z_{\mathfrak{p}}$  or  $(H \cap P_{\mathfrak{p}})P_{\mathfrak{p}}^{(1)} = P_{\mathfrak{p}}$ . By [Lu95, Lemma 4.7], if  $(H \cap P_{\mathfrak{p}})P_{\mathfrak{p}}^{(1)} = P_{\mathfrak{p}}$ , then  $H \cap P_{\mathfrak{p}} = P_{\mathfrak{p}}$  as  $H \cap P_{\mathfrak{p}}$  is a subnormal subgroup of  $P_{\mathfrak{p}}$ . We claim that if  $\mathfrak{p} \in V(H) \setminus \mathfrak{R}(\mathcal{P})$ , then  $\pi_{\mathfrak{p}}(H) \subseteq Z_{\mathfrak{p}}$ . By the same argument as above,  $\pi_{\mathfrak{p}}(H) \subseteq P_{\mathfrak{p}}$  if  $\pi_{\mathfrak{p}}(H) \not\subseteq Z_{\mathfrak{p}}$ . Let  $H = N_s \triangleleft N_{s-1} \triangleleft \cdots \triangleleft N_1 \triangleleft \prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}$ , and assume that  $P_{\mathfrak{p}} \subseteq N_i$  and  $P_{\mathfrak{p}} \not\subseteq N_{i+1}$ . So for any  $a \in P_{\mathfrak{p}}$ , there is  $y_a \in \prod_{\mathfrak{p}' \in V_k^\circ \setminus \{\mathfrak{p}\}} P_{\mathfrak{p}'}$  such that  $(a, y_a)$  is in  $N_{i+1}$ . On the other hand,  $N_{i+1}$  is a normal subgroup of  $N_i$  and  $P_{\mathfrak{p}}$  is contained in  $N_i$ . Hence, for any  $a, a' \in P_{\mathfrak{p}}$ ,  $(a, y_a)^{-1}(a', 1)^{-1}(a, y_a)(a', 1) = (a^{-1}a'^{-1}aa', 1)$  is in  $N_{i+1}$ . Since  $P_{\mathfrak{p}}$  is perfect, it is a subgroup of  $N_{i+1}$ , which is a contradiction.

Overall, we have shown that

$$H \subseteq \prod_{\mathfrak{p} \in \mathfrak{R}(\mathcal{P})} P_{\mathfrak{p}} \cdot \prod_{\mathfrak{p} \in V(H) \setminus \mathfrak{R}(\mathcal{P})} Z_{\mathfrak{p}} \cdot \prod_{\mathfrak{p} \notin V(H) \cup \mathfrak{R}(\mathcal{P}) \cup \{\mathfrak{p}_0\}} P_{\mathfrak{p}}.$$

In particular, the index of  $H$  in  $\prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}$  is at least a constant power of  $\prod_{\mathfrak{p} \in V(H) \setminus \mathfrak{R}(\mathcal{P})} q_{\mathfrak{p}}$  and so combining Lemma 34, we have the desired result.  $\square$

<sup>1</sup>In [Lu95],  $\mathbb{G}$  is assumed to be split. However the same argument works without this assumption.

By Lemma 35, we have that

$$s_x^{\lll} \left( \prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}} \right) \leq \sum_{T \in \mathcal{V}_k(c_7 \log x)} s_x^{\lll} \left( \prod_{\mathfrak{p} \in T} P_{\mathfrak{p}} \right) \leq \#\mathcal{V}_k(c_7 \log x) \cdot \sup_{T \in \mathcal{V}_k(c_7 \log x)} s_x \left( \prod_{\mathfrak{p} \in T} P_{\mathfrak{p}} \right),$$

where  $\mathcal{V}_k(y) := \{T \subseteq V_k^\circ \mid \sum_{\mathfrak{p} \in T} \deg(\mathfrak{p}) \leq y\}$ . By Lemma 27 and the argument after that,  $\#\mathcal{V}_k(c_7 \log x) \leq x^{c_8}$ , where  $c_8$  just depends on  $G$ , and so it is enough to get the desired upper bound only for  $s_x(\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}})$ , where  $T \in \mathcal{V}_k(c_7 \log x)$ .

We note that  $P_{\mathfrak{p}}^{(1)}$  the first congruence subgroup of  $P_{\mathfrak{p}}$  is a pro- $p$  normal subgroup of  $P_{\mathfrak{p}}$  and the index of  $\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)}$  in  $\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}$  is at most  $x^{c_9}$ , where  $c_9$  only depends on  $G$ . Hence, again by [LS03, Lemma 1.2.2, Proposition 1.3.2],

$$s_x \left( \prod_{\mathfrak{p} \in T} P_{\mathfrak{p}} \right) \leq s_x \left( \prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)} \right) \cdot s_x \left( \prod_{\mathfrak{p} \in T} P_{\mathfrak{p}} / P_{\mathfrak{p}}^{(1)} \right) \cdot x^{c_9 \log x} \leq s_x \left( \prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)} \right) \cdot x^{(c_8^2 + c_9) \log x}.$$

Thus the right upper bound for  $s_x(\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)})$ , where  $T \in \mathcal{V}_k(c_7 \log x)$ , finishes the proof of Theorem 33.

## 5.2 Reduction to Theorem 8 on graded Lie algebras.

Following [LS94, ANS03], in order to understand  $s_x(\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)})$ , where  $T \in \mathcal{V}_k(c_7 \log x)$ , we will work with the associated graded Lie algebra. In this section, we complete the proof of Theorem 1 modulo Theorem 8, which will be proved in 5.3.

Let  $\mathcal{L}$  be the graded Lie algebra associated with the filtration  $\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(i)}$  (for the definition of  $P_{\mathfrak{p}}^{(i)}$  and the associated graded Lie algebras see Sections 3.7 and 3.8). Thus  $\mathcal{L} \simeq \bigoplus_{\mathfrak{p} \in T} L_{\Theta_{\mathfrak{p}}}$ .

**Proposition 36.** *In the above setting, let  $\mathcal{H}$  be an  $\mathfrak{f}_p$ -subalgebra of  $\mathcal{L}$  with finite  $\mathfrak{f}_p$ -codimension; then there are positive numbers  $c_{10}$  and  $c_{11}$  depending only on  $G$  such that*

$$\text{codim}_{\mathcal{H}}[\mathcal{H}, \mathcal{H}] \leq c_{10} \deg T + c_{11} \text{codim}_{\mathcal{L}} \mathcal{H},$$

where  $\deg T = \sum_{\mathfrak{p} \in T} \deg \mathfrak{p}$ .

*Proof.* Let  $\mathfrak{F}$  be the algebraic closure of  $\mathfrak{f}_p$  and  $\mathfrak{H} = \mathcal{H} \otimes_{\mathfrak{f}_p} \mathfrak{F}$ ; then  $\mathfrak{H}$  is an  $\mathfrak{F}$ -subalgebra of

$$\mathcal{L} \otimes_{\mathfrak{f}_p} \mathfrak{F} \simeq (\mathcal{L} \otimes_{\mathfrak{f}_p} \mathfrak{f}_k) \otimes_{\mathfrak{f}_k} \mathfrak{F} \simeq (\bigoplus_{\mathfrak{p} \in T} \mathfrak{L}_{\Theta_{\mathfrak{p}}}^{\deg \mathfrak{p}})^{[\mathfrak{f}_k: \mathfrak{f}_p]},$$

and the  $\mathfrak{f}_p$ -codimension of  $\mathcal{H}$  in  $\mathcal{L}$  is equal to the  $\mathfrak{F}$ -codimension of  $\mathfrak{H}$  in  $\mathcal{L} \otimes_{\mathfrak{f}_p} \mathfrak{F}$ . Note that the Galois group of  $\mathfrak{F}/\mathfrak{f}_p$  acts on  $\mathcal{L} \otimes_{\mathfrak{f}_p} \mathfrak{F}$  and  $\mathcal{L}$  is the subalgebra which is fixed by this action. We claim that  $\text{codim}_{\mathcal{H}}[\mathcal{H}, \mathcal{H}] = \text{codim}_{\mathfrak{H}}[\mathfrak{H}, \mathfrak{H}]$ . Let  $\{h_i\}$  be an  $\mathfrak{f}_p$ -basis of  $\mathcal{H}$ ; then the  $\mathfrak{f}_p$ -span (resp.  $\mathfrak{F}$ -span) of  $\{[h_i, h_j]\}$  is equal to  $[\mathcal{H}, \mathcal{H}]$  (resp.  $[\mathfrak{H}, \mathfrak{H}]$ ). Hence  $[\mathcal{H}, \mathcal{H}]$  is the  $\mathfrak{f}_p$ -structure of  $[\mathfrak{H}, \mathfrak{H}]$  under the above Galois group action. Thus  $\mathcal{H}/[\mathcal{H}, \mathcal{H}]$  is an  $\mathfrak{f}_p$ -structure of  $\mathfrak{H}/[\mathfrak{H}, \mathfrak{H}]$ , which gives

the claimed equality.

On the other hand, by Corollary 11,  $(\bigoplus_{\mathfrak{p} \in T} \mathfrak{L}_{\Theta_{\mathfrak{p}}}^{\deg \mathfrak{p}})^{[f_k : f_p]}$ , has an  $\mathfrak{F}$ -subalgebra of  $\mathfrak{F}$ -codimension at most  $c_{12} \deg T$  ( $c_{12}$  just depends on  $G$ ) which is an  $\mathfrak{F}$ -subalgebra of  $\mathfrak{F}$ -codimension at most  $c_{12} \deg T$  in  $\mathfrak{L} = \bigoplus_{\mathfrak{p} \in T} \mathfrak{L}_{\mathfrak{p}, \psi_s}^{[f_k : f_p] \deg \mathfrak{p}}$  where  $\mathfrak{L}_{\mathfrak{p}, \psi_s}$  is the graded Lie algebra associated with the filtration of the parahoric subgroup of the type  $\{\psi_s\}$  in  $\mathbb{G}(\widehat{k}_{\mathfrak{p}})$  (for the definition of  $\psi_s$  see 3.5.). Hence one can find  $\mathfrak{h}$  an  $\mathfrak{F}$ -subalgebra of  $\mathfrak{H}$  such that

- 1-  $\text{codim}_{\mathfrak{H}} \mathfrak{h} \leq c_{12} \deg T$ .
- 2-  $\mathfrak{h}$  can be embedded in  $\mathfrak{L}$  as an  $\mathfrak{F}$ -subalgebra, and

$$\text{codim}_{\mathfrak{L}} \mathfrak{h} \leq \text{codim}_{\mathcal{L} \otimes_{f_p} \mathfrak{F}} \mathfrak{H} + c_{12} \deg T = \text{codim}_{\mathcal{L}} \mathcal{H} + c_{12} \deg T. \quad (14)$$

By the above discussion and inequality, we have that

$$\text{codim}_{\mathcal{H}} [\mathcal{H}, \mathcal{H}] = \text{codim}_{\mathfrak{H}} [\mathfrak{H}, \mathfrak{H}] \leq \text{codim}_{\mathfrak{H}} [\mathfrak{h}, \mathfrak{h}] \leq \text{codim}_{\mathfrak{h}} [\mathfrak{h}, \mathfrak{h}] + c_{12} \deg T. \quad (15)$$

By Corollary 13, we know that  $\mathfrak{L}_{\mathfrak{p}, \psi_s} \simeq \bigoplus_{i=1}^{\infty} \mathfrak{g}_{\mathfrak{p}, i(\text{mod } r_{\phi})} \otimes t^i$ , where  $\mathfrak{g}_{\mathfrak{p}} = \bigoplus_{i=1}^{r_{\phi}-1} \mathfrak{g}_{\mathfrak{p}, i}$  is a finite dimensional perfect  $\mathfrak{F}$ -algebra. Moreover  $\mathfrak{g}_{\mathfrak{p}}$  just depends on the type of  $\mathbb{G}$  over  $\widehat{k}_{\mathfrak{p}}$ . Thus

$$\mathfrak{L} \simeq \mathfrak{L}(\mathfrak{g}_s)^{[f_k : f_p] \deg T_s} \oplus \mathfrak{L}(\mathfrak{g}_r)^{[f_k : f_p] \deg T_r} \oplus \mathfrak{L}(\mathfrak{g}_n)^{[f_k : f_p] \deg T_n}$$

where  $T_s$  consists of the places in  $T$  over which  $\mathbb{G}$  splits,  $T_r$  consists of the places in  $T$  over which  $\mathbb{G}$  does not split but  $\Phi$  is reduced, and  $T_n$  consists of the places in  $T$  over which  $\Phi$  is non-reduced,  $\mathfrak{L}(\mathfrak{g}_{\bullet})$ 's are the associated graded Lie algebras, and  $\deg T_{\bullet} = \sum_{\mathfrak{p} \in T_{\bullet}} \deg \mathfrak{p}$ .

Let  $\mathfrak{L}_s = \mathfrak{L}(\mathfrak{g}_s)^{[f_k : f_p] \deg T_s}$  and  $\mathfrak{h}_s = \mathfrak{h} \cap \mathfrak{L}_s$ ; similarly define  $\mathfrak{L}_r$ ,  $\mathfrak{L}_n$ ,  $\mathfrak{h}_r$  and  $\mathfrak{h}_n$ . Therefore, by Theorem 8, there is  $c_{13}$  a constant depending on  $G$ , such that

- 1-  $\text{codim}_{\mathfrak{L}_s} [\mathfrak{h}_s, \mathfrak{h}_s] \leq c_{13}(\text{codim}_{\mathfrak{L}_s} \mathfrak{h}_s + [f_k : f_p] \deg T_s)$ ,
- 2-  $\text{codim}_{\mathfrak{L}_r} [\mathfrak{h}_r, \mathfrak{h}_r] \leq c_{13}(\text{codim}_{\mathfrak{L}_r} \mathfrak{h}_r + [f_k : f_p] \deg T_r)$ ,
- 3-  $\text{codim}_{\mathfrak{L}_n} [\mathfrak{h}_n, \mathfrak{h}_n] \leq c_{13}(\text{codim}_{\mathfrak{L}_n} \mathfrak{h}_n + [f_k : f_p] \deg T_n)$ .

Hence we have

$$\begin{aligned} \text{codim}_{\mathfrak{h}} [\mathfrak{h}, \mathfrak{h}] &\leq \text{codim}_{\mathfrak{L}_s} [\mathfrak{h}_s, \mathfrak{h}_s] + \text{codim}_{\mathfrak{L}_r} [\mathfrak{h}_r, \mathfrak{h}_r] + \text{codim}_{\mathfrak{L}_n} [\mathfrak{h}_n, \mathfrak{h}_n] + 3\text{codim}_{\mathfrak{L}} \mathfrak{h} \\ &\leq c_{13}(3 \text{codim}_{\mathfrak{L}} \mathfrak{h} + [f_k : f_p] \deg T) + 3 \text{codim}_{\mathfrak{L}} \mathfrak{h} \\ &= c_{13}[f_k : f_p] \deg T + 3(c_{13} + 1)\text{codim}_{\mathfrak{L}} \mathfrak{h}. \end{aligned} \quad (16)$$

Now inequalities 14, 15, and 16 complete our proof.  $\square$

*Proof of Theorem 33 modulo Theorem 8.* By the previous discussions, we only have to give the right upper bound for  $s_x(\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)})$ , where  $T \in \mathcal{V}_k(c_7 \log x)$ . We complete the proof as in [LS03, Page 115]. Let  $H$  be a subgroup of index  $p^d$  in  $\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)}$  and

$$\mathcal{L}(H) = \bigoplus_{i=1}^{\infty} (H \cap \prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(i)}) \prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(i+1)} / \prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(i+1)},$$

the associated  $\mathfrak{f}_p$ -subalgebra of  $\mathcal{L}$ . It is clear that the  $\mathfrak{f}_p$ -codimension of  $\mathcal{L}(H)$  in  $\mathcal{L}$  is  $d$  and  $[\mathcal{L}(H), \mathcal{L}(H)]$  is a subalgebra of  $\mathcal{L}([H, H])$ . Therefore, by Proposition 36,

$$d(H) := \dim_{\mathfrak{f}_p}(H/([H, H]H^p)) \leq \text{codim}_{\mathcal{L}(H)}[\mathcal{L}(H), \mathcal{L}(H)] \leq c_{10}c_7 \log x + c_{11}d.$$

Thus  $d_i(\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)}) := \max\{d(H) \mid [\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)} : H] = p^i\} \leq c_{14} \log x + c_{11}i$ . and so, by [LS03, Proposition 1.6.2],

$$a_{p^i}(\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)}) = \#\{H \mid [\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)} : H] = p^i\} \leq p^{\sum_{j=0}^i d_j(\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)})} \leq p^{c_{14}i \log x + c_{11}i^2}.$$

Hence we have

$$s_x(\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)}) \leq \sum_{p^i \leq x} a_{p^i}(\prod_{\mathfrak{p} \in T} P_{\mathfrak{p}}^{(1)}) \leq \sum_{p^i \leq x} p^{c_{12}i \log x + c_{11}i^2} \leq \log x \cdot x^{(c_{14} + c_{11}) \log x},$$

which finishes our proof modulo Theorem 8.  $\square$

### 5.3 Graded Lie algebras.

In this section, we prove Theorem 8, which completes our proof.

**Lemma 37.** *Let  $\mathfrak{g}$  be Lie algebra,  $\mathfrak{g}_0$  and  $\mathfrak{g}_1$  two subspaces of  $\mathfrak{g}$ , and  $D$  a natural number; then for any  $U$  and  $V$  subspaces of  $\mathfrak{g}_0^D$  and  $\mathfrak{g}_1^D$ , respectively, we have*

$$\text{codim}_{[\mathfrak{g}_0, \mathfrak{g}_1]^D} [U, V] \leq \dim(\mathfrak{g}_1) \text{codim}_{\mathfrak{g}_0^D} U + \dim[\mathfrak{g}_0, \mathfrak{g}_1] \text{codim}_{\mathfrak{g}_1^D} V.$$

*Proof.* Let  $d = \dim \mathfrak{g}_1$ . As in [LS03, Section 6.3], let us consider  $M_{D,d}(\mathfrak{g}_1)$  the set of all  $D$  by  $d$  matrices with entries in  $\mathfrak{g}_1$ . For any  $\mathbf{x} \in M_{D,d}(\mathfrak{g}_1)$ , let  $W_i(\mathbf{x})$  be the linear span of the entries in the  $i^{\text{th}}$  row of  $\mathbf{x}$  and  $\rho(\mathbf{x}) = \sum_{i=1}^D \dim W_i(\mathbf{x})$ . Let  $V^{(d)}$  be the the subspace of  $M_{D,d}(\mathfrak{g}_1)$  consisting of matrices whose columns are in  $V$ . Choose  $\mathbf{x}$  in  $V^{(d)}$  such that  $\rho(\mathbf{x}) = \max_{\mathbf{y} \in V^{(d)}} \rho(\mathbf{y})$ . By permuting the rows of  $\mathbf{x}$  and changing  $V$  and  $U$  if necessary, without loss of generality, we can assume that  $W_i(\mathbf{x}) = \mathfrak{g}_1$  for  $i \leq t$  and  $W_i(\mathbf{x}) \neq \mathfrak{m}$  for  $t < i$ , where  $0 \leq t \leq D$ . Hence  $\sum_{j=1}^d [\mathfrak{g}_0, x_{ij}] = [\mathfrak{g}_0, \mathfrak{g}_1]$  for any  $i \leq t$ , and so

$$[\mathfrak{g}_0, \mathfrak{g}_1]^t \oplus 0^{D-t} \subseteq \sum_{j=1}^d [\mathfrak{g}_0^D, \vec{x}_j], \quad (17)$$

where  $\vec{x}_j = (x_{1j}, \dots, x_{Dj})$  is the  $j^{\text{th}}$  column of  $\mathbf{x}$ . On the other hand, for any  $j$ , we have that

$$\dim[U, \vec{x}_j] + \dim U \cap \ker[\bullet, \vec{x}_j] = \dim U.$$

Hence  $\dim[U, \vec{x}_j] \geq \dim[\mathfrak{g}_0^D, \vec{x}_j] - \text{codim}_{\mathfrak{g}_0^D} U$ . Thus

$$\dim[U, V] \geq \dim \sum_{j=1}^d [U, \vec{x}_j] \geq \dim \sum_{j=1}^d [\mathfrak{g}_0^D, \vec{x}_j] - d \text{codim}_{\mathfrak{g}_0^D} U. \quad (18)$$

By (17) and (18), we have that

$$\dim[U, V] \geq t \dim[\mathfrak{g}_0, \mathfrak{g}_1] - d \text{codim}_{\mathfrak{g}_0^D} U,$$

which means

$$\text{codim}_{[\mathfrak{g}_0, \mathfrak{g}_1]^D} [U, V] \leq (D - t) \dim[\mathfrak{g}_0, \mathfrak{g}_1] + d \text{codim}_{\mathfrak{g}_0^D} U. \quad (19)$$

By (19), it is enough to show that

$$(D - t) \dim[\mathfrak{g}_0, \mathfrak{g}_1] \leq \dim[\mathfrak{g}_0, \mathfrak{g}_1] \text{codim}_{\mathfrak{g}_1^D} V.$$

Assume the contrary, i.e.  $D - t > \text{codim}_{\mathfrak{g}_1^D} V$ . In particular,  $D > t$ , i.e.  $W_D(\mathbf{x})$  is a proper subspace of  $\mathfrak{g}_1$ . Since  $\dim \mathfrak{g}_1 = d$ , without loss of generality, we can assume that

$$\text{span}\langle x_{D1}, \dots, x_{Dd} \rangle = \text{span}\langle x_{D2}, \dots, x_{Dd} \rangle.$$

For any  $i$  larger than  $t$ , take  $y_i \in \mathfrak{g}_1 \setminus W_i(\mathbf{x})$ , and let  $\hat{y}_i$  be a vector in  $\mathfrak{g}_1^D$  whose only non-zero entry is the  $i^{\text{th}}$  entry,  $y_i$ . By the contrary assumption,  $V$  intersects  $\text{span}\langle \hat{y}_{t+1}, \dots, \hat{y}_D \rangle$  non-trivially. Let  $0 \neq \hat{z} \in V \cap \text{span}\langle \hat{y}_{t+1}, \dots, \hat{y}_D \rangle$ . Without loss of generality, we can assume that  $\hat{z}_D \neq 0$  and define  $\mathbf{y}$  as follows:

$$y_{ij} = \begin{cases} x_{ij} & \text{if } j \neq 1, \\ \hat{z}_i + x_{i1} & \text{if } j = 1. \end{cases}$$

Therefore  $\mathbf{y}$  is in  $V^{(d)}$ . On the other hand,  $W_i(\mathbf{y}) = W_i(\mathbf{x})$  for  $i \leq t$ , and it is easy to see that  $\dim W_i(\mathbf{y}) \geq \dim W_i(\mathbf{x})$  for  $i > t$  where the equality does not hold at least for  $i = D$ . So  $\rho(\mathbf{y}) > \rho(\mathbf{x})$  which is a contradiction.  $\square$

**Remark 38.** 1- What is important in this lemma is the fact that the coefficients  $\dim \mathfrak{g}_1$  and  $\dim[\mathfrak{g}_0, \mathfrak{g}_1]$  are independent of  $D$ .

- 2- When  $\mathfrak{g}$  is a perfect Lie algebra and  $\mathfrak{g}_0 = \mathfrak{g}_1 = \mathfrak{g}$ , this lemma is proved in [LS03, Section 6.2]. Our argument is a modification of theirs.
- 3- When  $\mathfrak{g}$  is a split Lie algebra and  $\mathfrak{g}_0 = \mathfrak{g}_1 = \mathfrak{g}$ , in [ANS03], Abért, Nikolov, and Szegedy prove a similar inequality with coefficient 2 instead of  $\dim(\mathfrak{g})$ .

*Proof of Theorem 8.* For any  $x = \sum_{i=1}^{\infty} x_i t^i$  in  $\mathfrak{L}^D$ , let  $\deg(x)$  be the smallest integer  $i$  such that  $x_i$  is not zero, and  $ld(x) = x_{\deg(x)}$ . For any  $n$ , let

$$\mathfrak{h}_n = \{ld(x) \mid x \in \mathfrak{h}, \deg(x) = n\} \cup \{0\}.$$

In a similar fashion, we can define  $[\mathfrak{h}, \mathfrak{h}]_n$ . Clearly  $\mathfrak{h}_n$  and  $[\mathfrak{h}, \mathfrak{h}]_n$  are subspaces of  $\mathfrak{g}_n^D$ , for any  $n$ . One can also see that

$$\text{codim}_{\mathfrak{L}^D} \mathfrak{h} = \sum_{n=1}^{\infty} \text{codim}_{\mathfrak{g}_n^D} \mathfrak{h}_n, \quad (20)$$

and a similar formula holds for the codimension of  $[\mathfrak{h}, \mathfrak{h}]$ . On the other hand, since, for any  $n \geq 2m$ ,

$$\sum_{i=0}^{m-1} [\mathfrak{h}_{a(n,i)}, \mathfrak{h}_{b(n,i)}] \subseteq [\mathfrak{h}, \mathfrak{h}]_n,$$

where  $a(n, i) = m \lfloor n/(2m) \rfloor + i$  and  $b(n, i) = n - a(n, i)$ , we have

$$\text{codim}_{\mathfrak{g}_n^D} [\mathfrak{h}, \mathfrak{h}]_n \leq \text{codim}_{\mathfrak{g}_n^D} \sum_{i=0}^{m-1} [\mathfrak{h}_{a(n,i)}, \mathfrak{h}_{b(n,i)}].$$

Hence we have

$$\text{codim}_{\mathfrak{L}^D} [\mathfrak{h}, \mathfrak{h}] \leq \sum_{n=1}^{\infty} \text{codim}_{\mathfrak{g}_n^D} \sum_{i=0}^{m-1} [\mathfrak{h}_{a(n,i)}, \mathfrak{h}_{b(n,i)}]. \quad (21)$$

By Lemma 37, we know that, for any  $0 \leq i \leq m-1$  and  $2m \leq n$ ,

$$\text{codim}_{[\mathfrak{g}_{a(n,i)}^D, \mathfrak{g}_{b(n,i)}^D]} [\mathfrak{h}_{a(n,i)}, \mathfrak{h}_{b(n,i)}] \leq \dim \widehat{\mathfrak{g}} (\text{codim}_{\mathfrak{g}_{a(n,i)}^D} \mathfrak{h}_{a(n,i)} + \text{codim}_{\mathfrak{g}_{b(n,i)}^D} \mathfrak{h}_{b(n,i)}).$$

Since  $\widehat{\mathfrak{g}}$  is a perfect Lie algebra and  $\{a(n, i) \mid 0 \leq i \leq m-1\}$  is a complete residue system mod  $m$ ,

$$\mathfrak{g}_n = \sum_{i=0}^{m-1} [\mathfrak{g}_{a(n,i)}, \mathfrak{g}_{b(n,i)}],$$

for any  $2m \leq n$ . Thus, for  $2m \leq n$ , we have

$$\begin{aligned} \text{codim}_{\mathfrak{g}_n^D} \sum_{i=0}^{m-1} [\mathfrak{h}_{a(n,i)}, \mathfrak{h}_{b(n,i)}] &\leq \sum_{i=0}^{m-1} \text{codim}_{[\mathfrak{g}_{a(n,i)}^D, \mathfrak{g}_{b(n,i)}^D]} [\mathfrak{h}_{a(n,i)}, \mathfrak{h}_{b(n,i)}] \\ &\leq \dim \widehat{\mathfrak{g}} \sum_{i=0}^{m-1} (\text{codim}_{\mathfrak{g}_{a(n,i)}^D} \mathfrak{h}_{a(n,i)} + \text{codim}_{\mathfrak{g}_{b(n,i)}^D} \mathfrak{h}_{b(n,i)}). \end{aligned}$$

Combining it with the inequality 21, we get

$$\text{codim}_{\mathcal{L}^D}[\mathfrak{h}, \mathfrak{h}] \leq 2 \dim \widehat{\mathfrak{g}} \cdot D + \dim \widehat{\mathfrak{g}} \sum_{n=1}^{\infty} \sum_{i=0}^{m-1} (\text{codim}_{\mathfrak{g}_{a(n,i)}^D} \mathfrak{h}_{a(n,i)} + \text{codim}_{\mathfrak{g}_{b(n,i)}^D} \mathfrak{h}_{b(n,i)}).$$

It is also easy to see that any positive integer  $k$  is equal to either  $a(n, i)$  or  $b(n, i)$  for at most  $4m$  pairs of numbers  $(n, i)$ . Therefore overall we have

$$\text{codim}_{\mathcal{L}^D}[\mathfrak{h}, \mathfrak{h}] \leq 2 \dim \widehat{\mathfrak{g}} \cdot D + 4m \dim \widehat{\mathfrak{g}} \sum_{k=1}^{\infty} \text{codim}_{\mathfrak{g}_k^D} \mathfrak{h}_k \leq C(D + \text{codim}_{\mathcal{L}^D} \mathfrak{h}),$$

where  $C = 4m \dim \widehat{\mathfrak{g}}$ , which finishes the proof.  $\square$

#### 5.4 A lower bound on the number of subgroups.

In order to get the lower bound of Theorem 1, we essentially follow Shalev's idea [Sh92]. However, we have to be extra careful as we are counting up to an automorphism of  $G$ .

In fact, we show that inside any maximal lattice we can find at least the claimed number of subgroups which are distinct even up to an automorphism of  $G$ .

**Lemma 39.** *Let  $\Gamma$  be a maximal lattice in  $G$ . Then*

1. For any  $x > x_0$

$$x^{c \log x / \log(\text{vol}(G/\Gamma))} \leq s_x(\Gamma)$$

where  $c$  and  $x_0$  just depend on  $G$ .

2. For any  $x > x_0$

$$x^{c \log x} \leq |\{\Lambda \subseteq \Gamma \mid \Lambda \text{ is a subgroup of } \Gamma, [\Gamma : \Lambda] \leq x\} / \sim|,$$

where  $x_0$  just depends on  $G$ ,  $c$  depends on  $\Gamma$  and  $\Lambda_1 \sim \Lambda_2$  if and only if there is an automorphism  $\theta$  of  $G$  such that  $\Lambda_2 = \theta(\Lambda_1)$ .

*Proof.* Since  $\Gamma$  is a maximal lattice, we can find  $k, \mathfrak{p}_0, \mathbb{G}, \Lambda$  and  $\{P_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^\circ}$  as described in Section 4.1. By the discussion in Section 4.7, we know that if  $\deg(\mathfrak{p}) \gg \log v$  where  $v = \text{vol}(G/\Gamma)$  and the implied constant just depends on  $G$ , then  $P_{\mathfrak{p}}$  is hyper-special. On the other hand, by [Sc38], we know that the group of automorphisms of  $k$  is finite. Hence, by Chebotarev's density Theorem [FJ05], the set of places  $\mathfrak{p}$  of  $k$  whose decomposition group, i.e.  $\{\theta \in \text{Aut}(k) \mid \theta(\mathfrak{p}) = \mathfrak{p}\}$ , is trivial has positive density. Now in order to prove the first part, let  $\mathfrak{p}_1$  be any place with degree  $O(\log v)$  (the implied constants depend only on  $G$ ) such that  $P_{\mathfrak{p}_1}$  is hyper-special and for the second part, let  $\mathfrak{p}_1$  be a place such that  $P_{\mathfrak{p}_1}$  is hyper-special and also the decomposition group of  $\mathfrak{p}_1$  is trivial. For any positive integer  $n$ ,  $P_{\mathfrak{p}_1}^{(n)}/P_{\mathfrak{p}_1}^{(2n)}$  is an  $\mathfrak{f}_{\mathfrak{p}_1}$ -vector space of dimension  $n \dim \mathbb{G}$ . So

$P_{\mathfrak{p}_1}^{(n)}/P_{\mathfrak{p}_1}^{(2n)}$  has at least  $q_{\mathfrak{p}_1}^{\lfloor (n \dim \mathbb{G})/2 \rfloor^2}$  subspaces. Preimage of any such subspace  $W$  gives us  $Q_W$  a subgroup of  $P_{\mathfrak{p}_1}^{(n)}$  which contains  $P_{\mathfrak{p}_1}^{(2n)}$ . Let

$$\Lambda_W = \mathbb{G}(k) \cap \prod_{\mathfrak{p} \in V_k^\circ \setminus \{\mathfrak{p}_1\}} P_{\mathfrak{p}} \cdot Q_W.$$

By strong approximation, we have that  $[\Lambda : \Lambda_W] = q_{\mathfrak{p}_1}^{n \dim \mathbb{G} - \dim_{\mathfrak{p}_1} W} \leq q_{\mathfrak{p}_1}^{n \dim \mathbb{G}}$ .

This shows that

$$s_{q_{\mathfrak{p}_1}^{n \dim \mathbb{G}}}(\Lambda) \geq q_{\mathfrak{p}_1}^{\lfloor (n \dim \mathbb{G})/2 \rfloor^2},$$

which (coupled with the way we chose  $\mathfrak{p}_1$ ) implies that  $s_x(\Lambda) \geq x^{c'_2 \log x / \log v}$ , where  $v = \text{vol}(G/\Gamma)$  and  $c'_2$  only depends on  $G$ . Therefore we have

$$\log s_x(\Gamma) \gg (\log(x/|\Gamma/\Lambda|))^2 / \log v, \quad (22)$$

where the implied constant only depends on  $G$ . For  $x \geq |\Gamma/\Lambda|^{3/2}$ , we have  $\log(x/|\Gamma/\Lambda|) \geq \frac{1}{3} \log x$  and so by (22)  $\log s_x(\Gamma) \gg (\log x)^2 / \log v$  as we wished. On the other hand, by the discussion in Section 4.1,  $\Gamma/\Lambda$  is a finite abelian group and its quotient by a subgroup of order at most  $t(\mathbb{G})^{\varepsilon(\mathbb{G})}$  is  $t(\mathbb{G})$ -torsion. It is worth mentioning that  $t(\mathbb{G})$  and  $\varepsilon(\mathbb{G})$  have upperbounds which just depend on  $G$ . Hence for some prime factor  $r$  of  $t(\mathbb{G})$  we have that

$$d_r(\Gamma/\Lambda) := \dim_{\mathfrak{f}_r}((\Gamma/\Lambda)/(\Gamma/\Lambda)^r) \gg \log |\Gamma/\Lambda|,$$

where the implied constant only depends on  $G$ . Thus, for  $x \gg 0$ , we have

$$\log s_x(\Gamma) \geq \log s_x(\Gamma/\Lambda) \gg \log |\Gamma/\Lambda|, \quad (23)$$

where the implied constants only depend on  $G$ . On the other hand, by Lemma 32, we have  $\log |\Gamma/\Lambda| \ll \log v$ . Thus by (23) we have

$$\log s_x(\Gamma) \gg (\log |\Gamma/\Lambda|)^2 / \log v.$$

Hence for  $x < |\Gamma/\Lambda|^{3/2}$  we have  $\log s_x(\Gamma) \gg (\log x)^2 / \log v$ , as we wished.

To get the second part, we have to show that only small number of these subgroups are equivalent, which is proved in the next lemma.

**Lemma 40.** *For a given  $W$  as above there are at most  $q_{\mathfrak{p}_1}^{cn}$  subspaces  $W'$  such that  $\theta(\Lambda_W) = \Lambda_{W'}$  for some  $\theta \in \text{Aut}(G)$ , where  $c$  only depends on  $G$ .*

*Proof.* Assume that  $\theta(\Lambda_W) = \Lambda_{W'}$ ; then, by a similar argument as in the proof of Lemma 31, there are  $\theta_1 \in \text{Aut}(k)$  and  $\theta_2 : \theta_1 \mathbb{G} \rightarrow \mathbb{G}$  a  $k$ -isomorphism such that  $\theta = \theta_2 \circ \theta_1$ . Hence for any  $\mathfrak{p} \in V_k^\circ$  the closure of  $\Lambda_W$  in  $\mathbb{G}(k_{\mathfrak{p}})$  is isomorphic to the closure of  $\Lambda_{W'}$  in  $\mathbb{G}(k_{\theta_1(\mathfrak{p})})$ . On the other hand, by strong approximation, the closure of  $\Lambda_W$  is either  $P_{\mathfrak{p}}$  if  $\mathfrak{p} \neq \mathfrak{p}_1$  or  $Q_W$  if  $\mathfrak{p} = \mathfrak{p}_1$  and  $P_{\mathfrak{p}}$ 's are parahoric subgroups and  $Q_W$  is not. Thus  $\theta_1(\mathfrak{p}_1) = \mathfrak{p}_1$ . So by the way that we chose  $\mathfrak{p}_1$ ,



we have that  $\theta_1$  is trivial,  $\theta \in (\text{Aut } \mathbb{G})(k)$ , and moreover  $\theta \in \prod_{\mathfrak{p} \in V_k^\circ \setminus \{\mathfrak{p}_1\}} \tilde{P}_\mathfrak{p}$ , where

$$\tilde{P}_\mathfrak{p} = \{\theta_\mathfrak{p} \in (\text{Aut } \mathbb{G})(k_\mathfrak{p}) \mid \theta_\mathfrak{p}(P_\mathfrak{p}) = P_\mathfrak{p}\}.$$

It also belongs to

$$\tilde{N}(Q_W, P_\mathfrak{p}^{(n)}) = \{\theta_{\mathfrak{p}_1} \in (\text{Aut } \mathbb{G})(k_{\mathfrak{p}_1}) \mid P_{\mathfrak{p}_1}^{(2n)} \subseteq \theta_{\mathfrak{p}_1}(Q_W) \subseteq P_{\mathfrak{p}_1}^{(n)}\}.$$

Overall the number that we are interested in is at most the number of left cosets of

$$(\text{Aut } \mathbb{G})(k) \cap \prod_{\mathfrak{p} \in V_k^\circ \setminus \{\mathfrak{p}_1\}} \tilde{P}_\mathfrak{p} \cdot \tilde{Q}_W$$

in

$$(\text{Aut } \mathbb{G})(k) \cap \prod_{\mathfrak{p} \in V_k^\circ \setminus \{\mathfrak{p}_1\}} \tilde{P}_\mathfrak{p} \cdot \tilde{N}(Q_W, P_\mathfrak{p}^{(n)}),$$

where  $\tilde{Q}_W = \{\theta_{\mathfrak{p}_1} \in (\text{Aut } \mathbb{G})(k_{\mathfrak{p}_1}) \mid \theta_{\mathfrak{p}_1}(Q_W) = Q_W\}$ . So it is at most the number of left cosets of  $\tilde{Q}_W$  in  $\tilde{N}(Q_W, P_{\mathfrak{p}_1}^{(n)})$ , which is at most

$$\#(\text{Aut } \mathbb{G})(k_{\mathfrak{p}_1})/\text{Ad}(\mathbb{G}(k_{\mathfrak{p}_1})) \cdot \#N(Q_W, P_{\mathfrak{p}_1}^{(n)})/N_{\mathbb{G}(k_{\mathfrak{p}_1})}(Q_W),$$

where  $N(Q_W, P_\mathfrak{p}^{(n)}) = \{g \in \mathbb{G}(k_\mathfrak{p}) \mid P_\mathfrak{p}^{(2n)} \subseteq gQ_Wg^{-1} \subseteq P_\mathfrak{p}^{(n)}\}$ . As the first factor just depends on  $G$ , without loss of generality we will give an upper bound for the second factor.  $P_{\mathfrak{p}_1}$  acts from left on  $X = N(Q_W, P_{\mathfrak{p}_1}^{(n)})/N_{\mathbb{G}(k_{\mathfrak{p}_1})}(Q_W)$  and

$$\#X = \sum_{[g] \in P_{\mathfrak{p}_1} \backslash X} \#P_{\mathfrak{p}_1}/(P_{\mathfrak{p}_1} \cap N_{\mathbb{G}(k_{\mathfrak{p}_1})}(gQ_Wg^{-1})). \quad (24)$$

Since  $g \in N(Q_W, P_{\mathfrak{p}_1}^{(n)})$ , we have that  $P_{\mathfrak{p}_1}^{(2n)} \subseteq gQ_Wg^{-1} \subseteq P_{\mathfrak{p}_1}^{(n)}$ . Hence  $P_{\mathfrak{p}_1}^{(n)}$  is contained in  $N_{\mathbb{G}(k_{\mathfrak{p}_1})}(gQ_Wg^{-1})$  and so, by equation (24), the number of elements of  $X$  is at most  $\#P_{\mathfrak{p}_1} \backslash X \cdot \#P_{\mathfrak{p}_1}/P_{\mathfrak{p}_1}^{(n)}$ . Because the latter term is at most  $q_{\mathfrak{p}_1}^{c_{15}n}$ , where  $c_{15}$  just depends on  $G$ , it is enough to give the right upper bound for the number of elements of

$$P_{\mathfrak{p}_1} \backslash N(Q_W, P_{\mathfrak{p}_1}^{(n)})/N_{\mathbb{G}(k_{\mathfrak{p}_1})}(Q_W).$$

It is clear that the number of discussed double cosets is at most equal to the number of right cosets of  $P_{\mathfrak{p}_1}$  in  $Y = \{g \in \mathbb{G}(k_{\mathfrak{p}_1}) \mid gP_{\mathfrak{p}_1}^{(2n)}g^{-1} \subseteq P_{\mathfrak{p}_1}^{(n)}\}$ . By a similar argument as above, we have

$$\#P_{\mathfrak{p}_1} \backslash Y = \sum_{[g] \in P_{\mathfrak{p}_1} \backslash Y/P_{\mathfrak{p}_1}} \#(g^{-1}P_{\mathfrak{p}_1}g \cap P_{\mathfrak{p}_1}) \backslash P_{\mathfrak{p}_1} \leq \#P_{\mathfrak{p}_1} \backslash Y/P_{\mathfrak{p}_1} \cdot \#P_{\mathfrak{p}_1}^{(2n)} \backslash P_{\mathfrak{p}_1}.$$

Again the latter term is at most  $q_{\mathfrak{p}_1}^{c_{16}n}$ , where  $c_{16}$  only depends on  $G$ , so it is enough to give the right upper bound for the number of double cosets of  $P_{\mathfrak{p}_1}$  in  $Y$ . The latter is a direct consequence of the definitions of  $Y$  and  $P_{\mathfrak{p}_1}^{(n)}$ 's, and the Cartan decomposition [T79, Section 3.3.3].  $\square$

To complete the proof of Lemma 39, it is enough to notice that, for any positive integer  $n$ ,  $\Lambda$  has at least  $p^{c_{17}n^2}$  many subgroups  $\Lambda_W$ 's of index at most  $p^{c_{18}n}$ , where  $c_{17}, c_{18}$  only depend on  $\Gamma$ . On the other hand, by Lemma 40, each orbit of  $\text{Aut}(G)$  intersects this set of lattices in a set of at most  $p^{c_{19}n}$  many elements, where  $c_{19}$  only depends on  $G$ . Hence, overall, the proof of the lower bound is completed as we get  $p^{c_{20}n^2}$  many lattices of index at most  $p^{c_{18}n}$  in  $\Lambda$ , which are distinct up to automorphisms of  $G$ .  $\square$

*Proof of the lower bound of Theorem 1.* We fix a maximal lattice in  $G$  and apply the second part of Lemma 39.  $\square$

## 5.5 Completion of the proofs.

*Proof of Theorem 3.* By the definition of  $\Lambda_0$ , it is equal to  $\mathbb{G}(k) \cap \prod_{\mathfrak{p} \in V_k^\circ} Q_{\mathfrak{p}}$ , where  $Q_{\mathfrak{p}}$  is an open compact subgroup of  $\mathbb{G}(k_{\mathfrak{p}})$ . So, for any  $\mathfrak{p}$ , there is a maximal parahoric subgroups  $P_{\mathfrak{p}}$  which contains  $Q_{\mathfrak{p}}$ . Note that for almost all places,  $P_{\mathfrak{p}} = Q_{\mathfrak{p}}$  and it is a hyper-special parahoric subgroup [T79]. So the lower bound can be proved using a similar construction as in the proof of Lemma 39. In fact, the argument here is much easier as the implied constants can depend on  $\Lambda_0$ . We take any  $\mathfrak{p}$  such that  $Q_{\mathfrak{p}} = P_{\mathfrak{p}}$  is a hyper-special parahoric and construct subgroups of  $\Lambda_0$  using subspaces of  $P_{\mathfrak{p}}^{(n)}/P_{\mathfrak{p}}^{(2n)}$  as in the proof of Lemma 39.

For the upper bound, we notice that  $\Lambda_0$  is contained in  $\Lambda = \mathbb{G}(k) \cap \prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}}$  and  $c_x(\Lambda_0) \leq c_{[\Lambda:\Lambda_0]x}(\Lambda)$ , and so it is enough to give the right upper bound for the number of congruence subgroups of  $\Lambda$ . By the strong approximation, we have to estimate  $s_x(\prod_{\mathfrak{p} \in V_k^\circ} P_{\mathfrak{p}})$ , which has been done in the second half of Section 5.1 and Section 5.2.  $\square$

*Proof of Corollary 4.* Here we can and will normalize the Haar measure in a way that the covolume of any lattice is at least 1 (by changing  $C, D$  and  $x_0$  if necessary). We first prove the upper bound. By Theorem 33, we have

$$\log s_y(\Gamma_{max}) \ll (\log y)^2,$$

for any maximal lattice  $\Gamma_{max}$  and  $y \gg \text{vol}(G/\Gamma)$ , where the implied constants only depend on  $G$ . In particular, for any  $x \geq x_0$  (where  $x_0$  only depends on  $G$ ) and any maximal lattice  $\Gamma_{max}$  in  $G$ , we have

$$\log s_x(\Gamma_{max}) \leq \log s_{v_mx}(\Gamma_{max}) \ll (\log(v_mx))^2,$$

where the implied constant only depend on  $G$  and  $v_m = \text{vol}(G/\Gamma_{max})$ . For an arbitrary lattice  $\Gamma$  in  $G$ , let  $\Gamma_{max}$  be a maximal lattice in  $G$  containing  $\Gamma$ . Then

$$\log s_x(\Gamma) \leq \log s_{|\Gamma_{max}/\Gamma|x}(\Gamma_{max}) \ll (\log(|\Gamma_{max}/\Gamma|v_mx))^2 = (\log(\text{vol}(G/\Gamma)x))^2.$$

This gives us the claimed upper bound.

For a given lattice  $\Gamma$  in  $G$ , let  $\Gamma_{max}$  be a maximal lattice containing it. Furthermore let  $\Lambda_{max}$ ,  $\mathbb{G}$  and  $\{P_{\mathfrak{p}}\}$  be the parameters given by Rohlf's criterion and  $\Lambda = \Lambda_{max} \cap \Gamma$ . Let  $v_m = \text{vol}(G/\Gamma_{max})$  and  $v = \text{vol}(G/\Gamma) = v_m[\Gamma_{max} : \Gamma]$ . We notice that  $\Gamma/\Lambda$  can be embedded into  $\Gamma_{max}/\Lambda_{max}$ . Hence

1. By Lemma 32,  $\log |\Gamma/\Lambda| \ll \log v_m$ , where the implied constant just depends on  $G$ .
2.  $\Gamma/\Lambda$  is a finite abelian group. Its quotient by a subgroup of order  $t(\mathbb{G})^{\varepsilon(\mathbb{G})}$  is  $t(\mathbb{G})$ -torsion. (Let us again recall that  $t(\mathbb{G})$  and  $\varepsilon(\mathbb{G})$  have upper bounds which only depend on  $G$ .)

On the other hand,  $|\Lambda_{max}/\Lambda| \leq |\Gamma_{max}/\Gamma| \leq v$ . By CSP and MP, the profinite closure  $\widehat{\Lambda}$  of  $\Lambda$  can be viewed as an open subgroup of the profinite closure  $\widehat{\Lambda}_{max}$  of  $\Lambda_{max}$ . Therefore  $\widehat{\Lambda}$  is a subgroup of index at most  $v$  in  $\prod_{\mathfrak{p} \in V_k^c} P_{\mathfrak{p}}$ . By the discussions in Section 5.1 and Lemma 35, for any  $\mathfrak{p}$  with  $\deg \mathfrak{p} \gg \log v$  (where the implied constant only depends on  $G$ ), we have that

1.  $P_{\mathfrak{p}}$  is hyper-special.
2.  $P_{\mathfrak{p}} \subseteq \widehat{\Lambda}$ .

Thus by an identical argument as in the proof of the first part of Lemma 39, one can finish the proof.  $\square$

## References

- [ANS03] M. Abért, N. Nikolov, B. Szegedy, *Congruence subgroup growth of arithmetic groups in positive characteristic*, Duke Math. J. **117** no. 2 (2003) 367-383.
- [BCP82] L. Babai, P. J. Cameron, P. P. Palfy, *On the orders of primitive groups with restricted non-abelian composition factors*, J. algebra **79** (1982) 161-168.
- [Be07] M. Belolipetsky, *Counting maximal arithmetic subgroups*, Duke Math. J. **140** (2007), no. 1, 1-33, with an appendix by J. Ellenberg and A. Venkatesh.
- [BGLS] M. Belolipetsky, T. Gelander, A. Lubotzky, A. Shalev, *Counting arithmetic lattices and surfaces*, Preprint.
- [BL] M. Belolipetsky, A. Lubotzky, *Counting manifolds and class field towers*, Preprint.
- [BGLM02] M. Burger, T. Gelander, A. Lubotzky, S. Mozes, *Counting hyperbolic manifolds*, Geom. and funct. anal. **12** (2002), no. 6, 1161-1173.

- [BP89] A. Borel, G. Prasad, *Finiteness theorems for discrete subgroups of bounded co-volume in semisimple groups*, Publications mathématiques de l'I.H.E.S. **69** (1989) 119-171.
- [BP90] A. Borel, G. Prasad, *Addendum: Finiteness theorems for discrete subgroups of bounded covolume in semisimple groups*, Publications mathématiques de l'I.H.E.S. **71** (1990) 173-177.
- [BT87] F. Bruhat, J. Tits, *Groupes réductifs sur un corps local III*, J. fac. sci. Univ. Tokyo **84** (1987) 671-698.
- [dJK] A. J. de Jong, N. Katz, *Counting the number of curves over a finite field*, Preprint, <http://www.math.columbia.edu/~dejong/papers/curves.dvi>
- [FJ05] M. D. Fried, M. Jarden, *Field arithmetic*, Springer-Verlag, Berlin, 2005.
- [G71] F. Giraud, *Cohomologie non abélienne*, Grund. Math. Wiss., Springer-Verlag, 1971.
- [GLP04] D. Goldfeld, A. Lubotzky, L. Pyber, *Counting congruence subgroups*, Acta math. **193** (2004) 73-104.
- [H74] G. Harder, *Chevalley groups over function fields and automorphic forms*, Ann. Math. **100** (1974) 249-306.
- [H75] G. Harder, *Über die Galoiskohomologie halbeinfacher algebraischer Gruppen III*, J. Reine angew. math. **274/275** (1975) 125-138.
- [Lu95] A. Lubotzky, *Subgroup growth and congruence subgroups*, Inventiones mathematicae **119** (1995) 267-295.
- [LN04] A. Lubotzky, N. Nikolov, *Subgroup growth of lattices in semisimple Lie groups*, Acta math. **193** (2004) 105-139.
- [LS94] A. Lubotzky, A. Shalev, *On some  $\Lambda$ -analytic pro- $p$  group*, Israel J. Math. **85** (1994) 307-337.
- [LS03] A. Lubotzky, D. Segal, *Subgroup growth*, Birkhäuser Verlag, 2003.
- [M77] G. Margulis, *Cobounded subgroups in algebraic groups over local fields*, Functional Anal. Appl. **11** (1977) 119-122.
- [M91] G. A. Margulis, *Discrete subgroups of semisimple Lie groups*, Springer-Verlag, Berlin, 1991.
- [M80] J. S. Milne, *Étale cohomology*, Princeton University Press, 1980.
- [MP94] A. Moy, G. Prasad, *Unrefined minimal  $K$ -types for  $p$ -adic groups*, Invent. Math. **116** no. 1-3 (1994) 393-408.
- [Pr75] G. Prasad, *Triviality of certain automorphisms of semisimple groups over local fields*, Mathematische Annalen **218** (1975) 219-227.

- [Pr77] G. Prasad, *Strong approximation*, Annals of math., 2nd series, **105** (1977) 553-572.
- [Pr89] G. Prasad, *Volumes of  $S$ -arithmetic quotients of semisimple groups*, Publications mathématiques de l'I.H.E.S. **69** (1989) 91-117.
- [PR84] G. Prasad, M. Raghunathan, *Topological central extensions of semisimple groups over local fields*, Annals of math., 2nd series, **119** no 1 (1984) 143-201.
- [PR] G. Prasad, A. Rapinchuk, *Development on the congruence subgroup problem after the work of Bass, Milnor and Serre*, Preprint. <http://www.math.lsa.umich.edu/~gprasad/milnor090608.pdf>
- [Ra76] M. S. Raghunathan, *On the congruence subgroup problem*, Publ. Math. IHES **46** (1976) 107-161.
- [Ra86] M. S. Raghunathan, *On the congruence subgroup problem II*, Invent. Math. **85** (1986) 73-117.
- [R02] M. Rosen, *Number theory in function fields*, Springer-Verlag, New York, 2002.
- [Sc38] H. L. Schmid, *Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik*, Jour. Reine Angew. Math. **179** (1938) 5-15.
- [T79] J. Tits, *Reductive groups over local fields*, Proceedings of symposia in pure mathematics **33** (1979) 29-69.
- [Sc85] W. Scharlau, *Quadratic and hermitian forms*, Springer-Verlag, Berlin, 1985.
- [Sh92] A. Shalev, *Growth functions,  $p$ -adic analytic groups and groups of finite co-class*, J. London Math. Soc. **46** (1992) 111-122.
- [Sh72] S. S. Shatz, *Profinite groups, arithmetic and geometry*, Ann. of Math studies **67** Princeton University Press, 1972.
- [We82] A. Weil, *Adeles and algebraic groups*, Progress in Math. **23**, Birkhäuser, Boston, 1982.

## 5.6 Appendix: table of notations.

$p$	A prime number larger than 3
$K$	A local field of characteristic $p$
$\mathbb{G}_0$	A simply connected absolutely almost simple $K$ -group
$G$	$\mathbb{G}_0(K)$
$k$	A function field
$q_k$	Number of elements of the constant field of $k$
$g_k$	The genus of $k$
$h_k$	The class number of $k$
$Br(\bullet)$	The Brauer group
$l$	A finite extension of $k$ of degree either 2 or 3
$h_l$	The class number of $l$
$V_k$	The set of equivalence classes of all the places on $k$
$Div(k)$	The group of divisors of $k$
$Div^+(k)$	The set of effective divisors of $k$
$Div(T)$	$= \sum_{\mathfrak{p} \in T} \mathfrak{p}$
$deg(T)$	$= \sum_{\mathfrak{p} \in T} deg \mathfrak{p}$
$\mathcal{V}_k(y)$	$= \{T \subseteq V_k^\circ \mid \sum_{\mathfrak{p} \in T} deg(\mathfrak{p}) \leq y\}$
$l(D)$	$= \dim_{f_k}(\{x \in k^\times \mid (x) + D \geq 0\} \cup \{0\})$ for a given divisor $D$
$k_{\mathfrak{p}}$	The $\mathfrak{p}$ -adic completion of $k$
$\mathcal{O}_{\mathfrak{p}}$	The ring of integers in $k_{\mathfrak{p}}$
$f_{\mathfrak{p}}$	The residue field of $k_{\mathfrak{p}}$
$\mathcal{O}(\mathfrak{p})$	The ring of $\mathfrak{p}$ -integers in $k$
$\mathbb{A}_k$	The ring of adeles of $k$
$\mathfrak{p}_0$	A fixed element of $V_k$ such that $k_{\mathfrak{p}} \simeq K$
$V_k^\circ$	$= V_k \setminus \{\mathfrak{p}_0\}$
$\mu_n$	The schematic kernel of $x \mapsto x^n$ from $\mathbb{G}_m$ to itself
$R_{l/k}^{(1)}(\mu_n)$	The schematic kernel of the norm map from $R_{l/k}(\mu_n)$ to $\mu_n$
$\mathbb{G}$	A simply connected absolutely almost simple $k$ -group
$\mu$	The center of $\mathbb{G}$
$\overline{\mathbb{G}}$	The adjoint form of $\mathbb{G}$

$\mathcal{G}$	The unique quasi-split inner $k$ -form of $\mathbb{G}$
$\overline{\mathcal{G}}$	The adjoint form of $\mathcal{G}$
$\mathbb{G}$	$\simeq \mathbb{G}_0$ over $K$
$P_{\mathfrak{p}}$	A parahoric subgroup in $\mathbb{G}(k_{\mathfrak{p}})$
$P_{\mathfrak{p}}^m$	A “large” parahoric subgroup whose intersection with $P_{\mathfrak{p}}$ contains an Iwahori
$\mathcal{P}_{\mathfrak{p}}$	One of the “largest” parahoric subgroups of $\mathcal{G}(k_{\mathfrak{p}})$
$\Theta_{\mathfrak{p}}$	The type of the parahoric subgroup $P_{\mathfrak{p}}$
$\overline{P}_{\mathfrak{p}}$	The set of stabilizer of $P_{\mathfrak{p}}$ in $\overline{\mathbb{G}}(k_{\mathfrak{p}})$
$\text{Cl}(\overline{\mathbb{G}}, \{\overline{P}_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^{\circ}})$	$= \overline{\mathbb{G}}(\mathbb{A}_k) / (\overline{\mathbb{G}}(k) \cdot \overline{\mathbb{G}}(k_{\mathfrak{p}_0}) \prod_{\mathfrak{p} \in V_k^{\circ}} \overline{P}_{\mathfrak{p}})$ (The class group of $\overline{\mathbb{G}}$ w.r.t. $\{\overline{P}_{\mathfrak{p}}\}$ )
$\text{cl}(\overline{\mathbb{G}}, \{\overline{P}_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^{\circ}})$	$= \#\text{Cl}(\overline{\mathbb{G}}, \{\overline{P}_{\mathfrak{p}}\}_{\mathfrak{p} \in V_k^{\circ}})$ (The class number of $\overline{\mathbb{G}}$ w.r.t. $\{\overline{P}_{\mathfrak{p}}\}$ )
$P_{\mathfrak{p}}^{(i)}$	The $i^{\text{th}}$ congruence subgroup of $P_{\mathfrak{p}}$ (except in Lemma 28)
$e(\mathfrak{p})$	Local factor in covolume formula
$e_m(\mathfrak{p})$	Local factor associated with $P_{\mathfrak{p}}^m$
$e_{qs}(\mathfrak{p})$	Local factor associated with $\mathcal{P}_{\mathfrak{p}}$
$e'(\mathfrak{p})$	Correctional factor in the covolume formula
$Z(\mathcal{G})$	The product of $e_{qs}(\mathfrak{p})$
$\mathfrak{s}(\mathcal{G})$	A number which depends on the type of $\mathcal{G}$ (ref. 4.2)
$B(\mathcal{G})$	$= q_k^{(g_k-1)\dim \mathcal{G}} (q_l^{g_l-1} / q_k^{(g_k-1)[l:k]})^{\mathfrak{s}/2}$
$\text{vol}$	The Haar measure on $G$ such that $\text{vol}(P_{\mathfrak{p}_0}) = 1$
$\varepsilon(\mathbb{G})$	$= 2$ (resp. $= 1$ ) if $\mathbb{G}$ is of type $D_r$ with $r$ even (resp. otherwise)
$t(\mathbb{G})$	The exponent of $\mu$
$T(\mathbb{G})$	$= \{\mathfrak{p} \in V_k \mid \mathbb{G} \text{ splits } \widehat{k}_{\mathfrak{p}} \text{ and } \mathbb{G} \text{ is not quasi-split } /k_{\mathfrak{p}}\}$
$T_c$	The set of ramified primes at the level of commensurability (ref. Def.20)
$T_l$	The set of ramified primes at the local level (ref. Def.20)
$\mathfrak{R}(\Gamma)$	$= T_c \cup T_l$
$\mathcal{D}_{\mathfrak{p}}$	The local Dynkin diagram of $\mathbb{G}/k_{\mathfrak{p}}$
$\Xi_{\mathfrak{p}}$	The subgroup of $\text{Aut } \mathcal{D}_{\mathfrak{p}}$ coming from $\overline{\mathbb{G}}(k_{\mathfrak{p}})$
$\xi_{\mathfrak{p}}$	The homomorphism from $H^1(k, \mu)$ to $\text{Aut } \mathcal{D}_{\mathfrak{p}}$
$\xi^{\circ}$	$= (\xi_{\mathfrak{p}})_{\mathfrak{p} \in V_k^{\circ}}$
$\xi$	$= (\xi_{\mathfrak{p}})_{\mathfrak{p} \in V_k}$
$H^1(k, \mu)_{\xi^{\circ}}$	$= \ker \xi^{\circ}$
$H^1(k, \mu)_{\xi}$	$= \ker \xi$
$\bullet^{\times}$	The group of units of the given ring
$\mathfrak{M}_x$	A set of representatives of maximal lattices in $G$ with covolume at most $x$
$\rho_x(G)$	Number of lattices with covolume at most $x$ in $G$ , up to an automorphism of $G$
$m_x(G)$	The number of maximal lattices, up to $\text{Aut}(G)$ , with covolume at most $x$ .
$s_x(\bullet)$	Number of subgroups of index at most $x$
$s_x^{\ll}(\bullet)$	Number of subnormal subgroups of index at most $x$
$c_x(\bullet)$	Number of congruence subgroups of index at most $x$
$a_x(\bullet)$	Number of subgroups of index $x$
$d(\bullet)$	Minimum number of elements of a generating set of a pro- $p$ group
$d_i(\bullet)$	Maximum of $d(\bullet)$ 's for all the subgroups of index $p^i$

DEPT. OF MATH, UNIV. OF CALIFORNIA, SAN DIEGO, CA, 92093-0112  
*E-mail address*:: asalehigolfsefidy@ucsd.edu